Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI

Office fédéral de la santé publique OFSP
Unité de direction Politique de la santé

RS 816.11.n / Annexe 2 de l'ordonnance du DFI du ... sur le dossier électronique du patient

Critères techniques et organisationnels de certification applicables aux communautés et aux communautés de référence (CTO)

Version: 1.0 22.03.2016
Entrée en vigueur : ...

Exigences à l’égard des communautés

1 Gestion (art. 8 ODEP)

1.1 Gestion des institutions de santé (let. a et c)

1.1.1 Les processus d’entrée et de sortie des institutions de santé doivent être définis, documentés, mis en œuvre et respectés.

1.1.2 Le processus d’entrée des institutions de santé doit garantir :
1.1.2.1 la conclusion d’accords exigeant et contrôlant le respect des tâches et obligations incombant à l’institution de santé, au moins en matière de protection et de sécurité des données ;
1.1.2.2 l’actualisation des données du service de recherche des institutions de santé et des professionnels de la santé visé à l’art. 40 ODEP ;
1.1.2.3 le déclenchement du processus « entrée de professionnels de la santé » (voir ch. 1.2.2) pour tous les professionnels de la santé admis rattachés à une institution de santé.

1.1.3 Le processus de sortie des institutions de santé doit garantir :
1.1.3.1 le déclenchement du processus « sortie de professionnels de la santé » (voir ch. 1.2.4) pour tous les professionnels de la santé sortants rattachés à une institution de santé ;
1.1.3.2 si l’institution de santé sortante ne s’affilie à aucune autre communauté :
1.1.3.2.1 la suppression des documents figurant dans les lieux de stockage de l’institution de santé sortante ;
1.1.3.2.2 la suppression des saisies du registre des documents qui renvoient aux documents figurant dans les lieux de stockage de l’institution sortante ;
1.1.3.2.3 l’information en temps utile des patients concernés.

1.1.4 La communauté est tenue, pour les données qu’elle enregistre dans le service de recherche central des institutions de santé et des professionnels de la santé visé à l’art. 40 ODEP :
1.1.4.1 de désigner une personne responsable ;
1.1.4.2 de garantir que l’actualité et l’exactitude des données sont vérifiées et confirmées :
1.1.4.2.1 chaque semestre au moins, dans le cas des institutions de santé ;
1.1.4.2.2 chaque trimestre au moins, dans le cas des groupes de professionnels de la santé.

1.2 Gestion des professionnels de la santé (let. a à d)

1.2.1 Les processus d’entrée, de gestion et de sortie des professionnels de la santé doivent être définis, documentés, mis en œuvre et respectés.

1.2.2 Le processus d’entrée des professionnels de la santé doit garantir que :
1.2.2.1 le consentement du professionnel de la santé à respecter les directives spécifiques de la communauté ou de l’institution de santé est documenté ;
1.2.2.2 l’identification du professionnel de la santé

1.2.2.2.1 repose sur le moyen d'identification d'un éditeur certifié selon l'art. 30 ODEP, ou
1.2.2.2.2 correspond aux exigences de l'art. 23 ODEP ;
1.2.2.3 le professionnel de la santé en question répond à la définition énoncée à l'art. 2, let. b, LDEP ;
1.2.2.4 le moyen d'identification du professionnel de la santé émis par un éditeur selon l'art. 30 ODEP est enregistré ;
1.2.2.5 les données du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 40 ODEP sont actualisées. Si le professionnel de la santé figure dans un registre professionnel fédéral ou cantonal (p. ex. Registre des professions médicales universitaires MedReg, Registre des professions de la psychologie PsyReg ou registre des professions de la santé NAREG), les données correspondantes de ce registre sont reprises.

1.2.3 Le processus de gestion des professionnels de la santé doit garantir que :
1.2.3.1 les données du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 40 ODEP sont actualisées ;
1.2.3.2 l'accès au dossier électronique du patient fait l'objet de contrôles ;
1.2.3.3 les droits d'accès sont adaptés.

1.2.4 Le processus de sortie des professionnels de la santé doit garantir que :
1.2.4.1 les données du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 40 ODEP sont actualisées ;
1.2.4.2 l'accès au dossier électronique du patient du patient est désactivé ;
1.2.4.3 les droits d'accès sont supprimés.

1.3 Gestion des auxiliaires des professionnels de la santé

1.3.1 Les communautés doivent prévoir des processus permettant d'enregistrer, de gérer et de supprimer les auxiliaires de professionnels de la santé dans un service interne de gestion des institutions de santé et des professionnels de la santé.

1.3.2 La gestion des auxiliaires est soumise, en dehors des exceptions énumérées ci-dessous, aux mêmes exigences que celles concernant l'entrée, la gestion et la sortie des professionnels de la santé. Font exception :
1.3.2.1 la garantie qu'il s'agit d'un professionnel de la santé au sens de l'art. 2, let. b, LDEP ;
1.3.2.2 l'actualisation du service de recherche des institutions de santé et des professionnels visé à l'art. 40 ODEP.

1.4 Identification et authentification (art. 8, let. d)

1.4.1 L'accès des professionnels de la santé au dossier électronique du patient ne peut se faire qu'à l'aide de moyens d'identification valables émis par un éditeur certifié selon l'art. 30.

1.4.2 Les communautés doivent garantir, aussi bien pour les professionnels de la santé que pour les auxiliaires, que leur identificateur univoque figurant dans le moyen d'identification et leur identité enregistrée dans la communauté soient reliées.

1.4.3 Les communautés doivent garantir que tous les systèmes techniques, comme par exemple les systèmes primaires ou les portails d'accès qui y sont reliés, utilisés par des professionnels de la santé ou des auxiliaires pour accéder au dossier électronique du patient :
1.4.3.1 supportent une procédure d'authentification forte conforme à l'état actuel de la technique, qui prévoit au moins deux facteurs d'authentification, comme condition préalable au traitement des données du dossier électronique du patient ;

1.4.3.2 mettent à disposition un terminal fiable pour communiquer de manière sûre avec le fournisseur de services d'identité (éditeur du moyen d'identification) conformément au ch. 3.2 (*P.TrustedCommunityEndpoint*) du profil de protection visé à l'art. 8 ODEP-DFI.

1.4.4 Les communautés sont tenues de reconnaître l'authentification correspondante suivie par d'autres communautés ou communautés de référence certifiées.

1.5 Gestion de groupes de professionnels de la santé (art. 8, let. a, c, e et f)

1.5.1 Les communautés sont responsables de la gestion des groupes de professionnels de la santé. Les directives et les procédures de gestion y afférentes doivent être définies, documentées, mises en œuvre et respectées.

1.5.2 Les directives et procédures doivent garantir que :
1.5.2.1 la composition des groupes est en tout temps identifiable pour les patients ;
1.5.2.2 les patients peuvent être informés lorsque des professionnels de la santé intègrent un groupe de professionnels de la santé ;
1.5.2.3 la taille du groupe reste raisonnable ;
1.5.2.4 les données du service de recherche des institutions de santé et des professionnels de la santé visé à l'art. 40 ODEP sont actualisées.

2 Tenue et transfert des données (art. 9 ODEP)

2.1 Destruction de données (al. 1, let. a et b)

2.1.1 Les communautés doivent prévoir des procédures qui garantissent que :
2.1.1.1 les documents saisis auprès d'elles dans le dossier électronique du patient par des professionnels de la santé sont détruits après dix ans;
2.1.1.2 en cas de suppression du dossier électronique du patient en vertu de l'art. 20, al. 1, ODEP, toutes les données sont détruites ; ce faisant, sont détruites au moins les données des systèmes de recherche suivants :
2.1.1.2.1 registre de documents ;
2.1.1.2.2 lieux de stockage des documents ;
2.1.1.2.3 index des patients ;
2.1.1.2.4 gestion des autorisations ;
2.1.1.2.5 portail d'accès.

2.2 Stockage des documents (al. 1, let. c)

2.2.1 Les communautés doivent prévoir des procédures qui garantissent que :
2.2.1.1 les documents du dossier électronique du patient sont enregistrées uniquement dans des lieux de stockage prévus à cet effet ;
2.2.1.2 seuls les formats de fichiers autorisés en vertu de l'annexe 3 ODEP-DFI peuvent être enregistrées dans les lieux de stockage des documents ;
2.2.1.3 les données au format « Portable Document Format »(PDF) sont sauvegardées uniquement en version PDF/A-1 ou PDF/A-2 ;
2.2.1.4 l'Unicode UTF-8 est utilisé pour le codage des signes, dans les données ou documents consultables.

2.3 Gestion à la demande du patient (al. 2)

2.3.1.1 Les communautés doivent prévoir des procédures afin qu'à la demande du patient des données déterminées le concernant (al. 2) :

2.3.1.1.1 ne soient pas enregistrées dans son dossier électronique du patient ;

2.3.1.1.2 restent accessibles dix années supplémentaires en application de l'art. 9, al. 1, let. a, ODEP ;

2.3.1.1.3 soient détruites dans son dossier électronique du patient.

2.3.2 Ne sont pas assujetties aux prescriptions de l'art. 9, al. 1 et 2, ODEP les données historisées et les données figurant dans les systèmes primaires non interrogeables ainsi que dans les sauvegardes.

2.4 Mise en œuvre des niveaux de confidentialité (al. 3, let. a)

2.4.1 Les communautés doivent garantir que :

2.4.1.1 le patient peut attribuer les niveaux de confidentialité prévus à l'art. 1 ODEP aux données du dossier électronique du patient. A cet effet, elles sont tenues d'appliquer l'un des quatre niveaux de confidentialité aux données selon l'attribution réalisée par le patient via le portail d'accès de la communauté;

2.4.1.2 le niveau de confidentialité prévu à l'art. 1, al. 2, ODEP ou le niveau de confidentialité choisi par le patient en vertu de l'art. 3, let. c, ODEP est attribué aux nouvelles données enregistrées dans le dossier électronique du patient ;

2.4.1.3 les professionnels de la santé peuvent attribuer le niveau de confidentialité « données sensibles » aux données qu'ils enregistrent dans le dossier électronique du patient.

2.5 Respect des droits d'accès accordés (al. 3, let. a)

2.5.1.1 Les communautés doivent garantir qu'il est possible d'accéder aux données enregistrées dans leurs lieux de stockage de documents et dans leur registre de documents uniquement en conformité avec décisions d'accès accordés, qu'elles auront préalablement demandés à la communauté de référence.

2.6 Accès en cas d'urgence (al. 3, let. a)

2.6.1 Concernant l'accès en cas d'urgence médicale (art. 2, al. 5, ODEP), les communautés doivent garantir :

2.6.1.1 qu'une justification de l'accès en cas d'urgence est donnée au préalable ;

2.6.1.2 qu'un accès en cas d'urgence n'est possible qu'après une double confirmation, moyennant une action manuelle, non reproductible automatiquement, du professionnel de la santé ;

2.6.1.3 que le patient est aussitôt informé de l'accès en cas d'urgence (*art. 9, al. 5, EPDG*) ;

2.6.1.4 que l'information concernant l'accès effectué en cas d'urgence ne contient elle-même aucune donnée sensible si elle est transmise par un autre moyen que le dossier électronique du patient (p. ex. SMS, courriel, etc.).

2.7 Vérification de la gestion des autorisations (al. 3, let. a)

2.7.1 La gestion des autorisations doit permettre de vérifier l'exactitude des fonctionnalités et des évaluations des règles en place dans le cadre des scénarios de tests automatisés.

2.8 Métadonnées (let. c)

2.8.1 Les communautés doivent garantir que les métadonnées énumérées à l'annexe 4 ODEP-DFI sont utilisées pour la description des documents mis à disposition dans le dossier électronique du patient.

2.9 Profils d'intégration (art. 3, let. d)

Interface standard avec la base de données d'identification de la Centrale de compensation (CdC)

2.9.1 Les points d'accès des communautés doivent veiller à se servir des interfaces techniques à la base de donnée UPI proposées par la Centrale de compensation (CdC) pour l'attribution et l'utilisation du numéro d'identification du patient conformément au règlement de traitement de la CdC.

2.9.2 Outre l'utilisation techniquement correcte des interfaces, il faut également respecter les prescriptions organisationnelles énoncées dans le règlement de traitement de la CdC.

Profils d'intégration, adaptations nationales des profils d'intégration et profils d'intégration nationaux

2.9.3 Pour la transmission d'informations, les communautés doivent utiliser les profils d'intégration définis à l'art. 5, let. a à c, (profils d'intégration, adaptations nationales des profils d'intégration et profils d'intégration nationaux) de l'annexe 5 ODEP-DFI.

Acteurs et transactions des profils d'intégration – Communication intercommunautaire

2.9.4 Les acteurs IHE *Initiating Gateway* et *Responding Gateway* doivent supporter les transactions suivantes des profils d'intégration IHE XCA et IHE XCPD, dans les versions selon l'annexe 5 ODEP-DFI :

2.9.4.1 Cross Gateway Query [ITI-38]
2.9.4.2 Cross Gateway Retrieve [ITI-39]
2.9.4.3 Cross Gateway Patient Discovery [ITI-55]
2.9.4.4 Patient Location Query [ITI-56]

Acteurs et transactions des profils d'intégration – Communication d'identités attestées

2.9.5 Le regroupement d'autres acteurs avec les acteurs IHE *X-Service Provider* et *X-Service User* du profil d'intégration IHE XUA est régi par les prescriptions des profils d'intégration nationaux et des adaptations nationales des profils selon l'annexe 5 ODEP-DFI et doit être effectué conformément à ces prescriptions.

2.9.6 Les acteurs IHE *X-Service Provider* et *X-Service User* doivent supporter la transaction suivante du profil d'intégration IHE XUA, dans la version selon l'annexe 5 ODEP-DFI :

2.9.6.1 Provide X-User Assertion [ITI-40]

Acteurs et transactions des profils d'intégration – Service de recherche des institutions de santé et des professionnels de la santé

2.9.7 Les acteurs IHE *Provider Information Consumer* et *Provider Information Source* doivent supporter les transactions suivantes du profil d'intégration IHE HPD, dans la version selon l'annexe 5 ODEP-DFI :

2.9.7.1 Provider Information Query [ITI-58]

2.9.7.2 Provider Information Feed [ITI-59]

Acteurs et transactions des profils d'intégration – Requête de documents

2.9.8 L'acteur IHE *Document Consumer* doit supporter les transactions suivantes du profil d'intégration IHE XDS, dans la version selon l'annexe 5 ODEP-DFI :

2.9.8.1 Registry Stored Query [ITI-18]

2.9.8.2 Retrieve Document Set [ITI-43]

Acteurs et transactions des profils d'intégration – Mise à disposition de documents

2.9.9 L'acteur IHE *Document Source* doit supporter les transactions suivantes du profil d'intégration IHE XDS, dans la version selon l'annexe 5 ODEP-DFI :

2.9.9.1 Provide and Register Document Set-b [ITI-41]

2.9.9.2 Retrieve Document Set [ITI-43]

Acteurs et transactions des profils d'intégration – Mutation des métadonnées de documents

2.9.10 L'acteur IHE *Document Administrator* doit supporter les transactions suivantes du profil d'intégration IHE XDS Metadata Update, dans la version selon l'annexe 5 ODEP-DFI :

2.9.10.1 Update Document Set [ITI-57]

2.9.10.2 Delete Document Set [ITI-62]

Acteurs et transactions des profils d'intégration – Registre de documents

2.9.11 L'acteur IHE *Document Registry* doit supporter les transactions suivantes des profils d'intégration XDS et IHE XDS Metadata Update, dans les versions selon l'annexe 5 ODEP-DFI :

2.9.11.1 Register Document Set-b [ITI-42]

2.9.11.2 Register Stored Query [ITI-18]

2.9.11.3 Update Document Set [ITI-57]

2.9.11.4 Delete Document Set [ITI-62]

Acteurs et transactions des profils d'intégration – Lieux de stockage des documents

2.9.12 L'acteur IHE *Document Registry* doit supporter les transactions suivantes du profil d'intégration IHE XDS, dans la version selon l'annexe 5 ODEP-DFI :

2.9.12.1 Provide and Register Document Set-b [ITI-41]

2.9.12.2 Retrieve Document Set [ITI-43]

Acteurs et transactions des profils d'intégration – Mise à disposition de données pour l'index des patients

2.9.13 L'acteur IHE *Patient Identity Source* doit supporter la transaction suivante des profils d'intégration PIX V3, dans les versions selon l'annexe 5 ODEP-DFI :

2.9.13.1 Patient Identity Feed HL7 v3 [ITI-44]

Acteurs et transactions des profils d'intégration – Mise à disposition et requête de l'index des patients

2.9.14 Les acteurs IHE *Patient Demographics Supplier* et *Patient Demographics Consumer* doivent supporter la transaction suivante du profil d'intégration PDQV3, dans les versions selon l'annexe 5 ODEP-DFI :

2.9.14.1 Patient Demographics Query V3 [ITI-47]

Acteurs et transactions des profils d'intégration – Gestion de l'index des patients

2.9.15 L'acteur IHE *Patient Identifier Cross-reference Manager* doit supporter les transactions suivantes du profil d'intégration IHE PIX V3, dans les versions selon l'annexe 5 ODEP-DFI.

2.9.15.1 Patient Identity Feed HL7 V3 [ITI-44]

2.9.15.2 PIX V3 Query [ITI-45]

2.9.15.3 PIX V3 Update Notification [ITI-46]

Acteurs et transactions des profils d'intégration – Authentification des systèmes et historisation des transactions IHE

2.9.16 Le regroupement d'autres acteurs avec les acteurs IHE *Secure Application* et *Secure Node Grouped with Any IHE Actor* du profil d'intégration IHE ATNA (ou de son adaptation nationale) est régi par les prescriptions des profils d'intégration IHE, des profils d'intégration nationaux et des adaptations des profils d'intégration et doit être effectué conformément à ces prescriptions.

2.9.17 Les acteurs *Secure Node grouped with Any IHE Actor* doivent supporter les transactions suivantes du profil d'intégration IHE ATNA et son adaptation nationale, selon l'annexe 5 ODEP-DFI :

2.9.17.1 Maintain Time [ITI-1]

2.9.17.2 Node Authentication [ITI-19]

2.9.18 Les acteurs *Secure Application* doivent supporter la transaction suivante du profil d'intégration IHE ATNA et son adaptation nationale, selon l'annexe 5 ODEP-DFI :

2.9.18.1 Record Audit Event [ITI-20]

Acteurs et transactions des profils d'intégration nationaux – Requête de la décision d'accès

2.9.19 Le regroupement d'autres acteurs avec l'acteur *Authorization Decision Consumer* du profil d'intégration national CH:ADR est régi par les prescriptions spécifiques de ce profil et doit être effectué conformément à ces prescriptions.

2.9.20 Les acteurs *Authorization Decision Provider*, *Authorization Decision Consumer* et *Policy Repository* doivent supporter les transactions du profil d'intégration national CH:ADR conformément aux spécifications techniques selon l'annexe 5 ODEP-DFI.

Acteurs et transactions des profils d'intégration nationaux – gestion de la configuration des autorisations

2.9.21 Les acteurs *Policy Repository* et *Policy Manager* doivent supporter les transactions du profil d'intégration national CH:PPQ conformément aux spécifications techniques selon l'annexe 5 ODEP-DFI.

Authentification avec des certificats valables

2.9.22 Les communautés doivent disposer d'un certificat électronique valable, acquis auprès d'un fournisseur de services de certification reconnu selon la loi fédérale du 19 décembre 2003 sur la signature électronique[1], pour :

2.9.22.1 l'authentification réciproque de leurs points d'accès ;

2.9.22.2 l'authentification réciproque entre leurs points d'accès et les services de recherche visés à l'art. 38, al. 1, let. a à c, ODEP ;

2.9.22.3 l'authentification réciproque entre leurs points d'accès et la base de données d'identification de la CdC.

2.9.23 Pour les échanges de données avec les services de recherche visés à l'art. 38, al. 1, let. a, ODEP, les communautés doivent utiliser les transactions du profil d'intégration IHE ATNA.

2.9.24 Pour les échanges de données avec la base de données d'identification de la CdC, les communautés doivent utiliser la plateforme d'échange de données SEDEX (*secure data exchange*) de l'Office fédéral de la statistique (OFS).

Cohérence de l'heure en Suisse (al. 6)

2.9.25 L'heure légale en Suisse diffusée par METAS est utilisée pour l'horodatage dans la communication et pour l'historisation. Les horloges de tous les systèmes de traitement de l'information pertinents doivent être synchronisées avec l'heure légale en Suisse.

2.10 Données historisées (al. 3, let. e)

Exigences concernant le système d'historisation

2.10.1 Tout traitement de données du dossier électronique du patient doit être historisé et horodaté.

2.10.2 Les données historisées doivent se limiter à ce qui est nécessaire et ne peuvent contenir aucune donnée médicale.

2.10.3 Les exigences suivantes sont applicables :

2.10.3.1 l'historisation prévue ne doit pas pouvoir être contournée ;

2.10.3.2 toute modification ultérieure des données historisées doit être impossible ;

2.10.3.3 lors de l'historisation, il faut distinguer les accès résultant de l'utilisation du dossier électronique du patient, qui doivent être visibles pour les patients, des accès technico-administratifs dans le cadre de l'exploitation du système ;

2.10.3.4 les administrateurs du système ne doivent pas pouvoir effacer ou désactiver l'historisation de leurs propres activités.

2.10.4 Des saisies dans l'historique consultables par le patient doivent être générées à chaque fois

[1] RS 943.03

2.10.4.1 lors du traitement des données suivantes :

2.10.4.1.1 documents dans les lieux de stockage ;
2.10.4.1.2 saisies dans le registre de documents ;
2.10.4.1.3 configuration de la gestion des autorisations ;
2.10.4.1.4 données de l'index des patients.

2.10.4.2 lors des événements suivants :

2.10.4.2.1 authentification dans le système (connexion/déconnexion) ;
2.10.4.2.2 tentatives d'accès, réussies ou infructueuses, au système ;
2.10.4.2.3 recherche du dossier électronique du patient ;
2.10.4.2.4 recherche de documents dans le dossier électronique du patient ;
2.10.4.2.5 accès d'urgence effectués ;
2.10.4.2.6 tentatives d'accès, réussies ou infructueuses, à des documents ;
2.10.4.2.7 enregistrement d'un nouveau moyen d'identification.

2.10.5 En cas d'accès à une fonction de recherche, l'historique doit contenir au moins :
2.10.5.1 les critères de recherche utilisés (p. ex. identificateurs utilisés, nom, date de naissance, etc.) ;
2.10.5.2 des indications sur le résultat de la recherche (p. ex. nombre de résultats) ;
2.10.5.3 les éventuelles actions consécutives (p. ex. choix d'un enregistrement dans une liste de résultats, impression, exportation de données).

2.10.6 Les données historisées doivent être conservées pendant dix ans.

2.10.7 La requête et la présentation des informations historisées en vue de leur consultation par le patient sont régies par les adaptations nationales du profil d'intégration IHE ATNA (Audit Trail Consumption) et le format d'échange technique pour les informations historisées prévu dans ces adaptations, selon l'annexe 5 ODEP-DFI.

2.11 Association du numéro d'identification du patient avec des documents (al. 3)

2.11.1 Les communautés doivent garantir que le numéro d'identification du patient fourni par la CdC n'est pas enregistré de manière durable dans les lieux de stockage des documents et les registres de documents et qu'il n'est pas relié directement et durablement avec des documents du patient dans les systèmes primaires.

3 Portail d’accès pour les professionnels de la santé (art. 10 ODEP)

3.1 Conformité aux dispositions légales

3.1.1 Le portail d’accès destiné aux professionnels de la santé doit satisfaire aux exigences légales en la matière.

3.2 Présentation

3.2.1 La présentation des interfaces utilisateurs dans le portail d’accès doit être correcte et exhaustive, et montrer clairement :

3.2.1.1 si c’est un professionnel de la santé ou le patient lui-même qui a mis à disposition le document ;

3.2.1.2 quels documents ont été mis à disposition par le professionnel de la santé qui y accède ;

3.2.1.3 quels documents ont été annulés ;

3.2.1.4 quelles versions d’un document sont éventuellement également disponibles.

3.3 Accessibilité

3.3.1 Le portail d’accès doit :

3.3.1.1 être conçu pour être pleinement accessible aux professionnels de la santé âgés ou ayant un handicap ;

3.3.1.2 remplir les conditions de conformité des directives pour l’accessibilité aux contenus Web (WCAG) 2.0 et atteindre le niveau de conformité AA.

3.4 Formats de fichiers : mise à disposition

3.4.1 Le portail d’accès doit :

3.4.1.1 permettre d’enregistrer les formats de fichiers autorisés en vertu de l’annexe 3 ODEP-DFI ;

3.4.1.2 convertir les autres fichiers dans un format autorisé, avant leur enregistrement dans un lieu de stockage.

3.5 Formats de fichiers : requête

3.5.1 Le portail d’accès doit :

3.5.1.1 permettre de faire une requête des formats de fichiers autorisés en vertu de l’annexe 3 ODEP-DFI ;

3.5.1.2 permettre de faire une requête des fichiers à enregistrer dans le système primaire (« download ») ;

3.5.1.3 prévoir le téléchargement non seulement un par un, mais aussi en masse (« bulk download ») des documents sélectionnés ;

3.5.1.4 afficher les données structurées sous une forme directement lisible par l’être humain, correcte et complète ;

3.5.1.5 permettre de télécharger les données structurées aussi bien dans leur format d’origine que sous une forme lisible par l’être humain.

3.5.2 La requête de documents pour affichage ou sauvegarde doit respecter les limites maximales définies en nombre de documents par unité de temps (« rate limits »), qui déclenchent, en cas de dépassement, des mesures adéquates de blocage ou de sécurité renforcée.

4 Protection et sécurité des données (art. 11 ODEP)

4.1 Exigences envers les tiers

4.1.1 Il incombe aux communautés d'assurer le respect des exigences formulées dans le présent chapitre (Protection et sécurité des données), y compris lorsqu'elles confient à des tiers (organisations d'exploitation) la réalisation de leurs prestations.

4.2 Système de gestion de la protection et de la sécurité des données (al. 1)

4.2.1 Les communautés doivent exploiter un système de gestion de la protection et de la sécurité des données tel que défini dans la norme ISO/IEC 27001:2013 qui :

4.2.1.1 définit expressément et maintient à jour toutes les exigences légales auxquelles doivent satisfaire les ensemble de données sensibles ;

4.2.1.2 détermine les mesures spécifiques nécessaires à leur exécution et les personnes chargées d'en assurer la surveillance ;

4.2.1.3 protège tous les enregistrements pertinents contre la perte, la destruction ou la falsification conformément aux exigences légales.

4.2.2 Le système de gestion de la protection et de la sécurité des données doit comprendre au moins :

4.2.2.1 un catalogue des risques, évalué par le responsable de la protection et de la sécurité des données (voir ch. 4.3) ;

4.2.2.2 un plan de traitement des risques ;

4.2.2.3 un inventaire à jour des moyens d'exploitation suivants (voir ch. 4.8) :

4.2.2.3.1 hardware

4.2.2.3.2 logiciels (softwares)

4.2.2.3.3 ensemble de données

4.2.2.3.4 organisation structurelle

4.2.2.3.5 processus

4.2.3 Les changements apportés aux moyens d'exploitation qui ont une incidence sur la sécurité doivent être analysés et documentés.

4.2.4 Un examen de gestion doit intervenir au moins une fois par an ; la direction de la communauté statue à cette occasion sur le catalogue des risques et sur le plan de traitement des risques.

4.3 Responsable de la protection et de la sécurité des données (al. 1, let. a)

4.3.1 Un responsable de la protection et de la sécurité des données est désigné pour s'occuper du système de gestion de la protection et de la sécurité des données. La communauté définit son cahier des charges. Il surveille le respect des prescriptions relatives à la protection et à la sécurité des données et :

4.3.1.1 il a les moyens d’exercer sa fonction en toute indépendance ;
4.3.1.2 il dispose des ressources nécessaires pour accomplir ses tâches.

4.4 Détection des incidents de sécurité (SIEM) (al. 1, let. b)

4.4.1 Les communautés doivent :
4.4.1.1 exploiter un système de détection et de gestion des incidents de sécurité (*security information and event management system* [SIEM]) qui surveille, en fonction des risques, tous les systèmes pertinents de l’infrastructure informatique interne de la communauté, qui détecte les anomalies et enregistre les événements pertinents pour la protection et la sécurité des données ;
4.4.1.2 protéger ces enregistrements contre toute modification ou suppression ;
4.4.1.3 garantir que les événements pertinents pour la protection et la sécurité des données sont traités de manière adéquate sur le plan organisationnel et technique, conformément au ch. 4.5.

4.4.2 Le SIEM doit être conçu en fonction des spécificités de la communauté. Il doit détecter et traiter au moins les schémas suivants :
4.4.2.1 cyberattaques lancées contre le portail d’accès ou le point d’accès de la communauté ;
4.4.2.2 hausse inhabituelle du nombre d’accès en écriture ou en lecture au lieu de stockage des documents, au registre de documents ou à l’index des patients, indiquant une utilisation abusive ou une attaque automatisée ;
4.4.2.3 mutations inhabituelles et critiques au niveau de gestion des autorisations, du système de gestion des identités et des accès (IAM) ou, le cas échéant, du service de gestion des institutions de santé et des professionnels de la santé interne à la communauté de manière analogue au service de recherche des institutions de santé et des professionnels de la santé visé à l’art. 40 ODEP (« HPD local »).

4.5 Gestion des incidents de sécurité (SIEM) (al. 1, let. b)

4.5.1 Les communautés doivent :
4.5.1.1 avoir défini des procédures formelles de déclaration immédiate et d’escalade en cas d’événement pertinents pour la protection et la sécurité des données (signalement à l’OFSP et à l’organisme de certification conformément à l’art. 11, al. 2, ODEP), ainsi qu’en exiger et en contrôler le respect ;
4.5.1.2 garantir que ces procédures et les obligations qui en découlent sont familières à tous les collaborateurs concernés de l’institution de santé ainsi qu’aux organisations d’exploitation.

4.5.2 Le SIEM :
4.5.2.1 englobe les processus de gestion des événements pertinents pour la sécurité ;
4.5.2.2 définit, en cas d’événement critique revêtant un niveau de gravité donné, au moins les processus d’urgence suivants visant à stopper immédiatement toute communication :
4.5.2.2.1 modalités et conditions requises pour isoler la communauté, par blocage de son point d’accès, du traitement des données du dossier électronique du patient ;
4.5.2.2.2 modalités et conditions requises pour isoler la communauté d’Internet ;
4.5.2.2.3 modalités et conditions requises pour isoler la communauté d’un système primaire auquel elle est reliée.

4.6 Protection contre les logiciels malveillants (al. 1, let. b)

4.6.1 Les communautés doivent :

4.6.1.1.1 veiller à définir et mettre en œuvre des mesures, des procédures et des systèmes de protection, de détection et de suppression des logiciels malveillants, ainsi que de surveillance des programmes auto-réplicatif (p. ex. virus) ;

4.6.1.1.2 s'assurer que les responsables des systèmes vérifient régulièrement que les programmes de détection et d'élimination des logiciels malveillants sont à jour.

4.7 Gestion des failles de sécurité (al. 1, let. b)

4.7.1 Les communautés doivent disposer d'une gestion des failles de sécurité qui s'informe en temps utile des défauts techniques des systèmes d'information utilisés, qui évalue la vulnérabilité de l'organisation en cas d'exploitation de telles failles et qui adopte des mesures adéquates pour faire face aux risques qui s'ensuivent.

4.7.2 Les mises à jour des logiciels destinées à éliminer les failles de sécurité (appelées « *patch* ») doivent être testées avant leur installation, et évaluées quant à leurs éventuels effets indésirables.

4.7.3 S'il n'existe pas encore de patch disponible pour éliminer une faille de sécurité, d'autres mesures de sécurité doivent être envisagées (p. ex. adaptation des contrôles d'accès ou limitation du trafic réseau).

4.8 Gestion des données et des systèmes sensibles (al. 1, let. c et d)

4.8.1 Les communautés doivent garantir que les institutions de santé affiliées disposent d'un règlement en vertu duquel seules peuvent être rendues accessibles dans le dossier électronique du patient les données contenues dans le dossier médical du patient qui sont pertinentes pour le traitement.

4.8.2 Les communautés doivent veiller à ce que toutes les données sensibles, tous les systèmes et tous les dispositifs sensibles liés du dossier électronique du patient soient clairement identifiés, classifiés et inventoriés.

4.8.3 L'inventaire sert à recenser et à gérer au moins les systèmes suivants :

4.8.3.1 lieux de stockage des documents ;

4.8.3.2 registre de documents ;

4.8.3.3 systèmes d'historisation ;

4.8.3.4 système de gestion des autorisations ;

4.8.3.5 système de gestion des identités et des accès (IAM) ;

4.8.3.6 index des patients ;

4.8.3.7 ensemble de données du système d'exploitation pertinent pour la protection et la sécurité des données (p. ex. historiques, sauvegardes, gestion des accès privilégiés des administrateurs de systèmes) ;

4.8.3.8 systèmes primaires avec les rôles (acteurs IHE) *Document Source* et *Document Consumer*. L'inventaire précise au moins, pour ces éléments :

4.8.3.8.1 le certificat client TLS, permettant d'activer la sécurité de la couche transport (TLS) de l'acteur IHE.

4.8.4 Chaque élément de l'inventaire doit :

4.8.4.1 être attribué à un propriétaire, qui en porte la responsabilité ;

4.8.4.2 mentionner la source originale des données ;
4.8.4.3 préciser la date de la dernière confirmation du responsable de la sécurité et de la protection des données.

4.8.5 Le responsable de la sécurité et de la protection des données doit réexaminer l'inventaire au moins une fois par an.

4.9 Prescriptions relatives à la protection et à la sécurité des données imposées aux institutions de santé affiliées ainsi qu'à leurs professionnels de la santé et applicables aux terminaux (let. e)

4.9.1 Les communautés doivent prévoir des règles de protection et de sécurité des données pour les institutions de santé et leurs professionnels de la santé qui :
4.9.1.1 garantissent que les mesures de sécurité à respecter sont signalées aux institutions de santé (voir ch. 1.1.2.1) ;
4.9.1.2 astreignent les institutions de santé à informer leurs professionnels de la santé ayant accès au dossier électronique du patient sur leurs tâches, droits et devoirs liés au traitement des données dans le dossier électronique du patient ainsi que sur les risques et les mesures destinées à garantir la protection et la sécurité des données, et à obliger ces personnes au respect des mesures requises. L'obligation d'information couvre au moins les points suivants :
4.9.1.2.1 utilisation sûre des moyens d'identification et des données d'accès;
4.9.1.2.2 principes de description des documents à rendre accessibles avec des métadonnées ;
4.9.1.2.3 mesures en vue d'une utilisation sûre des terminaux (ordinateur, smartphone, tablette, etc.) ;
4.9.1.2.4 comportements à adopter pour se protéger contre les menaces auxquelles sont exposés les professionnels de la santé, p. ex. ingénierie sociale, « phishing », usage des supports de sauvegarde externes, etc. ;
4.9.1.2.5 services d'assistance et procédure pour la déclaration des incidents de protection et de sécurité des données ;
4.9.1.2.6 responsabilités en cas d'engagement d'auxiliaire.

Sécurité des terminaux utilisés par les professionnels de la santé

4.9.2 Les communautés astreignent les institutions de santé leur étant affiliées à garantir une configuration sûre des terminaux utilisés par les professionnels de la santé pour accéder au dossier électronique du patient.

4.9.3 La configuration des terminaux doit comprendre au moins :

4.9.3.1 l'utilisation d'un logiciel régulièrement actualisé contre les programmes malveillants ;
4.9.3.2 l'utilisation de systèmes de protection du réseau (p. ex. pare-feu) ;
4.9.3.3 une gestion restrictive des droits d'administrateur du système pour les utilisateurs normaux du système final ;
4.9.3.4 une actualisation régulière du système d'exploitation et des composants logiciels critiques pour la sécurité (p. ex. environnements de temps d'exécution comme Java, .Net, etc.).

4.10 Exigences relatives à la protection et à la sécurité des données imposées au personnel (al. 1, let. f)

4.10.1 Les communautés doivent disposer d'un recueil de normes qui fixe clairement, pour chaque utilisateur ou groupe d'utilisateurs, les règles de contrôle des accès et d'octroi des autorisations, et qui les mette en œuvre dans les systèmes de traitement d'information et dans les services réseau correspondants.

4.10.2 Les communautés doivent garantir que :

4.10.2.1 les personnes qui utilisent les données ou systèmes du dossier électronique du patient sont suffisamment compétentes pour les tâches prévues, assument leurs responsabilités et se montrent attentives à la protection et à la sécurité des données ;

4.10.2.2 des exigences sont formulées et communiquées pour l'usage des données d'authentification secrètes, comme les mots de passe, p. ex. ;

4.10.2.3 les personnes susceptibles d'avoir accès aux données du dossier électronique du patient sont soumises à un devoir de confidentialité analogue au secret médical ;

4.10.2.4 les processus définis pour la gestion du personnel sont mis en œuvre et respectés.

4.10.3 Les communautés doivent :

4.10.3.1 gérer une liste, visée par le responsable de la sécurité et de la protection des données de la communauté, de toutes les personnes qui ont accès aux données des patients – indépendamment de la gestion des droits prévue dans le dossier électronique du patient (« liste des personnes-clés ») ;

4.10.3.2 effectuer dans chaque cas un contrôle de sécurité relatif aux personnes (CSP) au sens de la loi sur l'armée ;

4.10.3.3 prévoir une procédure définie et officielle, afin de prononcer des mesures disciplinaires ou des sanctions à l'encontre des collaborateurs ayant contrevenu à la protection et à la sécurité des données.

4.11 Exigences relatives à la protection et à la sécurité des données imposées aux tiers (al. 1, let. f)

4.11.1 Les communautés doivent gérer une liste, visée par le responsable de la sécurité et de la protection des données de la communauté, de tous les fournisseurs et prestataires de services (« tiers ») qui, le cas échéant, accèdent aux données du dossier électronique du patient, les traitent, les enregistrent, les transmettent ou fournissent à cet effet des composants d'infrastructure informatique.

4.11.2 Les communautés doivent garantir qu'aucun accès aux données du dossier électronique du patient n'est effectué par des intermédiaires et que les tiers qui pourraient être amenés à accéder aux données du dossier électronique du patient dans le cadre de la fourniture de prestations ou de composants d'infrastructure informatique le font uniquement pour fournir leur prestation à la communauté, à l'exclusion de toute autre fin, et en aucun cas ne traitent ou ne transfèrent des données du dossier électronique du patient.

4.11.3 Toutes les exigences pertinentes de protection et de sécurité des données doivent être fixées en bonne et due forme avec les tiers et convenues dans des contrats de fourniture.

4.11.4 Les contrats de fourniture doivent fixer sans équivoque les obligations et responsabilités quant au respect des exigences pertinentes de protection et de sécurité des données.

4.11.5 Les contrats de fourniture doivent comprendre au moins les dispositions suivantes :

4.11.5.1 obligations du fournisseur de respecter les exigences pertinentes de protection et de

sécurité des données de la communauté, en cas d'utilisation ou de mise à disposition de produits technologiques de l'information et de la communication, de personnel et/ou de services ;

4.11.5.2 exigences et procédures pour la gestion des incidents de protection et de sécurité des données ;

4.11.5.3 indication des interlocuteurs pour toute question ou en cas d'incident dans le domaine de la protection et de la sécurité des données ;

4.11.5.4 droit de réexaminer régulièrement les processus des fournisseurs et les mesures de contrôle liées au contrat ;

4.11.5.5 obligation d'imposer le respect des exigences de protection et de sécurité des données de la communauté tout au long de la chaîne d'approvisionnement, au cas où les fournisseurs mandateraient des sous-traitants ;

4.11.5.6 prescriptions et mesures de contrôle applicables aux contrats de sous-traitance ;

4.11.5.7 devoir d'informer la communauté de toute modification des relations contractuelles avec les sous-traitants impliqués.

4.12 Surveillance et contrôle des prestations de service (al. 1, let. f)

4.12.1 Les communautés doivent régulièrement surveiller et contrôler les prestations de service, les rapports et la documentation fournis par des tiers et par d'éventuels sous-traitants, de façon à garantir que :

4.12.1.1 les conditions fixées par voie contractuelle pour la protection et la sécurité des données sont respectées ;

4.12.1.2 les incidents ou problèmes de protection et de sécurité des données sont traités de manière adéquate ;

4.12.1.3 les modifications apportées aux prestations de service sont soumises à une gestion dirigée du changement.

4.13 Obligation de déclarer les incidents de sécurité (al. 2)

4.13.1 Les communautés doivent avoir défini des procédures formelles de déclaration immédiate à l'organisme de certification et à l'OFSP en cas d'incident qui, selon le système de gestion de la protection et de la sécurité des données, est pertinent pour la sécurité, ainsi qu'en exiger et en contrôler le respect.

4.14 Sécurité d'exploitation (al. 3)

4.14.1 Les communautés doivent garantir que :

4.14.1.1 les accès privilégiés à l'environnement de production, p. ex. par les administrateurs de systèmes d'exploitation, de bases de données et d'applications :

4.14.1.1.1 reposent sur une authentification à deux facteurs ;

4.14.1.1.2 sont surveillés et historisés par un administrateur indépendant ;

4.14.1.1.3 ne permettent pas d'exporter les données de patients.

4.14.1.2 les accès externes par des tiers et des sous-traitants et en particulier les accès externes privilégiés à l'environnement de production, outre ce qui précède :

4.14.1.2.1 sont interdits ou comportent une protection adéquate ;

4.14.1.2.2 sont surveillés et historisés ;

4.14.1.2.3 ne sont autorisés que temporairement, et en cas de besoin.

4.14.1.3 les activités de développement, de test et de mise en service de nouveaux systèmes sont

documentées de façon compréhensible et se déroulent selon un processus contrôlé ;

4.14.1.4 des sauvegardes complètes sont faites et qu'elles sont cryptées ;

4.14.1.5 le matériel de cryptage pour la gestion des sauvegardes est soumis au principe du double contrôle ;

4.14.1.6 les sauvegardes sont horodatées ;

4.14.1.7 les sauvegardes sont enregistrées sur des dispositifs de stockage séparés, où leur intégrité est protégée, et que les dispositifs en question sont déconnectés du réseau après la copie ;

4.14.1.8 les procédures de restauration des systèmes sont convenablement documentées et régulièrement testées ;

4.14.1.9 les journaux techniques ne contiennent aucune donnée non cryptée de patients ;

4.14.1.10 les fichiers d'historisation sont horodatés et sauvegardés de manière à protéger leur intégrité ;

4.14.1.11 les supports de données de patients sont toujours éliminés correctement, et que toutes les données sont préalablement effacées ;

4.14.1.12 les horloges des systèmes sont synchronisées avec l'heure légale en Suisse.

4.14.2 L'environnement de production de l'infrastructure informatique du dossier électronique du patient interne à la communauté doit :

4.14.2.1 être isolé des autres environnements (p. ex. environnement de développement, de recette et de test) ;

4.14.2.2 adopter de nouveaux logiciels exclusivement lors de processus au déroulement contrôlé ;

4.14.2.3 faire l'objet de contrôles réguliers portant sur ses failles de sécurité ;

4.14.2.4 corriger les failles de sécurité détectées, lors d'un processus dûment contrôlé de gestion des patchs ;

4.14.2.5 être isolé des autres systèmes de l'exploitant par une propre segmentation réseau.

4.14.3 Outre le traitement des données du dossier électronique du patient par les professionnels de la santé ainsi que par les patients, il convient d'enregistrer au moins les informations suivantes à propos des événements survenant dans le cadre de l'exploitation du système :

4.14.3.1 date, heure et détails des événements-clés (p. ex. log in et log out) ;

4.14.3.2 tentatives d'accès, réussies ou infructueuses, au système ;

4.14.3.3 tentatives d'accès, réussies ou infructueuses, aux données ou aux documents ;

4.14.3.4 modifications apportées à la configuration du système ;

4.14.3.5 utilisation de droits d'accès privilégiés ;

4.14.3.6 adresses et protocoles réseau ;

4.14.3.7 activation et désactivation des systèmes de protection et d'authentification ;

4.14.3.8 modification des autorisations système et des accès ;

4.14.3.9 création, modification ou suppression de comptes d'utilisateurs (« accounts ») ;

4.14.3.10 copie ou impression d'informations sensibles.

4.15 Achat, développement et maintenance des systèmes (al. 3)

4.15.1 Les communautés doivent veiller à la protection et à la sécurité des données tout au long du cycle de vie des systèmes du dossier électronique du patient. A cet effet, il est nécessaire de définir, d'introduire et de respecter des processus formels de documentation, de spécification, de test, de contrôle-qualité et de mise en œuvre contrôlée pour :

4.15.1.1 l'introduction ou le développement de nouveaux systèmes ;

4.15.1.2 les modifications ou développements majeurs réalisés sur les systèmes existants ;

4.15.1.3 le changement des plateformes d'exploitation.

4.15.2 Il convient de démontrer au moins que dans chaque cycle de développement :

4.15.2.1 les exigences de sécurité sont définies dès le stade de la planification, au moyen d'une

analyse structurée des exigences, avant tout mandat de développement ou toute extension des systèmes d'information en place ;

4.15.2.2 les modifications apportées aux systèmes sont soumises à une procédure formelle documentée de contrôle des modifications ;

4.15.2.3 l'accès au code source des logiciels est limité, contrôlé et historisé ;

4.15.2.4 des lignes directrices en vue d'un développement en toute sécurité sont disponibles, y compris pour les activités de développement de systèmes qui ont été externalisées, et qu'elles sont utilisées et mises en œuvre durant le cycle de développement ;

4.15.2.5 les environnements de test ne comportent aucune donnée de patients ;

4.15.2.6 l'organisation d'exploitation supervise et contrôle le développement de logiciels en cas d'externalisation.

4.16 Cryptage de la communication (al. 3)

4.16.1 Les communautés veillent à ce que la confidentialité, l'authenticité et l'intégrité soient assurées lors de la transmission de données du dossier électronique du patient, au sein de la communauté ainsi qu'entre communautés, par des mesures cryptographiques adéquates et conformes à l'état actuel de la technique.

4.17 Enregistrement crypté des données (al. 3)

4.17.1 Les données sensibles du dossier électronique du patient doivent être sauvegardées sous une forme cryptée, à l'aide de mesures cryptographiques adéquates et conformes à l'état actuel de la technique, et de manière à ce que leur intégrité soit protégée.

4.18 Gestion des clés cryptographiques (al. 3)

4.18.1 Les communautés doivent garantir que :

4.18.1.1 les procédures de production, de distribution, d'activation, d'actualisation, de révocation ou de désactivation et de suppression des clés cryptographiques sont définies, mises en œuvre et contrôlées ;

4.18.1.2 les clés cryptographiques utilisées sont protégées contre toute modification ou perte ;

4.18.1.3 les clés secrètes et privées sont protégées contre toute utilisation ou divulgation non autorisée ;

4.18.1.4 les dispositifs de production, de sauvegarde et d'archivage des clés sont physiquement protégés.

4.19 Sécurité de la communication : gestion des réseaux (al. 3)

4.19.1 Les communautés doivent garantir que :

4.19.1.1 des directives sur la sécurité du réseau sont définies, respectées et contrôlées ;

4.19.1.2 les réseaux sont gérés de façon à ce que les données du dossier électronique du patient figurant dans les applications et les systèmes soient protégées contre les accès non autorisés ;

4.19.1.3 des règles sur les compétences en matière de gestion des réseaux à l'intérieur de la communauté sont définies, respectées et contrôlées.

4.20 Sécurité de la communication : services réseau (al. 3)

4.20.1 Les communautés doivent garantir, par une conception adéquate du réseau et de ses composants ainsi que par la structure adéquate et la configuration des services de réseau, que les données du dossier électronique du patient figurant dans les applications et les systèmes sont protégées :

4.20.1.1 en définissant des structures de réseau sûres et appropriées, en les représentant sur des plans de réseau et en les mettant en œuvre, tout en maintenant séparés des groupes dédiés de services d'information, d'utilisateurs et de systèmes d'information. En particulier, les pare-feu, les routeurs, les commutateurs réseaux, etc. et les solutions technologiques de services réseau doivent être configurés de façon à ce que :

4.20.1.1.1 seuls les systèmes faisant partie d'une communauté certifiée puissent accéder aux interfaces techniques de leur infrastructure informatique interne (« services IHE ») ;

4.20.1.1.2 les systèmes accédant à un service IHE par Internet s'authentifient auprès des services IHE au moyen du protocole TLS, en utilisant un certificat électronique valable. D'où la nécessité :

4.20.1.1.2.1 pour les portails ainsi que les *Responding Gateways*, d'utiliser au moins des certificats TLS publics à validation étendue (*extended validation, EV*) ;

4.20.1.1.2.2 pour d'autres services IHE, d'utiliser au moins des certificats TLS publics à validation étendue *EV* ou des certificats TLS uniquement valables au sein de la communauté.

4.20.1.1.3 tous les services IHE accessibles à partir d'Internet authentifient le système appelant via *TLS-Client-Authentication* ;

4.20.1.1.4 les *Responding Gateways* n'autorisent l'établissement d'une liaison que si le système appelant fait partie d'une communauté certifiée ;

4.20.1.1.5 tous les services IHE internes n'étant pas accessibles à partir d'Internet n'autorisent l'établissement d'une liaison que si le système appelant fait partie de la même communauté certifiée, s'il a été enregistré dans son inventaire et si le responsable de la protection et de la sécurité des données de la communauté l'a accepté ;

4.20.1.2 en documentant les procédures utilisées à cet effet (p. ex. certificats pour les serveurs clients, filtres d'adresses IP ou MAC).

4.20.2 Les communautés doivent :

4.20.2.1 séparer, au niveau du réseau, tous les systèmes de la communauté où sont enregistrées durablement des données du dossier électronique du patient (à savoir le registre de documents, leur lieu de stockage, la gestion des autorisations et l'index des patients) de tous les autres systèmes affichant un niveau de sécurité moins élevé ;

4.20.2.2 documenter les procédures utilisées à cet effet (p. ex. segmentation du réseau à l'aide de pare-feu).

4.20.3 Les communautés doivent notamment documenter le dispositif de sécurité implémenté pour assurer la protection de leur portail d'accès. La documentation comprend au moins :

4.20.3.1 la topologie du réseau et le justificatif concernant la « zone démilitarisée » (DMZ) ;

4.20.3.2 les versions et le niveau des logiciels utilisés pour le pare-feu applicatif Web (WAF) et le serveur Web ainsi que des composants logiciels employés par des tiers pertinents pour la sécurité ;

4.20.3.3 les mesures prévues pour la détection et le traitement des attaques et des failles de sécurité.

4.21 Expiration des sessions dans le réseau (« *session timeout* ») (al. 3)

4.21.1 Les sessions réseau inactives prennent fin après une période d'inactivité définie (20 minutes pour les patients, deux heures pour les professionnels de la santé).

4.21.2 L'authentification aux portails d'accès et sur les terminaux doit être répétée avant tout nouvel accès, faute d'interaction de l'utilisateur avec le dossier électronique du patient pendant 20 minutes dans le cas des patients, ou pendant deux heures pour les professionnels de la santé.

4.22 Système intermédiaire (al. 3)

4.22.1 Les éléments de l'infrastructure informatique interne à la communauté servant à transmettre les documents du dossier électronique du patient (notamment les points d'accès) ne peuvent pas les sauvegarder durablement.

4.23 Accessibilité (al. 3)

4.23.1 Les communautés doivent garantir que :

4.23.1.1 les services techniques destinés à l'utilisation du dossier électronique du patient sont à l'abri des interruptions, afin que de graves perturbations n'aient que des effets limités et prévus par contrat sur les systèmes de traitement de l'information et que la reprise en temps voulu de tous les services puisse être garantie ;

4.23.1.2 les services techniques exposés de l'infrastructure informatique affichent une disponibilité convenue contractuellement d'au moins 98 % sur la durée, et restent disponibles en cas de forte sollicitation ;

4.23.1.3 toutes les interfaces du dossier électronique du patient accessibles par Internet sont protégées contre les attaques DoS (par déni de service, *denial of service*) ;

4.23.1.4 des processus éprouvés leur permettent de réduire à un niveau acceptable, grâce à une combinaison de mesures de prévention et de remise en état, le temps de restauration après une perte d'information due, p. ex., à une catastrophe naturelle, à un accident, à une défaillance d'applications, de systèmes ou d'appareil, ou à des dommages intentionnels.

4.24 Dispositifs de stockage sous juridiction suisse (al. 4)

4.24.1 La communauté doit garantir que l'exploitation interne à la communauté d'un dispositif de stockage du dossier électronique du patient (lieux de stockage des documents, registre de documents et index des patients notamment) incombe à des personnes morales qui :

4.24.1.1 sont soumises au droit suisse ;

4.24.1.2 agissent exclusivement sous le régime du droit suisse pour accomplir leurs prestations ;

4.24.1.3 sont détenues en majorité en propriété suisse ;

4.24.1.4 fournissent toutes leurs prestations sur le territoire suisse.

5 Service d’assistance pour les professionnels de la santé (art. 12 ODEP)

5.1.1 Les communautés doivent proposer aux professionnels de la santé un service d’assistance (« *service desk* ») afin de les aider dans l’utilisation du dossier électronique du patient.

5.1.2 Les communautés doivent garantir au moins que :

5.1.2.1 les collaborateurs du « service desk » connaissent leurs tâches, leurs droits et devoirs, ainsi que les risques et les mesures propres à assurer la protection et la sécurité des données ;

5.1.2.2 les collaborateurs ayant accès aux données du dossier électronique du patient sont soigneusement sélectionnés et soumis à un devoir de confidentialité analogue au secret médical ;

5.1.2.3 le consentement des collaborateurs à respecter les directives spécifiques de la communauté est documenté ;

5.1.2.4 l’accès à distance aux terminaux des professionnels de la santé pour des activités d’assistance n’est possible que si les intéressés en ont connaissance et ont donné leur consentement, et que l’accès est documenté automatiquement.

Exigences supplémentaires applicables aux communautés de référence

6 Information du patient (art. 14 ODEP)

6.1 L’information du patient selon l’art. 14 ODEP comprend au moins les points suivants :

6.1.1 Informations sur le but du dossier électronique du patient.

6.1.2 Informations sur les principes essentiels du traitement des données, dont au moins :

6.1.2.1 la perpétuation des documents dans les systèmes primaires et les lieux de stockage ;

6.1.2.2 le droit de révoquer son consentement présumé à la mise à disposition de documents en cas de traitement ainsi que d’obtenir la destruction de certains documents ;

6.1.2.3 les possibilités et fonctions du portail d’accès destiné aux patients ;

6.1.2.4 les possibilité de consulter les données historisées ;

6.1.2.5 les possibilité de désigner un représentant ;

6.1.2.6 les possibilité d’habiliter des professionnels de la santé à transmettre des droits d’accès, conformément à l’art. 3, let. h, ODEP.

6.1.3 Informations sur les conséquences du consentement et sur la possibilité de le révoquer, dont au moins :

6.1.3.1 le consentement libre ;

6.1.3.2 la possibilité de disposer d’un seul dossier de patient à la fois ;

6.1.3.3 les modalités de l’attribution et de l’utilisation du numéro d’identification du patient ;

6.1.3.4 la possibilité de changer de communauté de référence, avec les conséquences qui s’ensuivent pour la perpétuation des données, ainsi que pour les éventuels représentants et professionnels de la santé habilités ;

6.1.3.5 la possibilité de révoquer son consentement, sans aucune exigence de forme ou de justification de motif ;

6.1.3.6 la possibilité, après une révocation, d'ouvrir à nouveau un dossier électronique du patient auquel sera assigné un nouveau numéro d'identification du patient ;

6.1.4 Informations sur les possibilités d'octroi des droits d'accès selon les art. 1 à 3 ODEP, dont au moins :

6.1.4.1 la configuration des droits d'accès des professionnels de la santé et du niveau de confidentialité des documents suite à l'ouverture du dossier électronique du patient ;

6.1.4.2 les possibilités d'accorder des droits d'accès à des professionnels de la santé et à des groupes de professionnels de la santé, de les modifier et de les retier ;

6.1.4.3 les possibilité d'accès prévue pour les auxiliaires enregistrés par les professionnels de la santé, avec le niveau d'accès accordé au professionnel de la santé responsable ;

6.1.4.4 les possibilité d'accès prévue pour les professionnels de la santé dans des situations d'urgence médicale, et possibilité de limiter, étendre ou exclure un tel accès ;

6.1.4.5 les possibilité d'exclure de tout accès certains professionnels de la santé (liste d'exclusion) ;

6.1.4.6 les possibilité des collaborateurs du « service desk » d'accéder à distance aux terminaux du patient, moyennant son consentement y relatif.

6.1.5 Informations sur les mesures recommandées en matière de protection et de sécurité des données, dont au moins :

6.1.5.1 éventuels risques résiduels et mesures prévues en matière de protection et de sécurité des données ;

6.1.5.2 authentification sécurisée et usage des moyens d'identification et des données d'accès ;

6.1.5.3 principes de description des documents à mettre à disposition avec les métadonnées ;

6.1.5.4 mesures visant à une utilisation sûre des terminaux (ordinateur, smartphone, tablette, etc.) ;

6.1.5.5 recommandations de comportement à adopter pour protéger les patients contre les risques auxquels ils sont exposés, p. ex. l'ingénierie sociale, le « phishing », etc.

7 Consentement (art. 15 ODEP)

7.1 Les procédures de constitution du dossier électronique du patient doivent être définies, documentées, mises en œuvre et respectées.

7.1.1 La procédure d'ouverture d'un dossier électronique du patient doit garantir que le consentement du patient est recueilli avec sa signature.

8 Gestion (art. 16 ODEP)

8.1 Entrée et sortie de patients (al. 1, let. a)

8.1.1 Les processus de gestion des patients doivent être définis, documentés, mis en œuvre et respectés. Ils doivent garantir en particulier que :

8.1.1.1 les processus visant à garantir le respect des prescriptions énoncées aux let. b à e sont définis, documentés, mis en œuvre et respectés.

8.2 Identification des patients (al. 1, let. b)

8.2.1 Les processus d'identification des patients doivent être définis, documentés, mis en œuvre et respectés.

8.2.2 Ils doivent garantir que :

8.2.2.1 l'identification du patient (let. b)

8.2.2.1.1 se base sur le moyen d'identification d'un éditeur certifié selon l'art. 30 ODEP, ou

8.2.2.1.2 satisfait aux exigences de l'art. 23, al. 1, ODEP ;

8.2.2.2 un dossier électronique du patient est ouvert uniquement lorsqu'il est préalablement établi que la personne concernée n'en possède pas déjà un ;

8.2.2.3 le patient figure dans l'index des patients de la communauté de référence ;

8.2.2.4 le moyen d'identification du patient est lié de manière univoque à son dossier électronique du patient (let. c) ;

8.2.2.5 un numéro d'identification du patient est demandé conformément aux art. 5 et 6 ODEP et qu'il est correctement attribué au dossier électronique du patient à constituer (let. d) ;

8.2.2.6 les données démographiques de la banque de données d'identification de la Centrale de compensation (CdC) sont reprises dans l'index des patients de la communauté de référence (let. d).

8.3 Identification et authentification (al. 1, let. c)

8.3.1 L'accès des patients au dossier électronique du patient ne peut se faire qu'à l'aide de moyens d'identification valables, émis par un éditeur certifié selon l'art. 30 ODEP.

8.3.2 Les communautés doivent garantir qu'un lien fiable est établi entre l'identificateur univoque figurant dans le moyen d'identification des patients et de leurs éventuels représentants et l'identité de chacune de ces personnes enregistrée dans la communauté.

8.3.3 Les communautés doivent garantir que les portails d'accès :

8.3.3.1 supportent une procédure d'authentification forte conforme à l'état actuel de la technique, qui prévoit au moins deux facteurs d'authentification, comme condition préalable au traitement des données du dossier électronique du patient ;

8.3.3.2 mettent à disposition un terminal fiable pour communiquer de manière sûre avec le fournisseur de services d'identité (éditeur du moyen d'identification) conformément au ch. 3.2 (*P.TrustedCommunityEndpoint*) du profil de protection visé à l'art. 8 ODEP-DFI.

8.4 Changement de communauté de référence (let. e)

8.4.1 Les processus de changement de communauté de référence par le patient doivent être définis, documentés, mises en œuvre et respectés.

8.4.2 Le processus de changement de communauté de référence doit garantir que :
8.4.2.1 la configuration individuelle de gestion des autorisations peut être transférée à la nouvelle communauté de référence et reprise par elle. A cet effet, il faut respecter les prescriptions relatives au format technique du profil d'intégration national CH:PPQ, selon l'annexe 5 ODEP;
8.4.2.2 l'habilitation dont dispose un professionnel de la santé en vertu de l'art. 3, let. h ODEP est supprimée ;
8.4.2.3 les possibilités d'accès d'éventuels représentants d'un patient sont supprimées.

8.5 Respect des décisions d'accès visant le traitement de la configuration des autorisations (al. 2) : droits d'accès (art. 2, al. 1, OPED) et options du patient (art. 3 OPED)

8.5.1 Les communautés doivent garantir que le traitement de la configuration de la gestion des autorisations est effectué uniquement en conformité avec les décisions d'accès accordés.

8.6 Gestion des autorisations (al. 2) : droits d'accès (art. 2, al. 1 à 4, ODEP)

8.6.1 Les patients doivent avoir la possibilité d'accorder et d'adapter les droits d'accès aux professionnels de la santé aux groupes de professionnels de la santé. Les prescriptions de l'art. 2, al. 1 à 4, OPED doivent être respectées dans ce contexte.

8.6.2 Les prescriptions à respecter concernent notamment :
8.6.2.1 la possibilité d'accorder des droits d'accès à certains professionnels de la santé ou groupes de professionnels de la santé conformément à l'art. 1, al. 1, ODEP ;
8.6.2.2 la validité des droits d'accès accordés jusqu'à leur retrait par le patient ;
8.6.2.3 la mise en œuvre correcte des modifications des droits d'accès au sens de l'art. 2, al. 4, ODEP, liées aux entrées et sorties de professionnels de la santé dans un groupe, y c. la prise en compte des éventuels droits d'accès leur étant accordés à titre individuel.

8.7 Options du patient (art. 3 ODEP)

8.7.1 Les communautés de référence doivent garantir que :
8.7.1.1 les patients peuvent faire usage des options que leur donne l'art. 3 ODEP ;
8.7.1.2 les exigences énoncées à l'art. 3 sont mises en œuvre correctement.

8.7.2 Les exigences à respecter concernent la mise en œuvre correcte des options suivantes :
8.7.2.1 la possibilité d'accorder des droits d'accès limités dans le temps en vertu de l'art. 3, let. a, ODEP ;
8.7.2.2 la limitation, l'extension et l'exclusion des accès en cas d'urgence médicale ;
8.7.2.3 le choix du niveau de confidentialité attribué aux nouvelles données saisies dans le dossier électronique du patient ;
8.7.2.4 l'exclusion de certains professionnels de la santé de l'accès au dossier électronique du patient ;
8.7.2.5 la désactivation de l'information prévue à l'art. 8, let. f, ODEP ;
8.7.2.6 le choix que les professionnels de la santé qui intègrent un groupe n'obtiennent pas automatiquement les droits d'accès accordés à ce groupe ;

8.7.2.7 la désignation d’un représentant ;
8.7.2.8 l’habilitation de certains professionnels de la santé à transmettre leurs droits d’accès, conformément à l’art. 3, let. h, ODEP ;
8.7.2.9 l’évaluation correcte des règles en vigueur concernant les autorisations.

8.8 Représentation (art. 16, al. 1, let. c et al. 3, ODEP)

8.8.1 Les communautés de référence doivent offrir au patient la possibilité de désigner un représentant.

8.8.2 Le représentant doit accéder par son propre moyen d’identification, émis par un éditeur certifié selon l’art. 30, au dossier électronique du patient du patient qu’il représente.

8.8.3 La communauté de référence doit garantir que :
8.8.3.1 l’identification du représentant
8.8.3.1.1 repose sur le moyen d’identification d’un éditeur certifié selon l’art. 30, ou
8.8.3.1.2 correspond aux exigences de l’art. 23, al. 1, ODEP ;
8.8.3.2 les conditions juridiques liées à l’exercice du droit de représentation sont remplies ;
8.8.3.3 le représentant est informé, selon l’art. 14, ODEP, des principes essentiels du traitement des données, ainsi que des possibilités, des droits et obligations liés à l’utilisation du dossier électronique du patient ;
8.8.3.4 le moyen d’identification servant au représentant du patient, émis par un éditeur certifié selon l’art. 30, est relié de manière univoque et correcte au dossier électronique du patient du patient qu’il représente ;
8.8.3.5 l’accès du représentant au dossier électronique du patient se limite à la durée de sa fonction en tant que représentant.

9 Portail d’accès pour les patients (art. 17 ODEP)

9.1 Conformité aux dispositions légales

9.1.1 Le portail d’accès pour les patients doit satisfaire aux exigences juridiques en la matière.

9.1.2 Le portail d’accès doit permettre aux patients et aux professionnels de la santé habilités au sens de l’art. 3, let. h, ODEP de procéder à la gestion des autorisations, conformément aux prescriptions énoncées aux art. 1 à 3 ODEP.

9.1.3 Le portail d’accès doit notamment remplir les conditions-cadres suivantes quant à l’utilisation des données du patient :
9.1.3.1 les données mises à disposition par le patient dans des domaines ne relevant pas du dossier électronique du patient ne peuvent y être enregistrées que si le patient y a consenti ;
9.1.3.2 les données mises à disposition par le patient lui-même doivent toujours pouvoir être enregistrées directement dans le dossier électronique du patient, soit sans recours à une lieu de stockage intermédiaire ;
9.1.3.3 les données du dossier électronique du patient ne peuvent être transférées automatiquement et sans l’accord explicite du patient dans des domaines fonctionnels situés « en dehors » du dossier électronique du patient.

9.2 Présentation

9.2.1 La présentation sur l'interface utilisateur du portail d'accès doit être correcte et exhaustive, et montrer clairement :

9.2.1.1 si c'est un professionnel de la santé ou le patient lui-même qui a mis à disposition le document ;

9.2.1.2 les documents fournis par le patient lui-même ;

9.2.1.3 les documents annulés ;

9.2.1.4 les versions d'un document éventuellement également disponibles ;

9.2.1.5 les droits d'accès dont dispose chaque professionnel de la santé ;

9.2.1.6 le niveau de confidentialité de chaque document ;

9.2.1.7 utiliser pour la présentation des métadonnées prescrites selon l'annexe 3 ODEP-DFI sur l'interface utilisateurs du portail d'accès les termes et expressions préconisés pour la langue choisie (« defined terms »).

9.3 Accessibilité

9.3.1 Le portail d'accès doit :

9.3.1.1 être conçu pour être pleinement accessible aux patients agés ou ayant un handicap ;

9.3.1.2 remplir les conditions de conformité des directives pour l'accessibilité aux contenus Web (WCAG) 2.0 et atteindre le niveau de conformité AA.

9.4 Formats de fichiers : mise à disposition

9.4.1 Le portail d'accès doit :

9.4.1.1 permettre de mettre à disposition des formats de fichiers autorisés en vertu de l'annexe 3 ODEP-DFI ;

9.4.1.2 convertir les fichiers différents dans un format autorisé, avant leur enregistrement dans un lieu de stockage.

9.5 Formats de fichiers : requête

9.5.1 Le portail d'accès doit :

9.5.1.1 permettre une requête des formats de fichiers autorisés en vertu de l'annexe 3 ODEP-DFI ;

9.5.1.2 permettre une requête des fichiers à enregistrer dans le système primaire (« download ») ;

9.5.1.3 prévoir le téléchargement non seulement un par un, mais aussi en masse (« bulk download ») des documents sélectionnés ;

9.5.1.4 présenter les données structurées sous une forme directement lisible par l'être humain, correcte et complète ;

9.5.1.5 permettre de télécharger les données structurées aussi bien dans leur format d'origine que sous une forme directement lisible par l'être humain.

9.5.2 La requête de documents pour affichage ou enregistrement doit respecter les limites maximales définies par unité de temps (« rate limits »), qui déclenchent, en cas de dépassement, des mesures adéquates de blocage ou de sécurité renforcée.

9.6 Données historisées (let. c)

9.6.1 Les patients doivent avoir la possibilité de consulter, sous une forme lisible pour eux, les données historisées de toutes les communautés ou communautés de référence concernant leur dossier électronique du patient.

10 Disponibilité des données enregistrées par les patients (art. 18 ODEP)

10.1 Stockage des documents de patients

10.1.1 Les communautés de référence doivent mettre à disposition des lieux de stockage internes spéciaux pour les documents enregistrés par les patients eux-mêmes.

10.1.2 Les documents ne doivent être soumis à aucun délai d'effacement.

10.1.3 L'espace de stockage prévu à cet effet comporte au moins deux gigaoctets (Go).

10.1.4 Les communautés de référence doivent gérer les capacités de l'espace de stockage destiné aux documents enregistrés par les patients.

10.2 Archivage hors ligne des documents et des métadonnées

10.2.1 Les données concernant les patients et les métadonnées afférentes doivent pouvoir être mises à la disposition des patients dans un format électronique usuel interopérable.

10.2.2 Il faut prévoir des procédures permettant de déterminer si les données ont été modifiées après leur mise à disposition.

10.2.3 Les communautés de référence doivent garantir que les données qui sont mises à disposition une nouvelle fois dans le dossier électronique du patient n'ont pas été modifiées entre-temps.

11 Service d’assistance pour les patients (art. 19 ODEP)

11.1.1 Les communautés de référence doivent désigner un service d’assistance (« *service desk* ») destiné aux patients afin de les aider dans l’utilisation du dossier électronique du patient.

11.1.2 Les communautés de référence doivent garantir au moins que :

11.1.2.1 les collaborateurs du « service desk » connaissent leurs tâches, leurs droits et obligations ainsi que les risques et les mesures propres à assurer la protection et la sécurité des données ;

11.1.2.2 les collaborateurs ayant accès aux données du dossier électronique du patient sont soigneusement sélectionnés et soumis à des obligations analogues au secret médical ;

11.1.2.3 le consentement des collaborateurs du « service desk » à respecter les directives spécifiques de la communauté est documenté ;

11.1.2.4 l’accès à distance aux terminaux des patients pour des activités d’assistance n’est possible que si les intéressés en ont connaissance et ont donné leur consentement, et que l’accès est documenté automatiquement.

12 Suppression du dossier électronique du patient (art. 20 ODEP)

12.1.1 Les communautés de référence doivent définir, documenter, mettre en œuvre et respecter des procédures régissant la suppression du dossier électronique du patient en cas de révocation, d’inutilisation ou de décès du patient.

12.2 Conditions de la suppression du dossier électronique du patient (al. 1)

12.2.1 La procédure de suppression du dossier électronique du patient doit être déclenchée lorsque :

12.2.1.1 le patient révoque son consentement à la tenue du dossier électronique du patient ;

12.2.1.2 personne n’a accédé au dossier électronique du patient durant dix ans ; ou

12.2.1.3 le patient est décédé.

12.3 Suppression du dossier électronique du patient (al. 2)

12.3.1 La procédure de suppression du dossier électronique du patient doit garantir que :

12.3.1.1 le dossier électronique du patient à supprimer est correctement identifié ;

12.3.1.2 tous les droits d’accès au dossier correspondant sont aussitôt retirés ;

12.3.1.3 toutes les données du dossier correspondant sont détruites en application de l’art. 9, al. 1, let. b, ODEP ;

12.3.1.4 toutes les communautés et communautés de référence sont informées dans un délai approprié de la suppression du dossier électronique du patient ;

12.3.1.5 la CdC est informée de la suppression du dossier électronique du patient dans un délai approprié.

12.4 Révocation du consentement à la tenue du dossier électronique du patient (al. 2, let. a)

12.4.1 En cas de révocation du consentement du patient à la tenue de son dossier électronique du patient, la procédure de suppression du dossier électronique du patient doit garantir, outre les points énoncés sous le ch. 12.3, que :

12.4.1.1 la révocation est documentée de façon juridiquement valable ;

12.4.1.2 la déclaration de révocation est conservée pendant dix ans.

12.4.2 Il doit être garanti que :

12.4.2.1 l'identification de la personne exerçant son droit de révocation

12.4.2.1.1 repose sur le moyen d'identification émis par un éditeur certifié selon l'art. 30, ou

12.4.2.1.2 correspond aux exigences de l'art. 23, al. 1, ODEP ;

12.4.2.2 la personne exerçant son droit de révocation a été informée des conséquences qui en découlent ;

12.5 Fermeture en cas d'inutilisation (al. 2, let. b)

12.5.1 En cas d'inutilisation, la procédure de suppression du dossier électronique du patient au sens de l'art. 20, al. 1, let. b, doit garantir, outre les points énoncés sous le ch. 12.3, que :

12.5.1.1 le patient est informé de la suppression de son dossier trois mois à l'avance.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI

Office fédéral de la santé publique OFSP
Unité de direction Politique de la santé

Métadonnées

Version: 1.0 22.03.2016
Entrée en vigueur: ...

Métadonnées à utiliser dans le cadre du dossier électronique du patient

1 Liste des attributs

1. Rôle de l'auteur
2. Discipline médicale de l'auteur
3. Statut de disponibilité du document
4. Classification du document
5. Niveau de confidentialité
6. Format du Document
7. Type de l'institution de santé
8. Langue du document
9. MIME Type du document
10. Discipline médicale des données saisies dans le document
11. Sexe du patient
12. Type du document

Un OID (Object Identifier) est attribué à la plupart des attributs et aux listes y relatives comprenant les valeurs autorisées, qui doit également être utilisé. Les OID sont des identifiants techniques qui doivent être employés par les systèmes techniques pour l'attribution univoque des attributs et des valeurs.

Remarque : Les terminologies autorisées en français et en italien seront définies ultérieurement avec le concours des milieux intéressés.

1.1 Rôle de l'auteur

OID national: 2.16.756.5.30.1.127.3.10.1.1.3

Code national	Désignation anglaise	Désignation allemande	Désignation française	Désignation italienne
40001	Pharmacist	Apothekerin/Apotheker		
40002	Physician	Ärztin/Arzt		
40003	Chiropractor	Chiropraktorin/Chiropraktiker		
40004	Dietitian	Ernährungsberaterin/Ernährungsberater		
40005	Midwife	Hebamme		
40006	Complementary therapist	Komplementärmedizinerin/ Komplementärmediziner /		
40007	Patient	Patientin/Patient		
40008	Professional nurse	Pflegefachperson		
40009	Psychologist	Psychologin/Psychologe		
40010	Social Worker	Sozialdienst-Mitarbeiterin/Mitarbeiter		
40011	Other Therapist	Therapeutin/Therapeut		
40012	Dentist	Zahnärztin/Zahnarzt		
40900	Unknown	Unbekannt		
40999	Other	Andere		

1.2 Discipline médicale de l'auteur

OID national: : 2.16.756.5.30.1.127.3.10.1.1.4

Code national	Désignation anglaise	Désignation allemande	Désignation française	Désignation italienne
50001	Internal medicine specialist	Fachärztin/Facharzt für Allgemeine Innere Medizin		
50002	Anesthesiologist	Fachärztin/Facharzt für Anästhesiologie		
50003	Occupational therapist	Fachärztin/Facharzt für Arbeitsmedizin		
50004	Surgeon	Fachärztin/Facharzt für Chirurgie		
50005	Dermatologist	Fachärztin/Facharzt für Dermatologie und Venerologie		
50006	Endocrinologist	Fachärztin/Facharzt für Endokrinologie / Diabetologie		
50007	Gastroenterologist	Fachärztin/Facharzt für Gastroenterologie		
50008	Obstetrician and gynecologist	Fachärztin/Facharzt für Gynäkologie und Geburtshilfe		
50009	Hematologist	Fachärztin/Facharzt für Hämatologie		
50010	Cardiovascular surgeon	Fachärztin/Facharzt für Herz- und thorakale Gefässchirurgie		
50011	Infectious disease specialist	Fachärztin/Facharzt für Infektiologie		
50012	Cardiologist	Fachärztin/Facharzt für Kardiologie		
50013	Pediatrician	Fachärztin/Facharzt für Kinder- und Jugendmedizin		
50014	Child and adolescent psychiatrist	Fachärztin/Facharzt für Kinder- und Jugendpsychiatrie und -psychotherapie		
50015	Pediatric surgeon	Fachärztin/Facharzt für Kinderchirurgie		
50016	Clinical pharmacologist	Fachärztin/Facharzt für Klinische Pharmakologie und Toxikologie		
50017	Oral and maxillofacial surgeon	Fachärztin/Facharzt für Mund-, Kiefer- und Gesichtschirurgie		
50018	Nephrologist	Fachärztin/Facharzt für Nephrologie		
50019	Neurosurgeon	Fachärztin/Facharzt für Neurochirurgie		
50020	Neurologist	Fachärztin/Facharzt für Neurologie		
50021	Nuclear medicine specialist	Fachärztin/Facharzt für Nuklearmedizin		
50022	Ophthalmologist	Fachärztin/Facharzt für Ophthalmologie		
50023	Orthopedic surgeon	Fachärztin/Facharzt für Orthopädische Chirurgie und Traumatologie des Bewegungsapparates		
50024	Otorhinolaryngologist	Fachärztin/Facharzt für Oto-Rhino-Laryngologie		
50025	Medical pathologist	Fachärztin/Facharzt für Pathologie		
50026	Rehabilitation physician	Fachärztin/Facharzt für Physikalische Medizin und Rehabiliation		
50027	Plastic surgeon	Fachärztin/Facharzt für Plastische, Rekonstruktive und Ästhetische Chirurgie		
50028	Pulmonologist	Fachärztin/Facharzt für Pneumologie		
50029	Preventive medicine specialist	Fachärztin/Facharzt für Prävention und Gesundheitswesen		
50030	Psychiatrist	Fachärztin/Facharzt für Psychiatrie und Psychotherapie		

50031	Radiologist	Fachärztin/Facharzt für Radiologie		
50032	Radio-Oncologist	Fachärztin/Facharzt für Radio-Onkologie / Strahlentherapie		
50033	Rheumatologist	Fachärztin/Facharzt für Rheumatologie		
50034	Tropical medicine specialist	Fachärztin/Facharzt für Tropen- und Reisemedizin		
50035	Urologist	Fachärztin/Facharzt für Urologie		
50036	Angiologist	Fachärztin/Facharzt für Angiologie		
50037	Intensive care specialist	Fachärztin/Facharzt für Intensivmedizin		
50038	Geneticist	Fachärztin/Facharzt für Medizinische Genetik		
50039	Medical oncologist	Fachärztin/Facharzt für Medizinische Onkologie		
50040	Pharmacologist	Fachärztin/Facharzt für Pharmazeutische Medizin		
50041	Forensic medicine specialist	Fachärztin/Facharzt für Rechtsmedizin		
50042	Hand surgeon	Fachärztin/Facharzt für Handchirurgie		
50043	Neuropathologist	Fachärztin/Facharzt für Neuropathologie		
50044	Dentist	Zahnärztin/Zahnarzt		
50045	Retail pharmacist	Apothekerin/Apotheker in Offizinpharmazie		
50046	Hospital pharmacist	Apothekerin/Apotheker in Spitalpharmazie		
50047	Dietician/public health nutritionist	Ernährungsberaterin/Ernährungsberater		
50048	Paramedic	Rettungssanitäterin/Rettungssanitäter		
50049	Chiropractor	Chiropraktorin/Chiropraktiker		
50050	Psychotherapist	Psychotherapeutin/Psychotherapeut		
50051	Clinical psychologist	Klinischer Psychologe/Klinische Psychologin		
50052	Health psychologist	Gesundheitspsychologin/Gesundheitspsychologe		
50053	Music therapist	Musiktherapeutin/Musiktherapeut		
50054	Midwife	Hebamme		
50055	Physiotherapist	Physiotherapeutin/Physiotherapeut		
50056	Laboratory technician - analysist	Biomedizinische Analytikerin/Biomedizinischer Analytiker		
50057	Medical X-ray technician	Radiologietechnologin/Radiologietechnologe		
50058	Diabetes dietitian	Diätologin/Diätologe		
50059	Occupational therapist	Ergotherapeutin/Ergotherapeut		
50060	Speech/language therapist	Logopädin/Logopäde		
50061	Orthoptist	Orthoptistin/Orthoptist		
50062	Professional nurse	diplomierte Pflegefachfrau/diplomierter Pflegefachmann		
50063	Professional nurse (Bachelor degree)	diplomierte Pflegefachfrau/diplomierter Pflegefachmann mit akademischem pflegefachlichem Abschluss (Bachelor)		
50064	Professional nurse (Master degree)	diplomierte Pflegefachfrau/diplomierter Pflegefachmann mit akademischem pflegefachlichem Abschluss (Master)		
50065	Specialized nurse	diplomierte Pflegefachfrau/diplomierter Pflegefachmann mit Zusatz- oder		

		Spezialfunktion, z.B. IPS, Anästhesie (NDS)		
50066	Specialized nurse (additional qualification)	diplomierte Pflegefachfrau/diplomierter Pflegefachmann mit fachvertiefendem NDK und weiteren Zusatzausbildungen wie Diabetesberaterin, Stillberaterin etc.		
50067	Nursing assistant	Pflegefachfrau/Pflegefachmann mit Attestabschluss		
50068	Health specialist (swiss federal certificate of competence)	Fachfrau/Fachmann Gesundheit, FaGe mit eidg. Fähigkeitszeugnis		
50069	Masseur	Heilmasseurin/Heilmasseur		
50070	Perfusionist	Kardiotechnikerin/Kardiotechniker		
50071	Health advisor	Gesundheits- und Sozialberaterin/-Berater		
50072	Audiologist	Hörgeräteakustiker/in		
50073	Clinical immunologist	Fachärztin/Facharzt für Allergologie und Immunologie		
50074	Allergist	Fachärztin/Facharzt für Allergologie		
50075	Pharmaceutical assistant	Pharma-Assistentin / Pharma-Assistent		
50900	Unknown	Unbekannt		
50999	Other	andere gesundheitsbezogene Fachrichtung		

1.3 Statut de disponibilité du document

Aucun OID nécessaire

Code national	Désignation anglaise	Désignation allemande	Désignation française	Désignation italienne
urn:oasis:names:tc:ebxml-regrep:StatusType:Approved	Approved	genehmigt		
urn:oasis:names:tc:ebxml-regrep:StatusType:Deprecated	Deprecated	abgelehnt		

1.4 Classification du document

OID national: : 2.16.756.5.30.1.127.3.10.1.3

Code national	Désignation anglaise	Désignation allemande	Désignation française	Désignation italienne
70001	Notes on Consultations	Konsultationseinträge/-Notizen		
70002	Progress Notes	Verlaufseinträge/-Notizen		
70003	Notes on Procedures	Interventionseinträge/-Notizen		
70004	Tests/Procedure Requests	Untersuchungs-/ Prozedur-Anforderungen		
70005	Clinical Care Referrals	Zuweisungen/Überweisungen		
70006	Episode Summary Reports	Zusammenfassende Berichte		
70007	Progress Reports	Verlaufs-Berichte		
70008	Diagnostic Test Results	Diagnostische Untersuchungsbefunde		
70009	Notifications	Meldungen		

70010	Historic Overviews	Zusammenfassungen der Krankengeschichte		
70011	Present State Summaries	Zusammenfassungen aktueller Zustand		
70012	Care Plans	Behandlungspläne, Behandlungsschemata		
70013	Alerts	Warnungen /Risiken		
70020	Scanned Documents	Gescannte Dokumente		
70021	Data from Patient	Eigene Daten des Patienten		
70999	Other Composition	anderweitige Dokumente		

1.5 Niveau de confidentialité

OID national: : 2.16.756.5.30.1.127.3.10.1.5

Code national	Désignation anglaise	Désignation allemande	Désignation française	Désignation italienne
30002	Useful medical data	nützliche Daten		
30003	Medical data	medizinische Daten		
30004	Sensitive data	sensible Daten		
30005	Secret data	geheime Daten		

1.6 Format du Document

Aucun OID nécessaire

Code national	Désignation anglaise	Désignation allemande	Désignation française	Désignation italienne
urn:che:epd:EPD_Basic_Document	EPD basic document	EPD Dokument		
urn:che:epd:2.16.756.5.30.1.1.1.1.3.5	eVaccination record	eImpfdossier		
urn:ihe:rad:1.2.840.10008.5.1.4.1.1.88.59	IHE KOS document	KOS Dokument		

1.7 Type de l'institution de santé

OID national: : 2.16.756.5.30.1.127.3.10.1.11

Code national	Désignation anglaise	Désignation allemande	Désignation française	Désignation italienne
20001	Diagnostic institution	Institut für medizinische Diagnostik		
20002	Accident and Emergency department	Notfall- / Rettungsdienste		
20003	Health Authority	Gesundheitsbehörde		
20004	Private home-based care	Organisation für Pflege zu Hause		

20005	Hospital	stationäre Einrichtung / Spital		
20006	Military health services	Armeeärztliche Dienste		
20007	Prison health services	Gesundheitseinrichtung in der Haftanstalt		
20008	Nursing home	Sozio-Medizinische Institution		
20009	Pharmacy	Apotheke		
20010	Ambulatory care site	Ambulante Einrichtung, inkl. Ambulatorium		
20011	Free-standing rehabilitation clinic	Organisation für stationäre Rehabilitation		
20012	Residential institution	zu Hause		
20900	Unknown	Unbekannt		
20999	Other	Andere Gesundheits-Organisation		

1.8 Langue du document

OID pour IETF RFC 3066: 1.3.6.1.2.1.101.1.1.3.1.1

Code national	Désignation anglaise	Désignation allemande	Désignation française	Désignation italienne
de-CH	German	Deutsch		
fr-CH	French	Französisch		
it-CH	Italian	Italienisch		
rm	Rhaeto-Romanic	Rätoromanisch		
en-US	English	Englisch		

1.9 MIME Type du document

OID pour HL7 MIME MediaType: 2.16.840.1.113883.6.10

Code national	Désignation anglaise	Désignation allemande	Désignation française	Désignation italienne
multipart/x-hl7-cda-level1	CDA Level 1 Multipart	CDA Level 1 Multipart		
text/xml	XML-Text	XML-Text		
application/pdf	PDF	PDF		
application/dicom	DICOM	DICOM		
audio/mpeg	MPEG audio layer 3	MPEG audio layer 3		
video/mpeg	MPEG Video	MPEG Video		
image/tiff	TIFF Image	TIFF Image		
image/jpeg	JPEG Image	JPEG Image		
text/plain	Plain Text	Plain Text		
multipart/x-hl7-cda-level1	CDA Level 1 Multipart	CDA Level 1 Multipart		
text/xml	XML-Text	XML-Text		
application/pdf	PDF	PDF		
application/dicom	DICOM	DICOM		
audio/mpeg	MPEG audio layer 3	MPEG audio layer 3		

1.10 Discipline médicale des données saisies dans le document

OID national: : 2.16.756.5.30.1.127.3.10.1.18

Code national	Désignation anglaise	Désignation allemande	Désignation française	Désignation italienne
10001	Allergology	Allergologie		
10002	General medicine	Allgemeinmedizin		
10003	Anesthetics	Anästhesiologie		
10004	Angiology	Angiologie		
10005	Clinical pharmacology	Pharmakologie		
10006	Occupational medicine	Arbeitsmedizin		
10007	Chiropraxy	Chiropraktik		
10008	Surgery	Chirurgie		
10009	Dermatology	Dermatologie und Venerologie		
10010	Endocrinology	Endokrinologie/Diabetologie		
10011	Occupational therapy	Ergotherapie		
10012	Unit of dietetics and nutrition	Ernährungsberatung		
10013	Geriatric medicine	Geriatrie		
10014	Gastroenterology	Gastroenterologie		
10015	Obstetrics and gynecology	Gynäkologie und Geburtshilfe		
10016	Cardiac surgery	Herz- und Gefässchirurgie		
10017	Infectious diseases (specialty)	Infektiologie		
10018	Internal medicine	Innere Medizin		
10019	Intensive care service	Intensivmedizin		
10020	Cardiology	Kardiologie		
10021	Complementary therapy service	Komplementärmedizin		
10022	Pediatric specialty	Pädiatrie		
10023	Psychology service	Psychologie		
10024	Laboratory Service	Labormedizin		
10025	Speech and language therapy service	Logopädie		
10026	Clinical genetics	Medizinische Genetik		
10027	Oral and maxillofacial surgery	Mund-, Kiefer- und Gesichtschirurgie		
10028	Nephrology	Nephrologie		
10029	Neurosurgery	Neurochirurgie		
10030	Neurology	Neurologie		
10031	Nuclear medicine - specialty	Nuklearmedizin		
10032	Ophthalmology	Ophthalmologie		
10033	Trauma and orthopedics	Orthopädie und Traumatologie		
10034	Osteopathy	Osteopathie		
10035	Oto-Rhino-Laryngology	Oto-Rhino-Laryngologie		
10036	Palliative medicine	Palliativmedizin		
10037	Pathology	Pathologie		
10038	Nursing service	Pflege		

10039	Physical medicine	Physikalische Medizin		
10040	Physiotherapy	Physiotherapie		
10041	Plastic surgery	Plastische, Rekonstruktive und Ästhetische Chirurgie		
10042	Pneumology	Pneumologie		
10043	Podiatry service	Podologie		
10044	Preventive medicine	Prävention		
10045	Psychiatry and Psychotherapy	Psychiatrie und Psychotherapie		
10046	Psychosomatic medicine	Psychosomatik		
10047	Radiology - specialty	Radiologie		
10048	Radiation oncology AND/OR radiotherapy	Radio-Onkologie/Strahlentherapie		
10049	forensic medicine	Rechtsmedizin		
10050	Rehabilitation - specialty	Rehabilitation		
10051	Emergency medical services	Notfall und Rettungsmedizin		
10052	Rheumatology	Rheumatologie		
10053	Thoracic surgery	Thoraxchirurgie		
10054	Blood transfusion (specialty)	Transfusionsmedizin		
10055	Tropical medicine	Tropen- und Reisemedizin		
10056	Urology	Urologie		
10057	Odontology	Zahnheilkunde		
10058	Clinical hematology	Hämatologie		
10059	Clinical immunology/allergy	Immunologie		
10900	unknown	Unbekannt		
10999	other	Andere nicht näher spezifizierte medzinische Fachrichtung		

1.11 Sexe du patient

OID pour HL7 administrative sex: 2.16.840.1.113883.12.1

Code national	Désignation anglaise	Désignation allemande	Désignation française	Désignation italienne
F	Female	weiblich		
M	Male	männlich		
O	Other	andere		

1.12 Type du document

OID national: : 2.16.756.5.30.1.127.3.10.1.27

Code national	Désignation anglaise	Désignation allemande	Désignation française	Désignation italienne
60001	Privacy policy acknowledgment Document	Patienteneinwilligung für die Verwendung der elektronischen Daten		
60002	Patient Consent	Patienteneinwilligung		
60003	Advance directive status	Patientenverfügung		
60004	Patient Summary document	Patient Summary (medizinische Zusammenfassung)		
60005	Medication summary Document	Medikamentenliste (aktuell)		
60006	Prescription For Medication Document	elektronisches Rezept		
60007	Admission request Document	Zuweisungsschreiben/Einweisungsschreiben		
60008	Physician consulting Initial evaluation note	Eintrittsbericht		
60009	Physician Discharge concise summary	Kurz-Austrittsbericht (ärztlich)		
60010	Physician Discharge summary	Austrittsbericht (lang-ärztlich)		
60011	nurse discharge concise summary	Kurz-Austrittsbericht (pflegerisch)		
60012	nurse discharge summary	Austrittsbericht (lang-pflegerisch)		
60013	Provider-unspecified Transfer summary	Verlegungsbericht		
60014	Obstetrics and Gynecology Discharge summary	Verlaufs- / Austrittsbericht Gynäkologie und Geburtshilfe		
60015	Overall Plan of Care/Advance Care Directives	Pflegeplan (allgemein)		
60016	nursing note	Pflegebericht		
60017	Referral note	Konsilauftrag (allgemein)		
60018	laboratory order	Laborauftrag		
60019	pathology order	Pathologieauftrag		
60020	Requested imaging studies information Document	Radiologieauftrag		
60021	Consult Note	Konsultationsbericht		
60022	Diagnostic studies.non-lab	Untersuchungsbefund (allgemein)		
60023	Laboratory report	Labor-Befund		
60024	Diagnostic Imaging Report	Radiologie-Befund		
60025	Pathology studies	Pathologie-Befund		
60026	Bone marrow Pathology biopsy report	Knochenmark-Biopsie-Befund		
60027	Tissue Pathology biopsy report	Histologie-Befund		

60028	Cardiac catherization study	Herzkatheter-Befund		
60029	Heart US	Echokardiographie-Befund		
60030	Pulmonary function report	Lungenfunktions-Befund		
60031	Physical therapy consult note	Physiotherapiebericht		
60032	Anesthesiology Note	Anästhesie Bericht		
60033	Surgery Surgical operation note	OP-Bericht		
60034	Wound care management Note	Wundbefund		
60035	Provider-unspecified ED Progress note	Notfallbericht		
60036	Provider-unspecified Progress note	klinisches Verlaufsblatt		
60037	Cardiology Hospital Progress note	Kardiologie Verlaufs-Bericht		
60038	Intensive care Unit Progress Note	Kurve Intensivstation		
60039	Conclusions (interpretation) document	Beschlussprotokoll		
60040	Photographic image Unspecified body region Document	Nicht spezifizierte Bilddaten		
60041	Radiology studies	Radiologische Bilddaten		
60042	Infectious disease Diagnostic study note	Meldung übertragbare Erkrankung		
60043	Vaccination record	elektronisches Impfdossier		
60044	Emergency record	Notfall-Ausweis		
60045	Treatment scheme	Behandlungsschema		
60046	Allergy record	Allergie-Ausweis		
60047	Birth certificate document	Geburtsanzeige		
60048	Eligibility acknowledgement	Kostengutsprache		
60049	Audit trail	Protokolldaten		
60900	Unknown	Unbekannt		
60999	Other	Andere nicht näher spezifiziert		

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI

Office fédéral de la santé publique OFSP
Unité de direction Politique de la santé

RS 816.11.n / Annexe 5 de l'ordonnance du DFI du ... sur le dossier électronique du patient

Adaptations nationales des profils d'intégration selon l'article 5, lettre b ODEP-DFI

National extensions to the IHE Technical Framework

Version: 1.0 22.03.2016
Entrée en vigueur: ...

National Extensions

The national extensions documented in this section shall be used in conjunction with the definitions of integration profiles, actors and transactions provided in Volumes 1 through 3 of the IHE IT Infrastructure Technical Framework. This section includes extensions and restrictions to effectively support the regional practice of healthcare in Switzerland. It also translates a number of English terms to ensure correct interpretation of requirements of the IT Infrastructure Technical Framework.
This IT Infrastructure national extension document was authored under the supervision of the Federal Office of Public Health (FOPH), eHealth Suisse and IHE Suisse in order to fulfil the Swiss regulations. See also Ordinance to the Federal Act on the Electronic Health Record, published in the Official Compilation of Federal Legislation[1] (available in German, French and Italian).

[1] German: https://www.admin.ch/opc/de/classified-compilation/20111795/index.html
French: https://www.admin.ch/opc/fr/classified-compilation/20111795/index.html
Italian: https://www.admin.ch/opc/it/classified-compilation/20111795/index.html

1.1 Definitions of terms

1.1.1 Electronic patient dossier (EPD)

The object of the Federal Law on Electronic Health Records (FLEHR) is to define the conditions for processing data and documents relating to electronic health records. Using electronic health records, healthcare professionals can access data relevant to treatment of their patients that was compiled and decentrally recorded by healthcare professionals involved in the treatment process. Healthcare professionals may save this data if necessary in their practice and hospital information systems outside of the electronic health records. To access electronic health records, healthcare professionals must join a certified community, which is an association of healthcare professionals and their institutions, and their patients must grant them the necessary access rights. In addition, the electronic health record also allows patients to view their data, to make their own data accessible and to manage the allocation of access rights. Healthcare professionals may only process data in electronic health records with the consent of the patient. Patients have the option of granting individual and graded access rights.
Notation of this term in the following text: **EPD**

1.1.2 EPD circle of trust

From an organizational perspective and in terms of the FLEHR, communities are an association of healthcare professionals and their institutions. Communities who want to participate in the Swiss EPD must comply with the certification requirements as laid down in the implementing provisions for the FLEHR. Such communities and, in particular, their gateways will be listed in a community portal index provided by the FOPH and therefore form a circle of trust by mutual recognition of their conformity related to data protection and data privacy. Furthermore, all required central services are also part of this circle of trust.
Notation of this term in the following text: **EPD circle of trust**

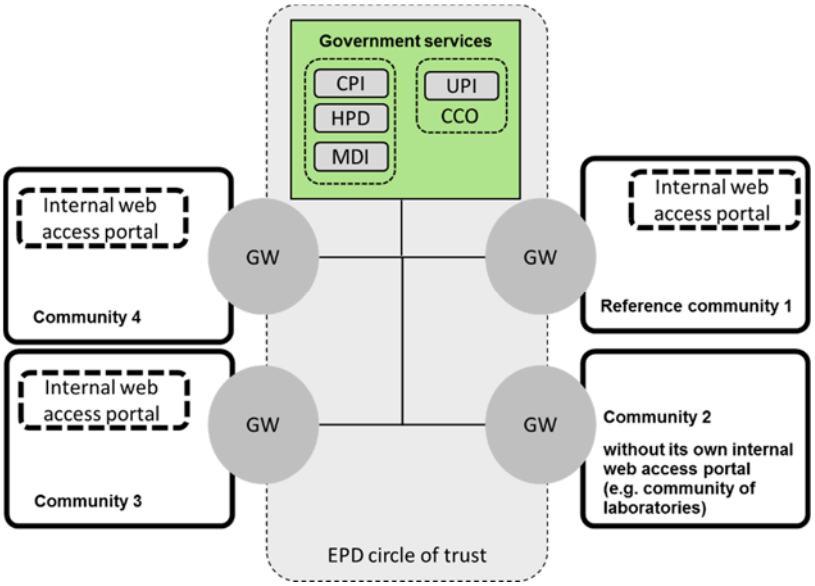


Figure 1: Swiss EPD circle of trust

Legend:

- GW: Gateway
- CPI: Community / Portal Index
- UPI: Unique Person Identification
- HPD: Healthcare Provider Directory
- MDI: Metadata Index-Service

1.1.3 Reference community

If a patient decides to open an EPD, she or he first chooses a community that manages all of his current consents and access right configurations to be used by other EPD users (in essence healthcare professionals) while accessing his personal EPD. Consents and access rights for one patient are managed by exactly one community in the EPD circle of trust.
Although the term home community is used by IHE in a slightly different way, the current specification states this consent and access right management community as reference community.
Cross-community accesses to documents within the EPD are only permitted when the initiating user gets permission by the access rights defined by the patient. Although cross-community accesses may occur between each community within the EPD circle of trust regardless whether it is the patient's reference community or not, the responding community must always apply the current access right settings managed by the reference community.
The patient may change his reference community at any time (for example, when moving to another residence).
Notation of this term in the following text: **referenceCommunity**

1.1.4 Patient Identifiers (EPD-PID, MPI-PID)

Communities in the EPD circle of trust use the national EPD patient identifier (EPD-PID) only for cross-community communication. The federal Central Compensation Office (CCO)[2] is the institution which issues EPD-PID's. CCO is the only institution which is allowed to correlate the Social Security Number (AVN13) with the EPD-PID. There is no correlation possible back from the EPD-PID to the Social Security Number. This is political intention in order to achieve highest possible patient privacy.
Within a community patients are identified by a MPI-PID which is managed by a community Master Patient Index (MPI). Primary Systems may correlate their local patient identifier with the MPI-PID. For cross-community communication the gateways may correlate the MPI-ID to the EPD-PID.

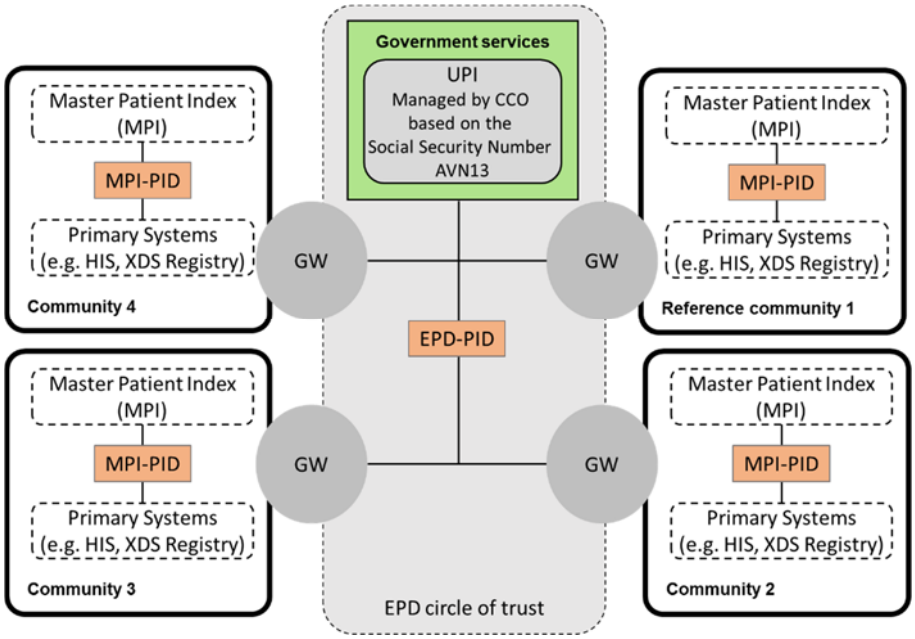


Figure 2 Swiss Patient Identifiers

1.2 IHE Suisse Scope of precisions

The extensions, restrictions and translations specified apply to the following IHE IT Infrastructure Integration profiles:

- IT Infrastructure: Consistent Time (CT)
- IT Infrastructure: Audit Trail and Node Authentication (ATNA)

[2] http://www.zas.admin.ch/index.html

- IT Infrastructure: Cross-Community Access (XCA)
- IT Infrastructure: Patient Identifier Cross-Reference HL7 V3 (PIXv3)
- IT Infrastructure: Patient Demographic Query HL7 V3 (PDQv3)
- IT Infrastructure Technical Framework Supplement: Cross-Community Patient Discovery (XCPD)
- IT Infrastructure Technical Framework Supplement: Healthcare Provider Directory (HPD)

1.3 Requirements on CT Profile for Swiss Time Service

ITI TF-1 does not specify any NTP Servers. The following Time Service MUST be used by all actors in the Swiss EPD circle of trust.

- Maintain Time [ITI-1]
  ntp.metas.ch MUST be used as Time Service.

1.4 Requirements on ATNA, XDS.b and XCA Profiles for Audit Trail Consumption

1.4.1 Introduction

The FLEHR requires a patient access on the complete audit trail within the EPD circle of trust. The access to the audit trail will be provided by certified web access portals for patients.
The present national extension will use and precise the existing transactions and content profiles of the Audit Trail and Node Authentication (ATNA), Cross-Enterprise Document Sharing (XDS.b) and Cross-Community Access (XCA) integration profiles in order to achieve the Swiss regulation needs on the audit trail access by patients.
This figure shows all relevant actors and transactions for the present national extension:

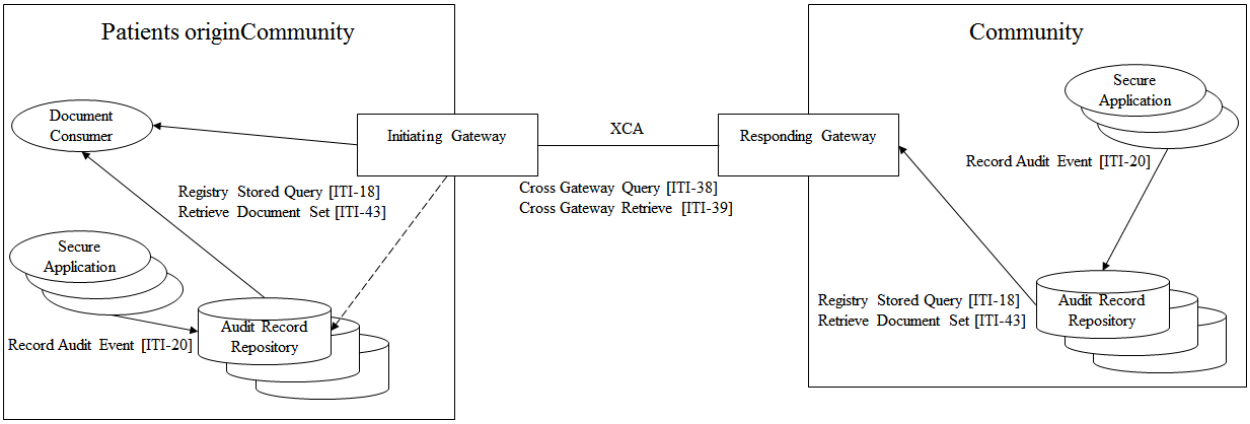


Figure 3: Big picture – actors and transactions

This figure shows all relevant content profiles for the present national extension:

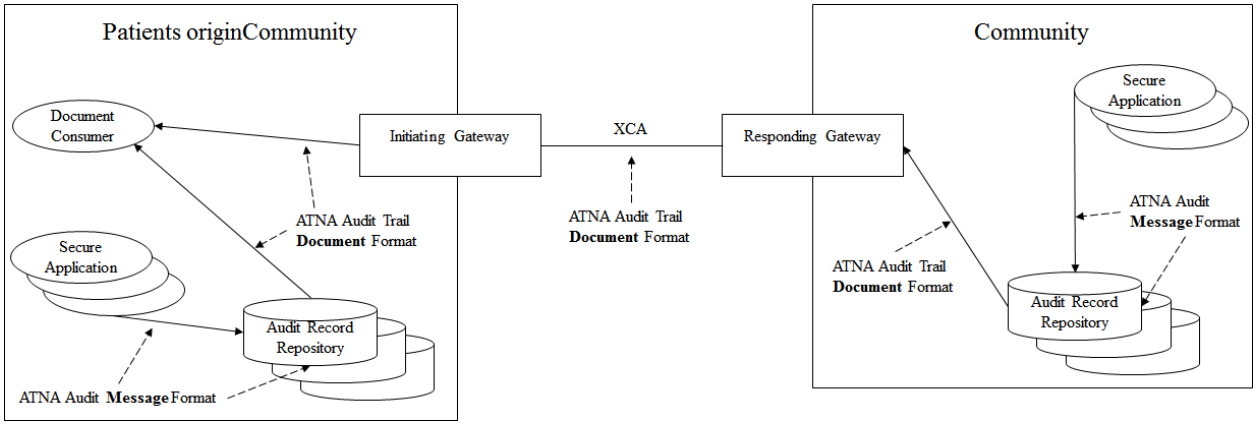


Figure 4: Big picture – content profiles

1.4.2 Actors

1.4.2.1 XDS.b Document Consumer

The following option MUST be implemented by all web access portal providers for patients in the Swiss EPD circle of trust:

- On-Demand Documents Option (see ITI TF-2a, 3.18.4.1.2.5)

These actors MUST …

- combine all Audit Trail Message entries of all Audit Trail Document entries into one single document of type ATNA Audit Trail Document Format (see chapter 1.4.4.2 on page 23). Relevant transactions:
  - Registry Stored Query [ITI-18] transaction that uses the parameters described in chapter "1.4.3.1.1 Parameters for stored query FindDocuments" on page 10.
  - Retrieve Document Set [ITI-43] transaction performed against an Audit Record Repository using a document UUID received by a previously executed by a Registry Stored Query mentioned before.
- translate the coded information into the language preferred by the user when provide it to the user through the UI or other results like reports. Translations MUST fulfil the following requirements:
  - Translations in German, French and Italian MUST be supported. Other language translations are permitted but remain in the responsibility of the software vendor.
  - Translations for coded values from the Swiss Metadata Value-Set[3] must match the translations provided in the Swiss Metadata Value-Set.
  - Translations for coded values mentioned in the present national extensions MUST be used.
  - No translation is required for narrative text.

1.4.2.2 XCA Initiating Gateway

The following option MUST be implemented by all community gateways in the Swiss EPD circle of trust:

- On-Demand Documents Option (see ITI TF-2a, 3.18.4.1.2.5)

These actors basically relay the XDS.b Registry Stored Query [ITI-18] and XDS.b Retrieve Document Set [ITI-43] transactions to XCA Cross Gateway Query [ITI-38] and XCA Cross Gateway Retrieve [ITI-39] as described in IHE ITI TF-2.

[3] <TODO: Laid down in the Departmental Ordinance on the Electronic Health Record and published elsewhere>

If the homeCommunityId represents the local community and the parameter $XDSDocumentEntryTypeCode contains the value 60049 (Audit trail), these actors MUST initiate a Registry Stored Query to all local ATNA Audit Repositories.
See also chapter "1.4.3.1.1 Parameters for stored query FindDocuments" on page 10.

1.4.2.3 XCA Responding Gateway

The following option MUST be implemented by all community gateways in the Swiss EPD circle of trust:

- On-Demand Documents Option (see ITI TF-2a, 3.18.4.1.2.5)

These actors basically relay the XCA Cross Gateway Query [ITI-38] and XCA Cross Gateway Retrieve [ITI-39] to XDS.b Registry Stored Query [ITI-18] and XDS.b Retrieve Document Set [ITI-43] transactions as described in ITI TF-2.
If the parameter $XDSDocumentEntryTypeCode contains the value 60049 (Audit trail), these actors MUST initiate a Registry Stored Query to all local ATNA Audit Repositories.
See also chapter "1.4.3.1.1 Parameters for stored query FindDocuments" on page 10.

1.4.2.4 ATNA Secure Application

The following transactions are declared as optional in ITI TF-1 but are REQUIRED by the present national extension:

- Maintain Time [ITI-1]
  See chapter "1.3 Requirements on " on page 7.
- Record Audit Event [ITI-20]
  The Audit Message Format described in chapter "1.4.4.1 ATNA Audit Message Format" on page 13 MUST be used.

This behaviour MUST be implemented by all applications in the Swiss EPD circle of trust that are requesting, consuming or producing health information of patients having an EPD.

1.4.2.4.1 Audit messages

All ATNA Secure Application actors are required to record the audit messages defined by the IHE actor they are grouped with as described in the IHE Technical Framework.
In case these audit messages do not fulfil the requirements described in chapter "1.4.4.1 ATNA Audit Message Format" on page 13, ATNA Secure Application actors within the Swiss EPD circle of trust MUST record an additional audit message as described in chapter "1.4.4.1 ATNA Audit Message Format" on page 13 for each transaction concerning a patient having an EPD.

1.4.2.5 ATNA Audit Record Repository

ATNA Audit Record Repository actors within the Swiss EPD circle of trust MUST …

- support the following options and transactions:
  (see chapter "1.4.3 Transactions" starting on page 10 for detailed descriptions)
  - On-Demand Documents Option (see ITI TF-2a, 3.18.4.1.2.5).
  - XDS.b Registry Stored Query [ITI-18].
  - XDS.b Retrieve Document Set [ITI-43].
- be able to receive and store audit messages of Audit Message Format described in chapter "1.4.4.1 ATNA Audit Message Format" on page 13 by the Record Audit Event [ITI-20] which is based on the preferred Audit Message Format by IHE ATNA (see ITI TF-2a, chapter 3.20.7.1).
- be able to perform the Retrieve Document Set transaction for all On-Demand documents specified by document and repository UUIDs created by a previously Registry Stored Query transaction.
- have assigned a unique repository ID within the community (similar to XDS.b Document Repository actors).

1.4.3 Transactions

1.4.3.1 Registry Stored Query [ITI-18]

See ITI TF-2a, chapter "3.18.4.1.2.3 Query Request Parameters – Coding Style". The query parameters described in the following chapter MUST be used for Audit Trail Consumption.

1.4.3.1.1 Parameters for stored query FindDocuments

ITI TF-2a specifies the query parameters for a stored query "FindDocuments" (see ITI TF-2a 3.18.4.1.2.3.7.1). The stored query "FindDocuments" MUST be used using the following parameters in order to retrieve Audit Trails within the Swiss EPD circle of trust.
The mentioned Swiss Metadata Value-Set can be found in appendix 3 of the Departmental Ordinance on the Electronic Health Record.

Table 1: Parameters for stored query FindDocuments

Element Name Attribute	Card.	Original descriptions	Swiss National Extension
$XDSDocumentEntryPatientId XDSDocumentEntry.patientId	[1..1]	The format of the patientId value is CX. See also ITI TF-3, 4.2.3.2.16	No further refinement.
$XDSDocumentEntryClassCode XDSDocumentEntry.classCode	[0..*]	The code specifying the high-level use classification of the document type (e.g., Report, Summary, Images, Treatment Plan, Patient Preferences, Workflow). See also description 1 below and ITI TF-3, 4.2.3.2.3	This value MUST represent the following value from the Swiss Metadata Value-Set "epd_xds_classCode" (2.16.756.5.30.1.127.3.10.1.3): DTC90 (Other Composition)
$XDSDocumentEntryTypeCode XDSDocumentEntry.typeCode	[0..*]	The code specifying the precise type of document from the user perspective. See also description 1 below and ITI TF-3, 4.2.3.2.25	This value MUST represent the following value from the Swiss Metadata Value-Set "epd_xds_typeCode" (2.16.756.5.30.1.127.3.10.1.27): 60049 (Audit Trail)
$XDSDocumentEntryPracticeSettingCode XDSDocumentEntry.practiceSettingCode	[0..*]	The code specifying the clinical specialty where the act that resulted in the document was performed (e.g., Family Practice, Laboratory, Radiology). See also description 1 below and ITI TF-3, 4.2.3.2.17	When specified, this value MUST represent a value from the Swiss Metadata Value-Set "epd_xds_practiceSettingCode" (2.16.756.5.30.1.127.3.10.1.18)
$XDSDocumentEntryCreationTimeFrom Lower value of XDSDocumentEntry.creationTime	[0..1]	creationTime represents the time the author created the document. See also description 6 below and ITI TF-3, 4.2.3.2.6	MUST NOT be specified ([0..0]).
$XDSDocumentEntryCreationTimeTo Upper value of XDSDocumentEntry.creationTime	[0..1]		
$XDSDocumentEntryServiceStartTimeFrom Lower value of	[0..1]	Represents the start time of the service	Used to specify the start time of the desired audit trail message to be returned.

Element Name Attribute	Card.	Original descriptions	Swiss National Extension
XDSDocumentEntry.serviceStartTime		being documented took place (clinically significant, but not necessarily when the document was produced or approved). See also ITI TF-3, 4.2.3.2.19	All audit trail messages having the @EventDateTime (AuditMessage/EventIdentification) equals or newer MUST be returned by the Audit Record Repository actor.
$XDSDocumentEntryServiceStartTimeTo Upper value of XDSDocumentEntry.serviceStartTime	[0..1]		MUST NOT be specified ([0..0]).
$XDSDocumentEntryServiceStopTimeFrom Lower value of XDSDocumentEntry.serviceStopTime	[0..1]	Represents the stop time of the service being documented took place (clinically significant, but not necessarily when the document was produced or approved). See also ITI TF-3, 4.2.3.2.20	MUST NOT be specified ([0..0]).
$XDSDocumentEntryServiceStopTimeTo Upper value of XDSDocumentEntry.serviceStopTime	[0..1]		Used to specify the stop time of the desired audit trail message to be returned. All audit trail messages having the @EventDateTime (AuditMessage/EventIdentification) equals or older MUST be returned by the Audit Record Repository actor.

Element Name Attribute	Card.	Original descriptions	Swiss National Extension
$XDSDocumentEntryHealthcareFacilityTypeCode XDSDocumentEntry.healthcareFacilityTypeCode	[0..*]	This code represents the type of organizational setting of the clinical encounter during which the documented act occurred. See also description 1 below and ITI TF-3, 4.2.3.2.11	When specified, this value MUST represent a value from the Swiss Metadata Value-Set "epd_xds_healthcareFacility-TypeCode" (2.16.756.5.30.1.127.3.10.1.11)
$XDSDocumentEntryEventCodeList XDSDocumentEntry.eventCodeList	[0..*]	This list of codes represents the main clinical acts, such as a colonoscopy or an appendectomy being documented. See also description 1, 3 below and ITI TF-3, 4.2.3.2.8	No further refinement.
$XDSDocumentEntryConfidentialityCode XDSDocumentEntry.confidentialityCode	[0..*]	The code specifying the security and privacy tags of the document. See also description 1 below and ITI TF-3, 4.2.3.2.5	This value MUST represent the following value from the Swiss Metadata Value-Set "epd_xds_confidentialityCode" (2.16.756.5.30.1.127.3.10.1.5): 30005 (very restricted)
$XDSDocumentEntryAuthorPerson XDSDocumentEntry.author	[0..*]	Represents the humans and/or machines that authored the document. See also description 4 below and ITI TF-3, 4.2.3.2.1	No further refinement.
$XDSDocumentEntryFormatCode XDSDocumentEntry.formatCode	[0..*]	The code specifying the detailed technical format of the document. See also description 1 below and ITI TF-3, 4.2.3.2.9	This value MUST represent the following value from the Swiss Metadata Value-Set "epd_xds_formatCode" (2.16.756.5.30.1.127.3.10.1.9): urn:che:epd:EPD_Basic_Document <*TODO OID to be registered for the content profile. As soon as it is registered change the format code to urn:che:epd:urn:che:epd:2.16.756.5.30…*>
$XDSDocumentEntryStatus XDSDocumentEntry.status	[1..*]	Represents the status of the DocumentEntry. A DocumentEntry shall have one of two availability statuses: Approved: The document is available for patient care. Deprecated: The document is obsolete. See also ITI TF-3, 4.2.3.2.2	While audit trail entries may not be deprecated, the following value MUST be used: urn:oasis:names:tc:ebxml-regrep:StatusType:Approved
$XDSDocumentEntryType XDSDocumentEntry.objectType	[0..*]	The objectType attribute reflects the type of DocumentEntry As described in Section 4.1.1, there are two	While queries to audit trails are On-Demand documents, the following value MUST be used: urn:uuid:34268e47-fdf5-41a6-ba33-82133c465248 (On-Demand)

Element Name Attribute	Card.	Original descriptions	Swiss National Extension
		DocumentEntry types: Stable Document Entry and On-Demand Document Entry. See also description 5 below and ITI TF-3, 4.2.3.2.30	

Descriptions from ITI TF-2a, 3.18.4.1.2.3.7.1:

1. Shall be coded according to specification in Section 3.18.4.1.2.3.4 Coding of Code/Code-Scheme.
2. Supports AND/OR semantics as specified in Section 3.18.4.1.2.3.5.
3. The value for this parameter is a pattern compatible with the SQL keyword LIKE which allows the use of the following wildcard characters: % to match any (or no) characters and _ to match a single character. The match shall be applied to the text contained in the Value elements of the authorPerson Slot on the author Classification (value strings of the authorPerson sub-attribute)
4. See Section 3.18.4.1.2.3.6.2
5. CreationTimeFrom and CreationTimeTo are ignored when evaluating an On-Demand Document Entry's selection for inclusion in the query response.

1.4.3.1.2 Response

ATNA Audit Record Repository actors within the Swiss EPD circle of trust MUST…

1. create a virtual document UUID and return it as one single document entry in the result (On-Demand Document) and
2. cache all audit messages matched by the filter parameters in order to provide them by the retrieve Document Set transaction using the corresponding document UUID in the ATNA Audit Trail Document Format. Caching is REQUIRED for 8 hours. Later accesses to the corresponding document UUID MUST fail.

1.4.3.2 Retrieve Document Set [ITI-43]

ATNA Audit Record Repository actors within the Swiss EPD circle of trust MUST return the audit messages matched by the filter parameters in the query of the corresponding document UUID. The contents of the document returned MUST exactly conform to the state at the point of time of the stored query FindDocuments execution.

1.4.3.3 Record Audit Event [ITI-20]

The ATNA Audit Message Format described in chapter 1.4.4.1 starting on page 13 MUST be used for all events for patients having an EPD.

1.4.4 Content profiles

1.4.4.1 ATNA Audit Message Format

IHE ITI TF-2a references to several Audit Message Formats (see ITI TF-2a, 3.20.7) and prefers use of the DICOM schema for audit records generated by all IHE actors (see ITI TF-2a, 3.20.7.1). ATNA Secure Application actors within the Swiss EPD circle of trust MUST record an audit message for each transaction concerning a patient having an EPD using the mentioned DICOM schema.
The schema can be found in the DICOM Standard, Part 15 Annex A.5 (available from: http://dicom.nema.org/medical/dicom/current/output/chtml/part15/sect_A.5.html).
Detailed contents to be provided by all ATNA Secure Application actors within the Swiss EPD circle of

trust are described in the following chapter.

1.4.4.1.1 Detailed AuditMessage definitions

The detailed specifications for IHE actor audit message requirements specified within the IHE integration profiles MUST be used with the following specification.

Table 2: Detailed AuditMessage definitions

Element Name	Card.	Original descriptions	Swiss National Extension
AuditMessage [1..1] (root element)			
AuditMessage/EventIdentification [1..1] (type: EventIdentificationContents)			
@EventActionCode (type: xs:token)	[0..1]	Indicator for type of action performed during the event that generated the audit. C= Create R= Read U= Update D= Delete E= Execute	No further refinement.
@EventDateTime (type: xs:dateTime)	[1..1]	Universal coordinated time (UTC), i.e., a date/time specification that is unambiguous as to local time zones The time at which the audited event occurred. See Section A.5.2.5	Date and time format following ISO 8601 MUST be used. Indication of the time zone in Switzerland during the daylight-savings time (summer): UTC +2 hours and during normal time (winter): UTC +1 hour. Sample daylight-savings time: 2016-08-10T20:29:10+02:00 Sample normal time: 2016-02-10T20:29:10+01:00

Element Name	Card.	Original descriptions	Swiss National Extension
@EventOutcomeIndicator (type: xs:token)	[1..1]	Indicates whether the event succeeded or failed. When a particular event has some aspects that succeeded and some that failed, then one message shall be generated for successful actions and one message for the failed actions (i.e., not a single message with mixed results). 0= Nominal Success (use if status otherwise unknown or ambiguous) 4=Minor failure (per reporting application definition) 8=Serious failure (per reporting application definition) 12=Major failure (reporting application now unavailable)	No further refinement.
EventID (type: CodedValueType)	[1..1]	Identifier for a specific audited event … The identifier for the family of event. E.g., "User Authentication"; Extended by DICOM using DCID (400)	No further refinement.
EventTypeCode (type: CodedValueType)	[0..*]	Identifier for the category of event. The specific type(s) within the family applicable to the event, e.g., "User Login". Note: DICOM/IHE defines and uses this differently than RFC-3881. Extended by DICOM using DCID (401).	No further refinement.
EventOutcomeDescription	[0..1]	N/A	No further refinement.
AuditMessage/ActiveParticipant [1..1] (type: ActiveParticipantContents)			
@UserID (type: text)	[1..1]	Unique identifier for the user actively participating in the event. If the participant is a person, then the User ID shall be the identifier used for that person on this particular system, in the form of loginName@domain-name. If the participant is an identifiable process, the UserID selected shall be one of the identifiers used in the internal system logs. See also A.5.2.1	No further refinement.
@AlternativeUserID (type: text)	[0..1]	Alternative unique identifier for the user. If the participant is a person, then Alternative User ID shall be the identifier used for that person within an enterprise for authentication purposes, for example, a Kerberos	No further refinement.

Element Name	Card.	Original descriptions	Swiss National Extension
		Username (user@realm). If the participant is a DICOM application, then Alternative User ID shall be one or more of the AE Titles that participated in the event. See also A.5.2.2	
@UserName (type: text)	[0..1]	A human readable identification of the participant. If the participant is a person, the person's name shall be used. If the participant is a process, then the process name shall be used. See also A.5.2.3	If the participant is a person, the person's name MUST be specified as follows: [<title>]<family name> <given name>
@UserIsRequestor (type: xs:Boolean)	[1..1]	Indicator that the user is or is not the requestor, or initiator, for the event being audited. Used to identify which of the participants initiated the transaction being audited. If the audit source cannot determine which of the participants is the requestor, then the field shall be present with the value FALSE in all participants. The system shall not identify multiple participants as UserIsRequestor. If there are several known requestors, the reporting system shall pick only one as UserIsRequestor.	No further refinement.
@NetworkAccessPointID (type: xs:token)	[0..1]	An identifier for the network access point of the user device This could be a device id, IP address, or some other identifier associated with a device. See also A.5.2.4	No further refinement.
@NetworkAccessPointTypeCode	[0..1]	An identifier for the type of network access point. 1= Machine Name, including DNS name 2= IP Address 3= Telephone Number 4= Email address 5= URI (user directory, HTTP-PUT, ftp, etc.) See also A.5.2.4	No further refinement.
RoleIDCode (type: CodedValueType)	[0..*]	Specification of the role(s) the user plays when performing the event, as assigned in role-based access control security Extended by DICOM using DCID (402) Usage of this field is refined in the individual message descriptions below. Other additional roles may also	When describing a human user's participation in an event, this value MUST represent a value from the Swiss Metadata Value-Set "epd_xds_authorRole" (2.16.756.5.30.1.127.3.10.1.1.3)

Element Name	Card.	Original descriptions	Swiss National Extension
		be present, since this is a multi-valued field. ITI TF-2a, 3.20.7.7: RoleIDCode is a CodedValueType. When describing a human user's participation in an event, this value should represent the access control roles/permissions that authorized the event/trans. Use of standards based roles/permissions is preferable to site or application specific. As RFC3881 indicates Many security systems are unable to produce this data, hence it is optional. For example: at a site "St Fraser" they have defined a functional role code "NURSEA" for attending nurse. This can be represented as EV("NURSEA", "St Fraser", "Attending Nurse") Candidate standards based structural/functional role codes can be found at ISO, HL7, ASTM, and various other sources.	
MediaIdentifier/MediaType (type: CodedValueType)	[0..1]	When importing or exporting data, e.g., by means of media, the UserID field is used both to identify people and to identify the media itself. See also A.5.2.1	When importing or exporting data, this value MUST represent either a unique media identifier or at least a unique media type (e.g., DVD, paper, film). Currently there is no Swiss Metadata Value-Set available for media types, but as soon as there is one, it MUST be used when describing media types.
AuditMessage/AuditSourceIdentification [1..1] (type: AuditSourceIdentificationContents)			
@code (type: xs:token)	[1..1]	1= End-user display device, diagnostic device 2= Data acquisition device or instrument 3= Web Server process or thread 4= Application Server process or thread 5= Database Server process or thread 6= Security server, e.g., a domain controller 7= ISO level 1-3 network component 8= ISO level 4-6 operating software 9= other Other values are allowed if a codeSystemName is present.	No further refinement.
other-csd-attributes	N/A	See descriptions for attribute group other-csd-attributes.	
@AuditEnterpriseSiteID	[0..1]	Logical source location within the healthcare enterprise network, e.g., a hospital or other provider location within a multi-entity provider group. Serves to further qualify the Audit Source ID, since Audit Source ID is not required to be globally unique.	[1..1] The GLN of the audit source MUST be specified. Audit sources may apply for a GLN. When presenting to the user, the GLN details MUST be provided[4].

[4] There exists a Webservice at the Refdata foundation which might be used: http://refdatabase.refdata.ch/Service/Partner.asmx?WSDL (see also http://www.refdata.ch/content/page_1.aspx?Nid=60&Aid=636&ID=296)

Element Name	Card.	Original descriptions	Swiss National Extension
@AuditSourceID (type: xs:token)	[1..1]	Identifier of the source. The identification of the system that detected the auditable event and created this audit message. Although often the audit source is one of the participants, it could also be an external system that is monitoring the activities of the participants (e.g., an add-on audit-generating device).	A meaningful description of the audit source, comprehensible for the patient / citizen must be specified.
AuditSourceTypeCode (type: xs:token)	[0..*]	Code specifying the type of source Used as defined in RFC 3881: 1= End-user display device, diagnostic display 2= Data acquisition device or instrument 3= Web server process 4= Application server process 5= Database server process 6= Security server, e.g., a domain controller 7= ISO level 1-3 network component 8= ISO level 4-6 operating software 9= External source, other or unknown type E.g., an acquisition device might use "2" (data acquisition device), a PACS/RIS system might use "4 "(application server process).	No further refinement.
AuditMessage/ParticipantObjectIdentification [0..*] (type: ParticipantObjectIdentificationContents)			
@ParticipantObjectID (type: xs:token)	[1..1]	Describes the identifier that is contained in Participant Object ID. Values may be drawn from those listed in RFC 3881 and DCID (404), as specified in the individual message descriptions.	No further refinement. To be used as specified in the IHE actor audit message requirements specified within the IHE integration profiles.
@ParticipantObjectTypeCode (type: xs:token)	[0..1]	1= Person 2= System object 3= Organization 4= Other	No further refinement. To be used as specified in the IHE actor audit message requirements specified within the IHE integration profiles.

Element Name	Card.	Original descriptions	Swiss National Extension
@ParticipantObjectTypeCodeRole (type: xs:token)	[0..1]	1= Patient 2= Location 3= Report 4= Resource 5= Master File 6= User 7= List 8= Doctor 9= Subscriber 10= guarantor 11= Security User Entity 12= Security User Group 13= Security Resource 14= Security Granulatiry Definition 15= Provider 16= Report Destination 17= Report Library 18= Schedule 19= Customer 20= Job 21= Job Stream 22= Table 23= Routing Criteria 24= Query	No further refinement. To be used as specified in the IHE actor audit message requirements specified within the IHE integration profiles.
@ParticipantObjectDataLifeCycle (type: xs:token)	[0..1]	1= Origination, Creation 2= Import/ Copy 3= Amendment 4= Verification 5= Translation 6= Access/Use 7= De-identification 8= Aggregation, summarization, derivation 9= Report 10= Export 11= Disclosure 12= Receipt of Disclosure 13= Archiving 14= Logical deletion 15= Permanent erasure, physical destruction	No further refinement. To be used as specified in the IHE actor audit message requirements specified within the IHE integration profiles.

Element Name	Card.	Original descriptions	Swiss National Extension
@ParticipantObjectSensitivity (type: xs:token)	[0..1]	Denotes policy-defined sensitivity for the Participant Object ID such as VIP, HIV status, mental health status, or similar topics. Used as defined in RFC 3881.	The current confidentiality code of the object MUST be specified when the object is a document in the EPD. This value MUST represent a value from the Swiss Metadata Value-Set "epd_xds_confidentialityCode" (2.16.756.5.30.1.127.3.10.1.5) in the HL7 CNE datatype format. The following sequences are required: CNE.1: Code national CNE.2: Text in ge, fr or it CNE.7: Publication date of the value-set in the format YYYYMMDD CNE.14: OID of the value-set Sample: 30003^medical data^^^^^ 20150702^^^^^^^ 2.16.756.5.30.1.127.3.10.1.5
ParticipantObjectIDTypeCode (type: CodedValueType)	[1..1]	Describes the identifier that is contained in Participant Object ID. Values may be drawn from those listed in RFC 3881 and DCID (404), as specified in the individual message descriptions.	No further refinement. To be used as specified in the IHE actor audit message requirements specified within the IHE integration profiles.
ParticipantObjectName (type: xs:token) Or ParticipantObjectQuery (type: xs:base64Binary)	[1..1]	An instance-specific descriptor of the Participant Object ID audited, such as a person's name. Or The actual query for a query-type participant object. Usage refined by individual message descriptions	No further refinement. To be used as specified in the IHE actor audit message requirements specified within the IHE integration profiles.

Element Name	Card.	Original descriptions	Swiss National Extension
ParticipantObjectDetail (type: ValuePair)	[0..*]	Implementation-defined data about specific details of the object accessed or used. Used as defined in RFC 3881. Note 1: The value field is xs:base64Binary encoded, making this attribute suitable for conveying binary data. Note 2: optional details, these can be extensive and large.	No further refinement. To be used as specified in the IHE actor audit message requirements specified within the IHE integration profiles.
ParticipantObjectDescription (type: xs:token)	[0..*]	Optional descriptive text	No further refinement. When used, it MUST be specified in the preferred language by the patient / citizen (see also chapter 1.4.2.1 on page 8).
DICOMObjectDescriptionContents	[0..1]	These are extensions made by DICOM to RFC-3881 schema for use describing DICOM objects. See descriptions for group DICOMObjectDescriptionContents.	
CodedValueType			
@csd-code (type: xs:token)	[1..1]	N/A	The code MUST be unique within the OID specified with @codeSystemName.
other-csd-attributes	N/A	See descriptions for attribute group other-csd-attributes	
other-csd-attributes			
@codeSystemName (type: xs:token)	[1..1]	codeSystemName is either an OID or String. OID pattern="[0-2]((\.0)|(\.[1-9][0-9]*))*"	An OID MUST be used.
@displayName (type: xs:token)	[0..1]	N/A	The name of the code system specified by the OID must be specified in the patient's preferred language. It MUST be a valuable translation of the original OID description in the ISO/IEC 9834-1 registration authority.
@originalText (type: xs:token)	[0..1]	Note: this also corresponds to DICOM "Code Meaning"	The name of the element must be specified in the patient's preferred language. It MUST be a valuable translation of the element's original text.
DICOMObjectDescriptionContents			
MPPS	[0..*]	DICOM extension. An MPPS Instance UID(s) associated with this participant object.	No further refinement.
Accession	[0..*]	DICOM extension. An Accession Number(s) associated with this participant object.	No further refinement.
SOPClass	[1..1]	DICOM extension. The UIDs of SOP classes referred to in this participant object. Required if ParticipantObjectIDTypeCode is (110180, DCM, "Study Instance UID")	No further refinement.

Element Name	Card.	Original descriptions	Swiss National Extension
		and any of the optional fields (AccessionNumber, ContainsMPPS, NumberOfInstances, ContainsSOPInstances,Encrypted, Anonymized) are present in this Participant Object. May be present if ParticipantObjectIDTypeCode is (110180, DCM, "Study Instance UID") even though none of the optional fields are present.	
ParticipantObjectContainsStudy	[0..1]	DICOM extension. A Study Instance UID, which may be used when the ParticipantObjectIDTypeCode is not (110180, DCM, "Study Instance UID").	No further refinement.
Encrypted	[0..1]	DICOM extension. A single value of True or False indicating whether or not the data was encrypted. Note: If there was a mix of encrypted and non-encrypted data, then create two event reports.	No further refinement.

Element Name	Card.	Original descriptions	Swiss National Extension
Anonymized	[0..1]	DICOM extension. A single value of True or False indicating whether or not all patient identifying information was removed from the data.	No further refinement.

See also Appendix A – AuditMessage schema starting on page 45.

1.4.4.2 ATNA Audit Trail Document Format

Following the Swiss regulations, any patient has the right to access the audit trail of his own EPD. While the audit trails are stored in multiple Audit Record Repositories in multiple communities, the purpose of the ATNA Audit Trail Document Format is to combine all Audit Trail entries of all Documents returned by Registry Stored Queries [ITI-18] that used the parameters described in chapter "1.4.3.1.1 Parameters for stored query FindDocuments" on page 10 into one single document. Detailed contents to be provided by all ATNA Audit Record Repository actors within the Swiss EPD circle of trust are described in the following chapter.

1.4.4.2.1 Detailed AuditTrail definitions

Table 3: Detailed AuditTrail definitions

Element Name	Card.	Description
AuditTrail [1..1] (root element)		
AuditMessage	[1..*]	An AuditTrail consist of one to many AuditMessage elements. See chapter "1.4.4.1.1 Detailed AuditMessage definitions" starting on page 14.

See also Appendix B – AuditTrail schema on page 52.

1.4.5 Translations

This chapter specifies the translations in German, French and Italien. These translations MUST be while presenting the audit trail to the user. Other translations are optional (see also chapter 1.4.2.1 on page 8).

1.4.5.1 EventActionCode

Table 4: Translations for EventActionCode

Code	English	German	French	Italian
C	Create	Erstellen	<*TODO*>	<*TODO*>
R	Read	Lesen	<*TODO*>	<*TODO*>
U	Update	Aktualisieren	<*TODO*>	<*TODO*>
D	Delete	Löschen	<*TODO*>	<*TODO*>
E	Execute	Ausführen	<*TODO*>	<*TODO*>

1.4.5.2 EventOutcomeIndicator

Table 5: Translations for EventOutcomeIndicator

Code	English	German	French	Italian
0	Nominal Success	Erfolgreich	<*TODO*>	<*TODO*>
4	Minor failure	Fehlgeschlagen	<*TODO*>	<*TODO*>
8	Serious failure	Schwerwiegender Fehler	<*TODO*>	<*TODO*>
12	Major failure	Fataler Fehler	<*TODO*>	<*TODO*>

1.4.5.3 NetworkAccessPointTypeCode

Table 6: Translations for NetworkAccessPointTypeCode

Code	English	German	French	Italian
1	Machine Name	Gerätename	*<TODO>*	*<TODO>*
2	IP Address	IP-Adresse	*<TODO>*	*<TODO>*
3	Telephone Number	Telefonnummer	*<TODO>*	*<TODO>*
4	Email address	e-Mail Adresse	*<TODO>*	*<TODO>*
5	URI	URI	URI	URI

1.4.5.4 AuditSourceIdentification code

Table 7: Translations for AuditSourceIdentification code

Code	English	German	French	Italian
1	End-user display device, diagnostic device	*<TODO>*	*<TODO>*	*<TODO>*
2	Data acquisition device or instrument	*<TODO>*	*<TODO>*	*<TODO>*
3	Web Server process or thread	*<TODO>*	*<TODO>*	*<TODO>*
4	Application Server process or thread	*<TODO>*	*<TODO>*	*<TODO>*
5	Database Server process or thread	*<TODO>*	*<TODO>*	*<TODO>*
6	Security server, e.g., a domain controller	*<TODO>*	*<TODO>*	*<TODO>*
7	ISO level 1-3 network component	*<TODO>*	*<TODO>*	*<TODO>*
8	ISO level 4-6 operating software	*<TODO>*	*<TODO>*	*<TODO>*
9	Other	*<TODO>*	*<TODO>*	*<TODO>*

1.4.5.5 AuditSourceTypeCode

Table 8: Translations for AuditSourceTypeCode

Code	English	German	French	Italian
1	End-user display device, diagnostic display	*<TODO>*	*<TODO>*	*<TODO>*
2	Data acquisition device or instrument	*<TODO>*	*<TODO>*	*<TODO>*
3	Web server process	*<TODO>*	*<TODO>*	*<TODO>*
4	Application server process	*<TODO>*	*<TODO>*	*<TODO>*
5	Database server process	*<TODO>*	*<TODO>*	*<TODO>*
6	Security server, e.g.,	*<TODO>*	*<TODO>*	*<TODO>*
7	ISO level 1-3 network component	*<TODO>*	*<TODO>*	*<TODO>*
8	ISO level 4-6 operating software	*<TODO>*	*<TODO>*	*<TODO>*
9	External source, other or unknown type	*<TODO>*	*<TODO>*	*<TODO>*

1.4.5.6 ParticipantObjectTypeCode

Table 9: Translations for ParticipantObjectTypeCode

Code	English	German	French	Italian
1	Person	*Person*	*<TODO>*	*<TODO>*
2	System object	Systemobjekt		
3	Organization	Organisation		
4	Other	Andere		

1.4.5.7 ParticipantObjectTypeCodeRole

Table 10: Translations for ParticipantObjectTypeCodeRole

Code	English	German	French	Italian
1	Patient	*<TODO>*	*<TODO>*	*<TODO>*
2	Location	*<TODO>*	*<TODO>*	*<TODO>*
3	Report	*<TODO>*	*<TODO>*	*<TODO>*
4	Resource	*<TODO>*	*<TODO>*	*<TODO>*

5	Master File	<*TODO*>	<*TODO*>	<*TODO*>
6	User	<*TODO*>	<*TODO*>	<*TODO*>
7	List	<*TODO*>	<*TODO*>	<*TODO*>
8	Doctor	<*TODO*>	<*TODO*>	<*TODO*>
9	Subscriber	<*TODO*>	<*TODO*>	<*TODO*>
10	Guarantor	<*TODO*>	<*TODO*>	<*TODO*>
11	Security User Entity	<*TODO*>	<*TODO*>	<*TODO*>
12	Security User Group	<*TODO*>	<*TODO*>	<*TODO*>
13	Security Resource	<*TODO*>	<*TODO*>	<*TODO*>
14	Security Granulatiry Definition	<*TODO*>	<*TODO*>	<*TODO*>
15	Provider	<*TODO*>	<*TODO*>	<*TODO*>
16	Report Destination	<*TODO*>	<*TODO*>	<*TODO*>
17	Report Library	<*TODO*>	<*TODO*>	<*TODO*>
18	Schedule	<*TODO*>	<*TODO*>	<*TODO*>
19	Customer	<*TODO*>	<*TODO*>	<*TODO*>
20	Job	<*TODO*>	<*TODO*>	<*TODO*>
21	Job Stream	<*TODO*>	<*TODO*>	<*TODO*>
22	Table	<*TODO*>	<*TODO*>	<*TODO*>
23	Routing Criteria	<*TODO*>	<*TODO*>	<*TODO*>
24	Query	<*TODO*>	<*TODO*>	<*TODO*>

1.4.5.8 ParticipantObjectDataLifeCycle

Table 11: Translations for ParticipantObjectDataLifeCycle

Code	English	German	French	Italian
1	Origination, Creation	<*TODO*>	<*TODO*>	<*TODO*>
2	Import/ Copy	<*TODO*>	<*TODO*>	<*TODO*>
3	Amendment	<*TODO*>	<*TODO*>	<*TODO*>
4	Verification	<*TODO*>	<*TODO*>	<*TODO*>
5	Translation	<*TODO*>	<*TODO*>	<*TODO*>
6	Access/Use	<*TODO*>	<*TODO*>	<*TODO*>
7	De-identification	<*TODO*>	<*TODO*>	<*TODO*>
8	Aggregation, summarization, derivation	<*TODO*>	<*TODO*>	<*TODO*>
9	Report	<*TODO*>	<*TODO*>	<*TODO*>
10	Export	<*TODO*>	<*TODO*>	<*TODO*>
11	Disclosure	<*TODO*>	<*TODO*>	<*TODO*>
12	Receipt of Disclosure	<*TODO*>	<*TODO*>	<*TODO*>
13	Archiving	<*TODO*>	<*TODO*>	<*TODO*>
14	Logical deletion	<*TODO*>	<*TODO*>	<*TODO*>
15	Permanent erasure, physical destruction	<*TODO*>	<*TODO*>	<*TODO*>

1.5 Requirements on PIXv3 for Patient Identity Feed

This section corresponds to the transaction Patient Identity Feed HL7 V3 [ITI-44] of the IHE IT Infrastructure Technical Framework. This transaction is used by the Patient Identity Source, Patient Identifier Cross-reference Manager and Document Registry Actors. With the PIXv3 Patient Identity Feed a primary system can register a local identifier within the MPI.

1.5.1 Message Semantics

1.5.1.1 Major Components of the Patient Registry Record Added/Revised Messages

PersonalRelationship
This is used for sending information pertaining to the mother's maiden name. See also IHE ITI TF-2b, chapter 3.44.4.1.2.1. In Switzerland the fathers and mothers name can be added here to.
Message Information Model
The Message Information Model for both the Patient Activate and Patient Revise messages, as it is described in IHE ITI TF-2b, Table 3.44.4.1.2-1 is further restricted for use in an MPI within the EPD on the following attributes:

Table 12 Patient Active and Revise Model Attributes

PRPA_HD201301IHE Patient Activate/Revise	**This HMD extract defines the message used to report that a new patient record was added, or a patient record was updated. Derived from Figure 3.44.4.1.2-1 (PRPA_RM201301IHE)**	**Swiss National Extension**
Patient	The primary record for the focal person in a Patient Identity Source.	
classCode [1..1] (M) Patient (CS) {CNE:PAT}	Structural attribute; this is a "patient" role.	No further refinement.
id [1..*] (M) Patient (SET<II>)	Identifiers designated by this patient identity source for the focal person.	No further refinement.
statusCode [1..1] Patient (CS) {CNE:active, fixed value= "active"}	A value specifying the state of this record in a patient registry (based on the RIM role class state-machine). This record is active.	No further refinement.
confidentialityCode [0..*] Patient (SET<CE>) {CWE:Confidentiality}	Value(s) that control the disclosure of information about this living subject as a patient.	No further refinement.
veryImportantPersonCode [0..1] Patient (CE) {CWE:PatientImportance}	A code specifying the patient's special status granted by the scoper organization, often resulting in preferred treatment and special considerations. Examples include board member, diplomat.	No further refinement.

PRPA_HD201301IHE Patient Activate/Revise	**This HMD extract defines the message used to report that a new patient record was added, or a patient record was updated. Derived from Figure 3.44.4.1.2-1 (PRPA_RM201301IHE)**	**Swiss National Extension**
Person	A subtype of LivingSubject representing a human being either Person.name or Patient.id must be non-null.	
classCode [1..1] (M) Person (CS) {CNE:PSN, fixed value= "PSN"}	Structural attribute; this is a "person" entity.	No further refinement.
determinerCode [1..1] (M) Person (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific person.	No further refinement.
name [1..*] Person (BAG<PN>)	Name(s) for this person.	The birth name is passed with the qualifier BR (HL7V3_Edition2012/infrastructure/ datatypes_r2/datatypes_r2.html#dt-DSET).
telecom [0..*] Person (BAG<TEL>)	Telecommunication address(es) for communicating with this person.	No further refinement.
administrativeGenderCode [0..1] Person (CE) {CWE:AdministrativeGender}	A value representing the gender (sex) of this person. Note: this attribute does not include terms related to clinical gender which is a complex physiological, genetic and sociological concept that requires multiple observations in order to be comprehensively described.	No further refinement.
birthTime [0..1] Person (TS)	The date and time this person was born.	No further refinement.
deceasedInd [0..1] Person (BL)	An indication that this person is dead.	No further refinement.
deceasedTime [0..1] Person (TS)	The date and time this person died.	No further refinement.
multipleBirthInd [0..1] Person (BL)	An indication that this person was part of a multiple birth.	No further refinement.
multipleBirthOrderNumber [0..1] Person (INT)	The order in which this person was born if part of a multiple birth.	No further refinement.
addr [0..*] Person (BAG<AD>)	Address(es) for corresponding with this person.	No further refinement.
maritalStatusCode [0..1] Person (CE) {CWE:MaritalStatus}	A value representing the domestic partnership status of this person.	No further refinement.
religiousAffiliationCode [0..1] Person (CE) {CWE:ReligiousAffiliation}	A value representing the primary religious preference of this person.	MUST NOT be used.
raceCode [0..*] Person (SET<CE>) {CWE:Race}	A set of values representing the races of this person.	MUST NOT be used.
ethnicGroupCode [0..*] Person (SET<CE>) {CWE:Ethnicity}	A set of values representing the ethnic groups of this person.	MUST NOT be used.

PRPA_HD201301IHE Patient Activate/Revise	**This HMD extract defines the message used to report that a new patient record was added, or a patient record was updated. Derived from Figure 3.44.4.1.2-1 (PRPA_RM201301IHE)**	**Swiss National Extension**
OtherIDs	Used to capture additional identifiers for the person such as a Drivers' license or Social Security Number. Please see notes above in the Major Components section on the use of OtherIDs.	If patient is already registered in a community, the MPI-PID MUST be provided here. The EPD-PID MAY be added here.
classCode [1..1] (M) Role (CS) {CNE:ROL}	Structural attribute. This can be any specialization of "role" except for Citizen, or Employee.	No further refinement.
id [1..*] (M) Role (SET<II>)	One or more identifiers issued to the focal person by the associated scopingOrganization (e.g., a Driver's License number issued by a DMV).	No further refinement.
PersonalRelationship	A personal relationship between the focal living subject and another living subject.	
classCode [1..1] (M) Role (CS) {CNE:PRS, fixed value= "PRS"}	Structural attribute; this is a "personal relationship" role.	No further refinement.
id [0..*] Role (SET<II>)	Identifier(s) for this personal relationship.	No further refinement.
code [1..1] (M) Role (CE) {CWE:PersonalRelationshipRoleType}	A required value specifying the type of personal relationship between the relationshipHolder and the scoping living subject drawn from the PersonalRelationshipRoleType domain, for example, spouse, parent, unrelated friend.	No further refinement. Codes: FTH: Father MTH: Mother
statusCode [0..1] Role (CE) {CWE:RoleStatus}	A value specifying the state of this personal relationship (based on the RIM Role class state-machine), for example, following divorce a spouse relationship would be "terminated".	No further refinement.
effectiveTime [0..1] Role (IVL<TS>)	An interval of time specifying the period during which this personal relationship is in effect, if such time is applicable and known.	No further refinement.
Citizen	Used to capture person information relating to citizenship.	
classCode [1..1] (M) Role (CS) {CNE:CIT, fixed value= "CIT"}	Structural attribute; this is a "citizen" role.	No further refinement.
id [0..*] Role (SET<II>)	Identifier(s) for the focal person as a citizen of a nation.	No further refinement.
effectiveTime [0..1] Employee (IVL<TS>)	An interval of time specifying the period during which this employment relationship is in effect, if such time limit is applicable and known.	No further refinement.
Nation	A politically organized body of people bonded by territory and known as a nation.	
classCode [1..1] (M) Organization (CS) {CNE:NAT, fixed value= "NAT"}	Structural attribute; this is a 'nation' type of entity.	No further refinement.
determinerCode [1..1] (M) Organization (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific entity.	No further refinement.
code [1..1] (M) Organization (CD) {CWE:NationEntityType}	A value that identifies a nation state.	No further refinement.
name [0..1]	A non-unique textual identifier or moniker for this	No further refinement.

PRPA_HD201301IHE Patient Activate/Revise	**This HMD extract defines the message used to report that a new patient record was added, or a patient record was updated. Derived from Figure 3.44.4.1.2-1 (PRPA_RM201301IHE)**	**Swiss National Extension**
Organization (ON)	nation.	
Employee	A relationship of the focal person with an organization to receive wages or salary. The purpose of this class is to identify the type of relationship the employee has to the employer rather than the nature of the work actually performed. For example, it can be used to capture whether the person is a Military Veteran or not.	
classCode [1..1] (M) Employee (CS) {CNE:EMP}	Structural attribute; this is an "employee" role.	No further refinement.
statusCode [0..1] Employee (CS) {CNE:RoleStatus}	A value specifying the state of this employment relationship (based on the RIM Role class state-machine), for example, active, suspended, terminated.	No further refinement.
statusCode [0..1] Employee (CS) {CNE:RoleStatus}	A value specifying the state of this employment relationship (based on the RIM Role class state-machine), for example, active, suspended, terminated.	No further refinement.
effectiveTime [0..1] Employee (IVL<TS>)	An interval of time specifying the period during which this employment relationship is in effect, if such time limit is applicable and known.	No further refinement.
occupationCode [0..1] Employee (CE) {CWE:EmployeeOccupationCode}	A code qualifying the classification of kind-of-work based upon a recognized industry or jurisdictional standard. OccupationCode is used to convey the person's occupation as opposed to jobClassCode (not used in this transaction) which characterizes this particular job. For example, it can be used to capture whether the person is a Military Veteran or not.	No further refinement.
BirthPlace	The birthplace of the focal living subject.	
classCode [1..1] (M) Birthplace (CS) {CNE:BIRTHPL}	Structural attribute; this is a "birthplace" role.	No further refinement.
id [0..*] Birthplace (SET<II>)	A living subject's birth place represented by a unique identifier.	No further refinement.
addr [0..*] Patient (BAG<AD>)	A living subject's birth place represented as an address. Note: Either BirthPlace.addr or an associated Place.name must be valued.	No further refinement.
classCode [1..1] (M) Birthplace (CS) {CNE:BIRTHPL}	Structural attribute; this is a "birthplace" role	No further refinement.
LanguageCommunication	A language communication capability of the focal person	
languageCode [1..1] (M) LanguageCommunication (CE) {CWE:HumanLanguage}	A value representing a language for which the focal person has some level of proficiency for written or spoken communication. Examples: Spanish, Italian, German, English, American Sign.	No further refinement.
preferenceInd [0..1] LanguageCommunication (BL)	An indicator specifying whether or not this language is preferred by the focal person for the associated mode.	No further refinement.

1.6 Requirements on PIXv3 Profile for Patient Identifier Cross-reference Query

This section corresponds to transaction PIXv3 Query [ITI-45] of the IHE IT Infrastructure Technical Framework. This transaction is used by the Patient Identifier Cross-reference Consumer and Patient Identifier Cross-reference Manager Actors. With the PIXv3 Query a primary system can query with the local identifier the MPI and get the corresponding MPI-PID and the EPD-PID.

1.6.1 Message Semantics

1.6.1.1 Major Components of the Patient Registry Query by Identifier

DataSource Parameter
This parameter specifies the assigning authority/authorities of the Patient Identity Domain(s) whose identifiers need to be returned. The DataSource Parameter MUST be specified to the assigning authority/authorities of the MPI-PID in the affinity domain. See also ITI TF-2b, chapter 3.45.4.1.2.1

1.6.2 Return Corresponding Identifiers

1.1.1.1 Major Components of the Get Corresponding Identifiers Query Response

The otherId MUST contain the EPD-PID. See also ITI TF-2b, chapter 3.45.4.2.2.1

1.7 Requirements on PDQv3 Profile for Patient Demographics Query

This section corresponds to Patient Demographics Query HL7 V3 transaction [ITI-47] of the IHE Technical Framework. This transaction is used by the Patient Demographics Consumer and Patient Demographics Supplier Actors.

1.7.1 Message Semantics

1.7.1.1 Major Components of the Patient Registry Query by Demographics

The PatientTelecom Query Parameter MUST NOT be used.

1.7.1.1.1 Additional components for the Swiss National Extension

MothersName Parameter
This optional parameter specifies the name of the mother of the person whose information is being queried. For this parameter item, a single person name (PN) data item shall be specified in the Person.value attribute. Within the PN data type, the given name and family name may be specified. If the sender needs to indicate that the name parts specified are not limited to an exact match, then the use attribute of the value element shall be set to "SRCH".

FathersName Parameter
This optional parameter specifies the name of the father of the person whose information is being queried. For this parameter item, a single person name (PN) data item shall be specified in the Person.value attribute. Within the PN data type, the given name and family name may be specified. If the sender needs to indicate that the name parts specified are not limited to an exact match, then the use attribute of the value element shall be set to "SRCH".

1.7.1.2 Message Information Model

The Message Information Model for both the Patient Activate and Patient Revise messages is described in IHE ITI TF-2b, Table 3.47.4.1.2-1. Within the Swiss national extensions the following sections MAY additionally be included:

Table 13: Patient Demographics Query – Swiss national extension sections

PRPA_HD201306IHE Patient Registry Query by Demographics	**This HMD extract defines the message used to query a patient registry for records matching a set of demographics information.** **Derived from Figure 3.47.4.1.2-1 (PRPA_RM201306IHE)**	**Swiss National Extension**
MothersName	N/A	Design Comments: This query parameter is the name of a focal person's mother. It is included as a parameter because it is a common attribute for confirming the identity of persons in some registries. This parameter does not map to a single RIM attribute, instead, in RIM terms Mother's name is the person name part of "family" for the person who is the player in a PersonalRelationship of type of "mother" to the focal person.
value [1..1] ParameterItem (PN)	N/A	Design Comments: A person name. In this case it may consist of only the given name part, the family name part, or both.
semanticsText [1..1] ParameterItem (ST) {default= "Person.MotherName"}	N/A	These static values MUST be used.
FathersName	N/A	Design Comments: This query parameter is the name of a focal person's father. It is included as a parameter because it is a common attribute for confirming the identity of persons in some registries. This parameter does not map to a single RIM attribute, instead, in RIM terms Father's name is the person name part of "family" for the person who is the player in a PersonalRelationship of type of "father" to the focal person.
value [1..1] ParameterItem (PN)	N/A	Design Comments: A person name. In this case it may consist of only the given name part, the family name part, or both.
semanticsText [1..1] ParameterItem (ST){default= "Person.Father.Name"}	N/A	These static values MUST be used.

1.7.2 Patient Demographics Query Response

1.7.2.1 Expected Actions

The Patient Demographics Supplier shall perform the matching of patient data based on the query parameter values it receives. The information provided by the Patient Demographics Supplier to Patient Demographics Consumers is a list of possible matching patients from the patient information source associated with the value that the Consumer sent in the Device class of the transmission wrapper of the query message. See also IHE ITI TF-2b, chapter 3.47.4.2.3.
The Message Information Model for both the Patient Registry Find Candidates Response messages, as it is described in IHE ITI TF-2b, Table 3.47.4.2.2-8: is further restricted for use in an MPI within the EPD on the following attributes:

Table 14: Message Information Model for Patient Registry Find Candidates

PRPA_HD201310IHE Patient Registry Find Candidates Response	**This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query. Derived from Figure 3.47.4.2.2-1 (PRPA_RM201310IHE)**	**Swiss National Extension**
Patient	The primary record for the focal person in a Patient Demographics Supplier.	
classCode [1..1] (M) Patient (CS) {CNE:PAT}	Structural attribute; this is a "patient" role.	No further refinement.
id [1..*] (M) Patient (SET<II>)	Patient identifiers. Patient Identifiers from different Identity Domains may be contained either here, or in the OtherIDs.id attributes, but not in both places. At least one Patient Identifier shall be present in this attribute.	No further refinement. Note: The EPD-PID should be added in OtherIDs.id.
statusCode [1..1] Patient (CS) {CNE:active, fixed value= "active"}	A value specifying the state of this record in a patient registry (based on the RIM role class state-machine). This record is active.	No further refinement.
confidentialityCode [0..*] Patient (SET<CE>) {CWE:Confidentiality}	Value(s) that control the disclosure of information about this living subject as a patient.	No further refinement.
veryImportantPersonCode [0..1] Patient (CE) {CWE:PatientImportance}	A code specifying the patient's special status granted by the scoper organization, often resulting in preferred treatment and special considerations. Examples include board member, diplomat.	No further refinement.
Person	A subtype of LivingSubject representing a human being either Person.name or Patient.id must be non-null.	
classCode [1..1] (M) Person (CS) {CNE:PSN, fixed value= "PSN"}	Structural attribute; this is a "person" entity.	No further refinement.
determinerCode [1..1] (M) Person (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific person.	No further refinement.
name [1..*] Person (BAG<PN>)	Name(s) for this person.	The birth name is passed with the qualifier BR (HL7V3_Edition2012/ infrastructure/datatypes_r2/ datatypes_r2.html#dt-DSET).
telecom [0..*] Person (BAG<TEL>)	Telecommunication address(es) for communicating with this person.	No further refinement.
administrativeGenderCode [0..1] Person (CE) {CWE:AdministrativeGender}	A value representing the gender (sex) of this person. Note: this attribute does not include terms related to clinical gender which is a complex physiological, genetic and sociological concept that requires multiple observations in order to be comprehensively described.	No further refinement.
birthTime [0..1] Person (TS)	The date and time this person was born.	No further refinement.
deceasedInd [0..1] Person (BL)	An indication that this person is dead.	No further refinement.
deceasedTime [0..1] Person (TS)	The date and time this person died.	No further refinement.
multipleBirthInd [0..1] Person (BL)	An indication that this person was part of a multiple birth.	No further refinement.
multipleBirthOrderNumber [0..1] Person (INT)	The order in which this person was born if part of a multiple birth.	No further refinement.
addr [0..*] Person (BAG<AD>)	Address(es) for corresponding with this person.	No further refinement.
maritalStatusCode [0..1] Person (CE) {CWE:MaritalStatus}	A value representing the domestic partnership status of this person.	No further refinement.
religiousAffiliationCode [0..1] Person (CE) {CWE:ReligiousAffiliation}	A value representing the primary religious preference of this person.	MUST NOT be used.

PRPA_HD201310IHE **Patient Registry Find Candidates Response**	**This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query.** **Derived from Figure 3.47.4.2.2-1 (PRPA_RM201310IHE)**	**Swiss National Extension**
raceCode [0..*] Person (SET<CE>) {CWE:Race}	A set of values representing the races of this person.	MUST NOT be used.
ethnicGroupCode [0..*] Person (SET<CE>) {CWE:Ethnicity}	A set of values representing the ethnic groups of this person.	MUST NOT be used.
OtherIDs	Used to capture additional identifiers for the person such as a Drivers' license or Social Security Number.	The EPD-PID MAY be added here.
classCode [1..1] (M) Role (CS) {CNE:ROL}	Structural attribute. This can be any specialization of "role" except for Citizen, or Employee.	No further refinement.
id [1..*] (M) Role (SET<II>)	One or more identifiers issued to the focal person by the associated scopingOrganization (e.g., identifiers from a different Patient Identity Domain).	No further refinement.
PersonalRelationship	A personal relationship between the focal living subject and another living subject.	
classCode [1..1] (M) Role (CS) {CNE:PRS, fixed value= "PRS"}	Structural attribute; this is a "personal relationship" role.	No further refinement.
id [0..*] Role (SET<II>)	Identifier(s) for this personal relationship.	No further refinement.
code [1..1] (M) Role (CE) {CWE:PersonalRelationshipRoleType}	A required value specifying the type of personal relationship between the relationshipHolder and the scoping living subject drawn from the PersonalRelationshipRoleType domain, for example, spouse, parent, unrelated friend.	No further refinement. Codes: FTH: Father MTH: Mother
Citizen	Used to capture person information relating to citizenship.	
classCode [1..1] (M) Role (CS) {CNE:CIT, fixed value= "CIT"}	Structural attribute; this is a "citizen" role.	No further refinement.
id [0..*] Role (SET<II>)	Identifier(s) for the focal person as a citizen of a nation.	No further refinement.
Nation	A politically organized body of people bonded by territory and known as a nation.	
classCode [1..1] (M) Organization (CS) {CNE:NAT, fixed value= "NAT"}	Structural attribute; this is a 'nation' type of entity.	No further refinement.
determinerCode [1..1] (M) Organization (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific entity.	No further refinement.
code [1..1] (M) Organization (CD) {CWE:NationEntityType}	A value that identifies a nation state.	No further refinement.
name [0..1] Organization (ON)	A non-unique textual identifier or moniker for this nation.	No further refinement.

PRPA_HD201310IHE **Patient Registry Find Candidates Response**	**This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query.** **Derived from Figure 3.47.4.2.2-1 (PRPA_RM201310IHE)**	**Swiss National Extension**
Employee	A relationship of the focal person with an organization to receive wages or salary. The purpose of this class is to identify the type of relationship the employee has to the employer rather than the nature of the work actually performed. For example, it can be used to capture whether the person is a Military Veteran or not.	
classCode [1..1] (M) Employee (CS) {CNE:EMP}	Structural attribute; this is an "employee" role.	No further refinement.
statusCode [0..1] Employee (CS) {CNE:RoleStatus}	A value specifying the state of this employment relationship (based on the RIM Role class state-machine), for example, active, suspended, terminated.	No further refinement.
occupationCode [0..1] Employee (CE) {CWE:EmployeeOccupationCode}	A code qualifying the classification of kind-of-work based upon a recognized industry or jurisdictional standard. OccupationCode is used to convey the person's occupation as opposed to jobClassCode (not used in this transaction) which characterizes this particular job. For example, it can be used to capture whether the person is a Military Veteran or not.	No further refinement.
LanguageCommunication	A language communication capability of the focal person.	
languageCode [1..1] (M) LanguageCommunication (CE) {CWE:HumanLanguage}	A value representing a language for which the focal person has some level of proficiency for written or spoken communication. Examples: Spanish, Italian, German, English, American Sign.	No further refinement.
preferenceInd [0..1] LanguageCommunication (BL)	An indicator specifying whether or not this language is preferred by the focal person for the associated mode.	No further refinement.
QueryMatchObservation	Used to convey information about the quality of the match for each record.	
classCode [1..1] (M) Observation (CS) {CNE:http://hl7.org/v3ballot2007may/html/infrastructure/vocabulary/ActClass.htm - ActClass, default= "OBS"}	Structural attribute – this is an observation.	No further refinement.
moodCode [1..1] (M) Observation (CS) {CNE:http://hl7.org/v3ballot2007may/html/infrastructure/vocabulary/ActMood.htm - ActMood, default= "EVN"}	Structural attribute – this is an event.	No further refinement.
code [1..1] (M) Observation (CD) {CWE:QueryMatchObservationType}	A code, identifying this observation as a query match observation.	No further refinement.
value [1..1] (M) QueryMatchObservation (INT)	A numeric value indicating the quality of match for this record. It shall correspond to the MinimumDegreeMatch.value attribute of the original query, and it shall have the same meaning (e.g., percentage, indicating confidence in the match).	No further refinement.

1.7.2.1.1 Special handling for more attributes requested

If there are more than 5 matches zero matches a special handling like in the XCPD transaction (see IHE ITI TF-2b, chapter 3.55.4.2.2.6) is necessary.
The Responding Gateway has the option of informing the Initiating Gateway when additional demographic attributes may result in a match. This would most often be used in cases where the security and privacy policies do not allow release of patient data unless and until there is a level of assurance that the same patient is referenced. In this case the Responding Gateway cannot return a matching patient or patients because the level of assurance is not great enough. If the Initiating Gateway was able to specify further demographic attributes the Responding Gateway might have

greater assurance of the match and thus be able to return the match information.
To indicate this situation in its response the Responding Gateway codes a DetectedIssueEvent within the controlActProcess element, where the code in the actOrderRequired element references one of the coded elements described in Table 15 . There may be as many triggerFor elements, each of them containing an ActOrderRequired element, as needed to code the attributes which would increase the assurance of the match. The codeSystem for these code elements is <*TODO oid to be registered*> instead of 1.3.6.1.4.1.19376.1.2.27.1 as described in IHE ITI TF-2b, Table 3.55.4.4.2-4.

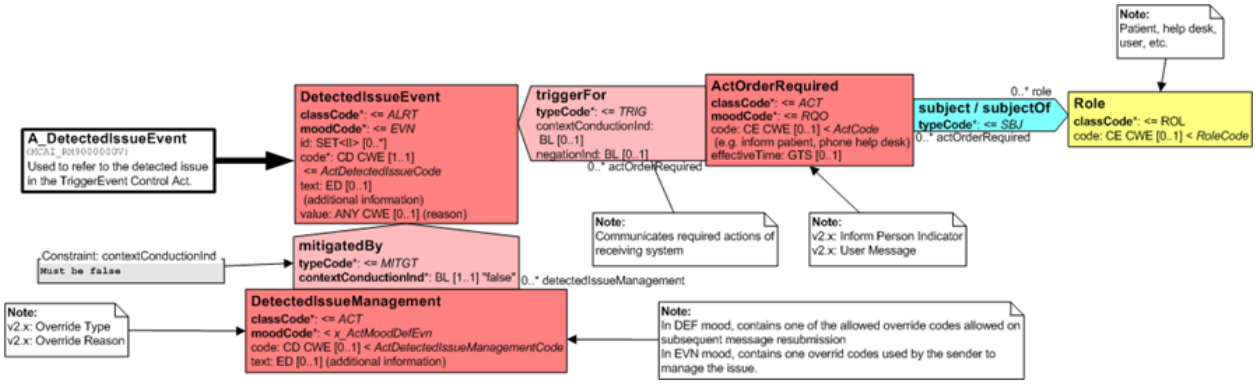


Figure 5: XCPD – RMIM for DetectedIssueEvent

Table 15: Coded Values for actOrderRequired code (codeSystem=<*TODO oid to be registered*>)

Value for code	Meaning of code
LivingSubjectAdministrativeGenderRequested	Requests the LivingSubjectAdministrativeGender attribute be specified
PatientAddressRequested	Requests the PatientAddress attribute be specified
LivingSubjectBirthPlaceNameRequested	Requests the LivingSubjectBirthPlaceName attribute be specified
BirthNameRequested	Requests the Birth Name attribute be specified
MothersNameRequested	Requests the Mothers Name attribute be specified
FahtersNameRequested	Requests the Fathers Name attribute be specified

The following example shows part of a response requesting the PatientAddress and PatientTelecom attributes.

```
<detectedIssueEvent classCode="ALRT" moodCode="EVN">
 <code code="ActAdministrativeDetectedIssueCode"
codeSystem="2.16.840.1.113883.5.4"/>
 <triggerFor typeCode="TRIG">
 <actOrderRequired classCode="ACT" moodCode="RQO">
  <code code="PatientAddressRequested" codeSystem="<TODO>" />
 </actOrderRequired>
 </triggerFor>
 <triggerFor typeCode="TRIG">
 <actOrderRequired classCode="ACT" moodCode="RQO">
  <code code=" LivingSubjectAdministrativeGenderRequested" codeSystem="<TODO>"/>
 </actOrderRequired>
 </triggerFor>
</detectedIssueEvent>
```

The different return cases should be handled equivalent to the XCPD cases in IHE ITI TF-2b, chapter 3.55.4.2.3 Expected Actions.

1.8 Requirements on XCPD Profile for Cross-Community Patient Discovery

XCPD is used in Switzerland for resolving the national patient identifier (EPD-PID) into the community identifiers (MPI-PID) in another affinity domain/community. The Query can either return an exact match or no match.

1.8.1 Modes and Options

The Cross Gateway Patient Discovery transaction [ITI-55] has several modes. For the EPD only the Shared/National Patient Identifier Query mode MUST be used. Other modes as defined in this transaction (see also IHE ITI TF-2b, chapter 3.55.1) MUST NOT be used.
The Health Data Locator and Revoke Option of the Patient Location Query transaction [ITI-56] MUST NOT be used.[5]

1.8.2 Cross Gateway Patient Discovery Request

Caching
The Initiating Gateway may specify a duration value in the SOAP Header element of the request. This value suggests to the Responding Gateway a length of time that the Initiating Gateway recommends caching any correlation resulting from the interaction. This values MUST NOT exceed 3 days. See also IHE ITI TF-2b, chapter 3.55.4.1.

1.8.2.1 Major Components of the Patient Registry Query by Demographics

LivingSubjectId Parameter is the only allowed query Parameter. All other parameter in IHE ITI TF-2b, chapter 3.55.4.1.2.1 MUST NOT be used.
The LivingSubjectId Parameter MUST contain the EPD-PID.
Reverse Cross-Gateway Queries
Reverse Cross-Gateway Queries MUST NOT be used (see IHE ITI TF-2b, chapter 3.55.4.1.2.4).

1.8.3 Cross Gateway Patient Discovery Response

Caching
The Responding Gateway may specify a duration value in the SOAP Header element of the response. This value suggests to the Initiating Gateway a length of time that the Responding Gateway recommends caching any correlation resulting from the interaction. This values MUST NOT exceed 3 days. See also IHE ITI TF-2b, chapter 3.55.4.2.

1.8.3.1 Major Components of the Patient Registry Find Candidates Response Message

The QueryMatchObservation class is used to convey information about the quality of the match for the record returned by the query response. This value MUST state 100 for an exact match.
The Message Information Model for the Patient Registry Find Candidates Response message is further restricted within the EPD:

Table 16: Message Information Model for Patient Registry Find Candidates

[5] http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCPD_HDL_Revoke_Option.pdf

PRPA_HD201310IHE **Patient Registry Find Candidates Response**	**This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query.** **Derived from Figure 3.55.4.2.2-1 (PRPA_RM201310IHE)**	**Swiss National Extension**
Patient	The primary record for the focal person.	
classCode [1..1] (M) Patient (CS) {CNE:PAT}	Structural attribute; this is a "patient" role.	No further refinement.
id [1..1] (M) Patient (SET<II>)	The Patient Identifier to be used in subsequent XCA Cross Gateway Query transactions related to this patient when sent to the Responding Gateway sending the response. All other patient identifiers shall be specified in the OtherIDs.id attribute.	The MPI-PID MUST be returned if there is a match from the EPD-PID.
statusCode [1..1] Patient (CS) {CNE:active, fixed value= "active"}	A value specifying the state of this record in a patient registry (based on the RIM role class state-machine). This record is active.	No further refinement.
confidentialityCode [0] Patient (SET<CE>) {CWE:Confidentiality}	Value(s) that control the disclosure of information about this living subject as a patient.	MUST NOT be used.
veryImportantPersonCode [0] Patient (CE) {CWE:PatientImportance}	A code specifying the patient's special status granted by the scoper organization, often resulting in preferred treatment and special considerations. Examples include board member, diplomat.	MUST NOT be used.
Person	A subtype of LivingSubject representing a human being either Person.name or Patient.id must be non-null.	
classCode [1..1] (M) Person (CS) {CNE:PSN, fixed value= "PSN"}	Structural attribute; this is a "person" entity.	No further refinement.
determinerCode [1..1] (M) Person (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific person.	No further refinement.
name [1] Person (BAG<PN>) {null, fixed value nullFlavor="NA"}	Name(s) for this person. Fixed to be null, <name nullFlavor="NA"/>, request contains only a patient identifier and no demographic data.	No further refinement.
telecom [0] Person (BAG<TEL>)	Telecommunication address(es) for communicating with this person.	MUST NOT be used.
administrativeGenderCode [0] Person (CE) {CWE:AdministrativeGender}	A value representing the gender (sex) of this person. Note: this attribute does not include terms related to clinical gender which is a complex physiological, genetic and sociological concept that requires multiple observations in order to be comprehensively described.	MUST NOT be used.
birthTime [0] Person (TS)	The date and time this person was born.	MUST NOT be used.
deceasedInd [0] Person (BL)	An indication that this person is dead.	MUST NOT be used.
deceasedTime [0] Person (TS)	The date and time this person died.	MUST NOT be used.

PRPA_HD201310IHE **Patient Registry Find Candidates Response**	**This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query.** **Derived from Figure 3.55.4.2.2-1 (PRPA_RM201310IHE)**	**Swiss National Extension**
multipleBirthInd [0] Person (BL)	An indication that this person was part of a multiple birth.	MUST NOT be used.
multipleBirthOrderNumber [0] Person (INT)	The order in which this person was born if part of a multiple birth.	MUST NOT be used.
addr [0] Person (BAG<AD>)	Address(es) for corresponding with this person.	MUST NOT be used.
maritalStatusCode [0] Person (CE) {CWE:MaritalStatus}	A value representing the domestic partnership status of this person.	MUST NOT be used.
religiousAffiliationCode [0] Person (CE) {CWE:ReligiousAffiliation}	A value representing the primary religious preference of this person.	MUST NOT be used.
raceCode [0] Person (SET<CE>) {CWE:Race}	A set of values representing the races of this person.	MUST NOT be used.
ethnicGroupCode [0] Person (SET<CE>) {CWE:Ethnicity}	A set of values representing the ethnic groups of this person.	MUST NOT be used.
OtherIDs	Used to capture additional identifiers for the person such as a Drivers' license or Social Security Number.	
classCode [1..1] (M) Role (CS) {CNE:ROL}	Structural attribute. This can be any specialization of "role" except for Citizen, or Employee.	MUST NOT be used
id [1] (M) Role (SET<II>)	One or more identifiers issued to the focal person by the associated scopingOrganization (e.g., identifiers from a different Patient Identity Domain).	MUST NOT be used.
PersonalRelationship	A personal relationship between the focal living subject and another living subject.	
classCode [1..1] (M) Role (CS) {CNE:PRS, fixed value= "PRS"}	Structural attribute; this is a "personal relationship" role.	MUST NOT be used.
id [0..*] Role (SET<II>)	Identifier(s) for this personal relationship.	MUST NOT be used.
code [1..1] (M) Role (CE) {CWE:PersonalRelationshipRoleType}	A required value specifying the type of personal relationship between the relationshipHolder and the scoping living subject drawn from the PersonalRelationshipRoleType domain, for example, spouse, parent, unrelated friend.	MUST NOT be used.
Citizen	Used to capture person information relating to citizenship.	
classCode [1..1] (M) Role (CS) {CNE:CIT, fixed value= "CIT"}	Structural attribute; this is a "citizen" role.	MUST NOT be used.
id [0..*] Role (SET<II>)	Identifier(s) for the focal person as a citizen of a nation.	MUST NOT be used.
Nation	A politically organized body of people bonded by territory and known as a nation.	
classCode [1..1] (M) Organization (CS) {CNE:NAT, fixed value= "NAT"}	Structural attribute; this is a 'nation' type of entity.	MUST NOT be used.
determinerCode [1..1] (M) Organization (CS) {CNE:INSTANCE, fixed value= "INSTANCE"}	Structural attribute; this is a specific entity.	MUST NOT be used.

PRPA_HD201310IHE **Patient Registry Find Candidates Response**	**This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query.** **Derived from Figure 3.55.4.2.2-1 (PRPA_RM201310IHE)**	**Swiss National Extension**
code [1..1] (M) Organization (CD) {CWE:NationEntityType}	A value that identifies a nation state.	MUST NOT be used.
name [0..1] Organization (ON)	A non-unique textual identifier or moniker for this nation.	MUST NOT be used.
Employee	A relationship of the focal person with an organization to receive wages or salary. The purpose of this class is to identify the type of relationship the employee has to the employer rather than the nature of the work actually performed. For example, it can be used to capture whether the person is a Military Veteran or not.	
classCode [1..1] (M) Employee (CS) {CNE:EMP}	Structural attribute; this is an "employee" role.	MUST NOT be used.
statusCode [0..1] Employee (CS) {CNE:RoleStatus}	A value specifying the state of this employment relationship (based on the RIM Role class state-machine), for example, active, suspended, terminated.	MUST NOT be used.
occupationCode [0..1] Employee (CE) {CWE:EmployeeOccupationCode}	A code qualifying the classification of kind-of-work based upon a recognized industry or jurisdictional standard. OccupationCode is used to convey the person's occupation as opposed to jobClassCode (not used in this transaction) which characterizes this particular job. For example, it can be used to capture whether the person is a Military Veteran or not.	MUST NOT be used.
LanguageCommunication	A language communication capability of the focal person.	
languageCode [1..1] (M) LanguageCommunication (CE) {CWE:HumanLanguage}	A value representing a language for which the focal person has some level of proficiency for written or spoken communication. Examples: Spanish, Italian, German, English, American Sign.	MUST NOT be used.
preferenceInd [0..1] LanguageCommunication (BL)	An indicator specifying whether or not this language is preferred by the local person for the associated mode.	MUST NOT be used.
QueryMatchObservation	Used to convey information about the quality of the match for each record.	
classCode [1..1] (M) Observation (CS) {CNE:http://hl7.org/v3ballot2007may/html/infrastructure/vocabulary/ActClass.htm - ActClass, default= "OBS"}	Structural attribute – this is an observation.	No further refinement.

PRPA_HD201310IHE **Patient Registry Find Candidates Response**	**This HMD extract defines the message used to return records from a patient registry in response to a Find Candidates Query.** **Derived from Figure 3.55.4.2.2-1 (PRPA_RM201310IHE)**	**Swiss National Extension**
moodCode [1..1] (M) Observation (CS) {CNE:http://hl7.org/v3ballot2007may/html/infrastructure/vocabulary/ActMood.htm - ActMood, default= "EVN"}	Structural attribute – this is an event.	No further refinement.
code [1..1] (M) Observation (CD) {CWE:QueryMatchObservationType}	A code, identifying this observation as a query match observation.	No further refinement.
value [1..1] (M) QueryMatchObservation (INT)	A numeric value indicating the quality of match for this record. It shall correspond to the MinimumDegreeMatch.value attribute of the original query, and it shall have the same meaning (e.g., percentage, indicating confidence in the match).	This value MUST state 100 for a match, 0 otherwise.

1.9 Requirements on HPD Profile for Replication

1.9.1 Introduction

The Healthcare Provider Directory (HPD) profile is extended to support the incremental replication of the entire directory or part of it to a second directory (across organizational boundaries). This extension will support the integration of multiple Swiss organizations with a single national HPD service, providing them with the support for the asynchronous synchronization of the directory content, without scarifying their operational independence.
This extension also defines some content profiles to ease the integration between communities, by limiting the value-set of several attributes, e.g. identifiers, organization types, provider types, etc.

1.9.2 Use-case: Provider information replication

Table 17: Use-case: Provider information replication

Scenario	A *Provider Information Consumer* is used to feed a second directory based on changes applied to *Provider Information Directory*.
Triggering event	A new provider is published to the *Provider Information Directory*.
Involved actors	*Provider Information Directory, Provider Information Consumer.*
Short description	The *Provider Information Consumer* issues a *Provider Information Delta Download* transaction to retrieve valid mutations from the *Provider Information Directory*.
Pre-conditions	The actor is authenticated and authorized to communicate with the *Provider Information Directory*.
Post-conditions	The content of the *Provider Information Directory* is unchanged and the replication at the *Provider Information Consumer* is updated.
Activities flow	1. Based on a timer (or on a notification), the *Provider Information Consumer* issues a *Provider Information Delta Download* transaction to download all delta changes since the last successful transaction; 2. Optionally, some filtering criteria are processed.

1.9.3 Actors / Transactions

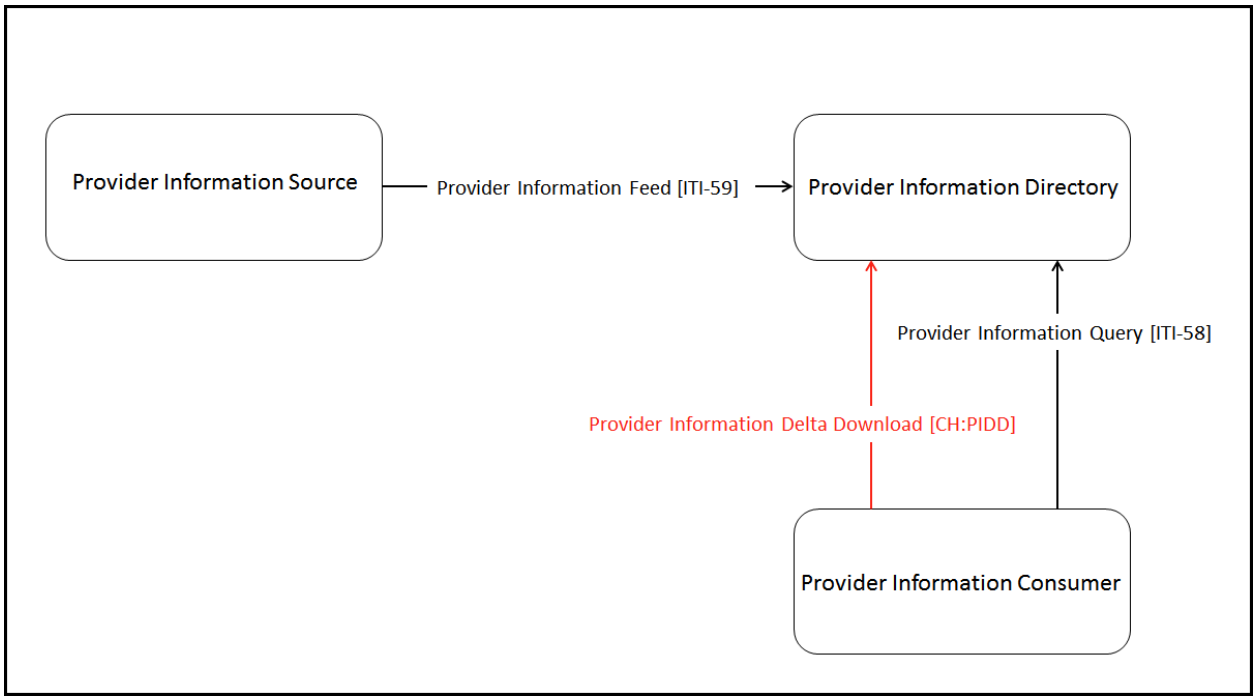


Figure 6: Swiss extended HPD Actors / Transactions

1.9.3.1 Provider Information Directory

The Provider Information Directory is extended with the following option:

- Provider Information Delta Download Option

This option requires the implementation of the Swiss Provider Information Delta Download [CH:PIDD] transaction.

1.9.3.2 Provider Information Consumer

The Provider Information Consumer is extended with the following option:

- Provider Information Delta Download Option

This option requires the implementation of the Swiss Provider Information Delta Download [CH:PIDD] transaction.

1.9.4 Transactions

1.9.4.1 Provider Information Delta Download (CH:PIDD)

This transaction schema extends the DSMLv2 interface by supporting an additional SOAP schema (see Appendix C – Provider Information Delta Download schema on page 53) and an additional wsdl operation:

```
<operation name="ProviderInformationDownloadRequest">
  <soap:operation soapAction="urn:ihe:iti:hpd:2010:ProviderInformationDownloadRequest" />
    <input>
     <soap:body use="literal" />
  </input>
  <output>
    <soap:body use="literal" />
  </output>
</operation>
```

1.9.4.1.1 Interaction Diagram

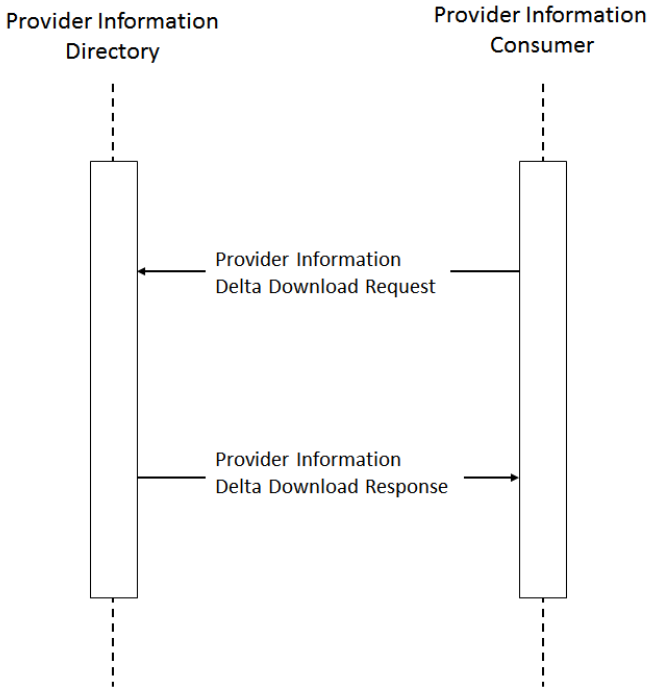


Figure 7: Provider Information Delta Download (CH:PIDD) interaction diagram

1.9.4.1.2 Provider Information Delta Download Request

Provider Information Consumer initiates a Provider Information Delta Download Request to the Provider Information Directory. This request includes:

- A required **fromDate** parameter to define the inclusive range starting date of the requested transactions sequence;
- An optional **toDat** parameter to define the inclusive range ending date of the requested transactions sequence (default: now);
- An optional **filterMyTransactions** boolean parameter to manage the the server side filtering of the author issued transactions (default: true);

1.9.4.1.3 Provider Information Delta Download Response

The response message contains a sequence of DSMLv2 batchRequest elements.

1.9.5 Message Semantics

1.9.5.1 HPD Schema Content

1.9.5.1.1 Identifiers

Organizational (e.g. hospitals) and Individual (health professionals) providers are identified by a Global Location Number (GLN).
A GLN number is a GTIN-13 digits unique number distributed by GS1 (http://www.gs1.ch/), where the first 12 digits are identifying the entity and the 13th is a check digit that can be used to validate manual inputs. In Switzerland GLN's can be obtained from the Refdata foundation[6] at no costs.
The format to persist identifiers for both organizational and individual providers is:
`Issuing Authority:Type:ID:Status`

Example (for an individual provider):
`GS1:GLN:9085632587458:active`

[6] http://www.refdata.ch/content/partner_d.aspx?Nid=6&Aid=908&ID=412

1.9.5.1.2 Attributes

Some additional restrictions apply to the Swiss national extension of the IHE ITI HPD Profile to ensure a better quality of the data. The following sections report the list of attributes supported, together with some indications on the deviations from the original HPD profile and ISO standard for both organizational and individual providers.

Conventions:
Optionality column (?): O=optional, R=required, R2=required if available;
Cardinality column (#): S=Single-valued, M=Multi-valued;
Deviations from the HPD profile are **highlighted**.

Table 18: Swiss refined HPD Organizational provider attributes

HPD profile [1]			**Swiss National Extension**		
Attribute name	**?**	**#**	**?**	**#**	***Notes***
Unique Entity Identifier	R	S	R	S	*Auto-generated*
Org Identifiers	R	M	R	**S**	GLN
Org Names	R	M	R	M	Legal name(s)
Org Known Names	R2	M	R2	M	Other name(s)
Org Type	O	M	**R**	M	HealthCareFacilityCode value [App. A-1]
Org Type description	O	M	O	M	HealthCareFacilityCode display name [App. A-1]
Org Status	O	S	O	S	Possible values: *Active, Inactive*
Org Supported Lang.	O	M	O	M	Encoded using ISO-639-1
Org Specialty	O	M	**R2**	M	PracticeSettingCode value [App. A-2]
Org Relationships	O	M	**R**	M	Reference to community or parent org.

NOTE: HPD profile or ISO standard format restrictions are not reported here; more information on these restrictions and on additional attributes are available in the IHE ITI TF-2b, Table 3.58.4.1.2.2.3-1: Organizational Provider Mapping applies.

Table 19: Swiss refined HPD Individual provider attributes

HPD profile [1]			**Swiss National Extension**		
Attribute name	**?**	**#**	**?**	**#**	***Notes***
Unique Entity Identifier	R	S	R	S	*Auto-generated*
Provider Identifiers	R	M	R	**S**	GLN
Provider Type	R	M	R	M	IndProviderTypeCode value [App. A-3]
Provider Type descript.	R	M	R	M	IndProviderTypeCode display name [App. A-3]
Provider Status	O	S	O	S	Possible values: *Active, Inactive*
Provider Primary Name	R	S	R	S	i.e. provider display name
Provider First Name	R2	M	**R**	M	Actual first name
Provider Last Name	R	M	R	**S**	Actual last name
Provider Known Names	R	M	R	M	Composed name string (e.g. title, first name,...)
Provider Supported Lang.	O	M	O	M	Encoded using ISO-639-1
Provider Gender	O	S	O	S	RFC 2985
Provider Specialty	O	M	O	M	AuthorSpecialtyCode value [App. A-4]
Provider Relationships	O	M	**R**	**M**	Reference to community or parent org.

NOTE: HPD profile or ISO standard format restrictions are not reported here; more information on these restrictions and on additional attributes are available in the IHE ITI TF-2b, Table 3.58.4.1.2.2.2-1: Individual Provider Mapping applies.

Appendices

Appendix A – AuditMessage schema (AuditMessage.xsd)

This XML schema is identical to the DICOM A.5.1-1 Audit Message Schema, which is provided in Relax NG Compact format.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified">
  <!--
  This defines the coded value type. The comment shows a pattern that can be used to further
  constrain the token to limit it to the format of an OID.  Not all schema software
  implementations support the pattern option for tokens.
  -->
  <!-- The basic message -->
  <xs:element name="AuditMessage">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="EventIdentification"/>
        <xs:element maxOccurs="unbounded" ref="ActiveParticipant"/>
        <xs:element ref="AuditSourceIdentification"/>
        <xs:element minOccurs="0" maxOccurs="unbounded" ref="ParticipantObjectIdentification"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="EventIdentification" type="EventIdentificationContents"/>
  <xs:element name="ActiveParticipant" type="ActiveParticipantContents"/>
  <xs:element name="AuditSourceIdentification" type="AuditSourceIdentificationContents"/>
  <xs:element name="ParticipantObjectIdentification"
type="ParticipantObjectIdentificationContents"/>

  <xs:complexType name="EventIdentificationContents">
    <xs:sequence>
      <xs:element ref="EventID"/>
      <xs:element minOccurs="0" maxOccurs="unbounded" ref="EventTypeCode"/>
      <xs:element minOccurs="0" ref="EventOutcomeDescription"/>
    </xs:sequence>
    <xs:attribute name="EventActionCode">
      <xs:simpleType>
        <xs:restriction base="xs:token">
          <xs:enumeration value="C"/>
          <xs:enumeration value="R"/>
          <xs:enumeration value="U"/>
          <xs:enumeration value="D"/>
          <xs:enumeration value="E"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
    <xs:attribute name="EventDateTime" use="required" type="xs:dateTime"/>
    <xs:attribute name="EventOutcomeIndicator" use="required">
      <xs:simpleType>
        <xs:restriction base="xs:token">
          <xs:enumeration value="0"/>
          <xs:enumeration value="4"/>
```

```
        <xs:enumeration value="8"/>
        <xs:enumeration value="12"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
</xs:complexType>

<xs:attributeGroup name="other-csd-attributes">
  <xs:attribute name="codeSystemName" use="required" type="xs:token"/>
  <xs:attribute name="displayName" type="xs:token"/>
  <xs:attribute name="originalText" use="required" type="xs:token"/>
</xs:attributeGroup>

<xs:attributeGroup name="CodedValueType">
  <xs:attribute name="csd-code" use="required" type="xs:token"/>
  <xs:attributeGroup ref="other-csd-attributes"/>
</xs:attributeGroup>

<xs:element name="EventID">
  <xs:complexType>
    <xs:attributeGroup ref="CodedValueType"/>
  </xs:complexType>
</xs:element>

<xs:element name="EventTypeCode">
  <xs:complexType>
    <xs:attributeGroup ref="CodedValueType"/>
  </xs:complexType>
</xs:element>

<xs:element name="EventOutcomeDescription" type="xs:string"/>

<xs:complexType name="AuditSourceIdentificationContents">
  <xs:sequence>
    <xs:element minOccurs="0" maxOccurs="unbounded" ref="AuditSourceTypeCode"/>
  </xs:sequence>
  <xs:attribute name="code" use="required">
    <xs:simpleType>
      <xs:union memberTypes="xs:token">
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="1"/>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="2"/>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="3"/>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="4"/>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>
```

```
          <xs:restriction base="xs:token">
            <xs:enumeration value="5"/>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="6"/>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="7"/>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="8"/>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="9"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:union>
    </xs:simpleType>
  </xs:attribute>
  <xs:attribute name="codeSystemName" type="xs:token"/>
  <xs:attributeGroup ref="other-csd-attributes"/>
  <xs:attribute name="AuditEnterpriseSiteID" type="xs:token"/>
  <xs:attribute name="AuditSourceID" use="required" type="xs:token"/>
</xs:complexType>

<xs:element name="AuditSourceTypeCode" type="xs:token"/>

<xs:complexType name="ActiveParticipantContents">
  <xs:sequence>
    <xs:element minOccurs="0" maxOccurs="unbounded" ref="RoleIDCode"/>
    <xs:element minOccurs="0" ref="MediaIdentifier"/>
  </xs:sequence>
  <xs:attribute name="UserID" use="required"/>
  <xs:attribute name="AlternativeUserID"/>
  <xs:attribute name="UserName"/>
  <xs:attribute name="UserIsRequestor" use="required" type="xs:boolean"/>
  <xs:attribute name="NetworkAccessPointID" type="xs:token"/>
  <xs:attribute name="NetworkAccessPointTypeCode">
    <xs:simpleType>
      <xs:restriction base="xs:token">
        <xs:enumeration value="1"/>
        <xs:enumeration value="2">
          <xs:annotation>
            <xs:documentation>Machine Name, including DNS name</xs:documentation>
          </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="3">
          <xs:annotation>
            <xs:documentation>IP Address</xs:documentation>
          </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="4">
```

```
          <xs:annotation>
            <xs:documentation>Telephone Number</xs:documentation>
          </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="5">
          <xs:annotation>
            <xs:documentation>Email address</xs:documentation>
          </xs:annotation>
        </xs:enumeration>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
</xs:complexType>

<xs:element name="RoleIDCode">
  <xs:complexType>
    <xs:attributeGroup ref="CodedValueType"/>
  </xs:complexType>
</xs:element>

<xs:element name="MediaIdentifier">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="MediaType"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="MediaType">
  <xs:complexType>
    <xs:attributeGroup ref="CodedValueType"/>
  </xs:complexType>
</xs:element>

<xs:attributeGroup name="ValuePair">
  <xs:annotation>
    <xs:documentation>URI (user directory, HTTP-PUT, ftp, etc.)</xs:documentation>
  </xs:annotation>
  <xs:attribute name="type" use="required" type="xs:token"/>
  <xs:attribute name="value" use="required" type="xs:base64Binary"/>
</xs:attributeGroup>

<xs:group name="DICOMObjectDescriptionContents">
  <xs:sequence>
    <xs:element minOccurs="0" maxOccurs="unbounded" ref="MPPS"/>
    <xs:element minOccurs="0" maxOccurs="unbounded" ref="Accession"/>
    <xs:element ref="SOPClass"/>
    <xs:element ref="ParticipantObjectContainsStudy"/>
    <xs:element minOccurs="0" ref="Encrypted"/>
    <xs:element minOccurs="0" ref="Anonymized"/>
  </xs:sequence>
</xs:group>

<xs:element name="MPPS">
  <xs:complexType>
    <xs:attribute name="UID" use="required" type="xs:token"/>
  </xs:complexType>
</xs:element>

<xs:element name="Accession">
```

```
  <xs:complexType>
    <xs:attribute name="Number" use="required" type="xs:token"/>
  </xs:complexType>
</xs:element>

<xs:element name="SOPClass">
  <xs:complexType>
    <xs:sequence>
      <xs:element minOccurs="0" maxOccurs="unbounded" ref="Instance"/>
    </xs:sequence>
    <xs:attribute name="UID" type="xs:token"/>
    <xs:attribute name="NumberOfInstances" use="required" type="xs:integer"/>
  </xs:complexType>
</xs:element>

<xs:element name="Instance">
  <xs:complexType>
    <xs:attribute name="UID" use="required" type="xs:token"/>
  </xs:complexType>
</xs:element>

<xs:element name="ParticipantObjectContainsStudy">
  <xs:complexType>
    <xs:sequence>
      <xs:element minOccurs="0" maxOccurs="unbounded" ref="StudyIDs"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="StudyIDs">
  <xs:complexType>
    <xs:attribute name="UID" use="required" type="xs:token"/>
  </xs:complexType>
</xs:element>

<xs:element name="Encrypted" type="xs:boolean"/>

<xs:element name="Anonymized" type="xs:boolean"/>

<xs:complexType name="ParticipantObjectIdentificationContents">
  <xs:sequence>
    <xs:element ref="ParticipantObjectIDTypeCode"/>
    <xs:choice>
      <xs:element ref="ParticipantObjectName"/>
      <xs:element ref="ParticipantObjectQuery"/>
    </xs:choice>
    <xs:element minOccurs="0" maxOccurs="unbounded" ref="ParticipantObjectDetail"/>
    <xs:element minOccurs="0" maxOccurs="unbounded" ref="ParticipantObjectDescription"/>
    <xs:group ref="DICOMObjectDescriptionContents"/>
  </xs:sequence>
  <xs:attribute name="ParticipantObjectID" use="required" type="xs:token"/>
  <xs:attribute name="ParticipantObjectTypeCode">
    <xs:simpleType>
      <xs:restriction base="xs:token">
        <xs:enumeration value="1"/>
        <xs:enumeration value="2"/>
        <xs:enumeration value="3"/>
        <xs:enumeration value="4"/>
      </xs:restriction>
    </xs:simpleType>
```

```
  </xs:attribute>
  <xs:attribute name="ParticipantObjectTypeCodeRole">
    <xs:simpleType>
      <xs:restriction base="xs:token">
        <xs:enumeration value="1"/>
        <xs:enumeration value="2"/>
        <xs:enumeration value="3"/>
        <xs:enumeration value="4"/>
        <xs:enumeration value="5"/>
        <xs:enumeration value="6"/>
        <xs:enumeration value="7"/>
        <xs:enumeration value="8"/>
        <xs:enumeration value="9"/>
        <xs:enumeration value="10"/>
        <xs:enumeration value="11"/>
        <xs:enumeration value="12"/>
        <xs:enumeration value="13"/>
        <xs:enumeration value="14"/>
        <xs:enumeration value="15"/>
        <xs:enumeration value="16"/>
        <xs:enumeration value="17"/>
        <xs:enumeration value="18"/>
        <xs:enumeration value="19"/>
        <xs:enumeration value="20"/>
        <xs:enumeration value="21"/>
        <xs:enumeration value="22"/>
        <xs:enumeration value="23"/>
        <xs:enumeration value="24"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
  <xs:attribute name="ParticipantObjectDataLifeCycle">
    <xs:simpleType>
      <xs:restriction base="xs:token">
        <xs:enumeration value="1"/>
        <xs:enumeration value="2"/>
        <xs:enumeration value="3"/>
        <xs:enumeration value="4"/>
        <xs:enumeration value="5"/>
        <xs:enumeration value="6"/>
        <xs:enumeration value="7"/>
        <xs:enumeration value="8"/>
        <xs:enumeration value="9"/>
        <xs:enumeration value="10"/>
        <xs:enumeration value="11"/>
        <xs:enumeration value="12"/>
        <xs:enumeration value="13"/>
        <xs:enumeration value="14"/>
        <xs:enumeration value="15"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
  <!-- spelling correction!!
  ParticipantObjectSensistity seems to be wrong.
  Using ParticipantObjectSensitivity instead
  -->
  <xs:attribute name="ParticipantObjectSensitivity" type="xs:token"/>
</xs:complexType>

<xs:element name="ParticipantObjectIDTypeCode">
```

```
    <xs:complexType>
      <xs:attributeGroup ref="CodedValueType"/>
    </xs:complexType>
  </xs:element>

  <xs:element name="ParticipantObjectName" type="xs:token"/>

  <xs:element name="ParticipantObjectQuery" type="xs:base64Binary"/>

  <xs:element name="ParticipantObjectDetail">
    <xs:complexType>
      <xs:attributeGroup ref="ValuePair"/>
    </xs:complexType>
  </xs:element>

  <xs:element name="ParticipantObjectDescription" type="xs:token"/>

</xs:schema>
```

Appendix B – AuditTrail schema (AuditTrail.xsd)

Includes the AuditMessage schema, introduced in chapter "1.4.4.1.1 Detailed AuditMessage definitions" starting on page 14.
See also Appendix A – AuditMessage schema starting on page 45.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified">

  <xs:include schemaLocation="AuditMessage.xsd"/>

  <xs:element name="AuditTrail">
    <xs:complexType>
      <xs:sequence>
        <xs:element minOccurs="1" maxOccurs="unbounded" ref="AuditMessage"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

</xs:schema>
```

Appendix C – Provider Information Delta Download schema (PIDD.xsd)

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema targetNamespace="urn:ehealth-suisse:names:tc:CS:1" xmlns="urn:ehealth-
suisse:names:tc:CS:1" elementFormDefault="qualified">
  <xsd:element name="downloadRequest" type="DownloadRequest" />
  <xsd:element name="downloadResponse" type="DownloadResponse" />

  <!-- **** Download Request **** -->
  <xsd:complexType name="DownloadRequest">
    <xsd:sequence>
      <xsd:element name="authRequest" type="dsml:AuthRequest" minOccurs="0" maxOccurs="1" />
    </xsd:sequence>
    <xsd:attribute name="requestID" type="xsd:string" use="optional" />
    <xsd:attribute name="fromDate" use="required">
      <xsd:simpleType>
        <xsd:restriction base="xsd:dateTime" />
      </xsd:simpleType>
    </xsd:attribute>
    <xsd:attribute name="toDate" use="optional">
      <xsd:simpleType>
        <xsd:restriction base="xsd:dateTime" />
      </xsd:simpleType>
    </xsd:attribute>
    <xsd:attribute name="filterMyTransactions" use="optional" default="true">
      <xsd:simpleType>
        <xsd:restriction base="xsd:boolean" />
      </xsd:simpleType>
    </xsd:attribute>
  </xsd:complexType>

  <!-- **** Download Response **** -->
  <xsd:complexType name="DownloadResponse">
    <xsd:sequence>
      <xsd:element ref="dsml:batchRequest" maxOccurs="unbounded" minOccurs="0" />
    </xsd:sequence>
    <xsd:attribute name="requestID" type="xsd:string" use="optional" />
  </xsd:complexType>

</xsd:schema>
```

Glossary

The IHE Glossary can be found as an appendix to the *IHE Technical Frameworks General Introduction*.
See also chapter “1.1 Definitions of terms” on page 5.

Illustrations

Tables

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI

Office fédéral de la santé publique OFSP
Unité de direction Politique de la santé

Profils d'intégration nationaux selon l'article 5, lettre c ODEP-DFI

Authorization Decision Request (CH:ADR) and Privacy Policy Query (CH:PPQ)

Version: 1.0 22.03.2016
Entrée en vigueur: ...

Table of Content

1 Introduction

The Swiss Electronic Health Record (EPD) depends on an IHE XDS and multi-community based system where the patient not only consents to the creation and use of the record, but does so by explicitly defining access rules through a patient portal.

The patient's privacy choices (concerning access to his health record) are stored by the community where the patient has established his EPD (reference community) and MUST be respected by all participating systems. It has been specified for the Document Registries to act as Policy Enforcing Service Providers in terms of a XACML PEP. However, as the rules to be enforced MAY not be available to the Document Registry of a community, the XACML PDP needs to be implemented as its own separated actor to establish interoperability regarding policy enforcements. Furthermore, Policy Repositories themselves (XACML PAP) are specified to act as a Policy Enforcing Service Provider.

The complexity and flexibility of access rule definitions that were granted to patients by law, require the Patient Portals to act as Policy Managers that use an API into Policy Repositories to add, query, update and delete policies. There is a lack of interoperability standards regarding this use case.

1.1 Definitions of terms

1.1.1 Electronic patient dossier (EPD)

The object of the Federal Law on Electronic Health Records (FLEHR) is to define the conditions for processing data and documents relating to electronic health records. Using electronic health records, healthcare professionals can access data relevant to treatment of their patients that was compiled and decentrally recorded by healthcare professionals involved in the treatment process. Healthcare professionals may save this data if necessary in their practice and hospital information systems outside of the electronic health records. To access electronic health records, healthcare professionals must join a certified community, which is an association of healthcare professionals and their institutions, and their patients must grant them the necessary access rights. In addition, the electronic health record also allows patients to view their data, to make their own data accessible and to manage the allocation of access rights. Healthcare professionals may only process data in electronic health records with the consent of the patient. Patients have the option of granting individual and graded access rights.
Notation of this term in the following text: **EPD**

1.1.2 EPD circle of trust

From an organizational perspective and in terms of the FLEHR, communities are an association of healthcare professionals and their institutions. Communities who want to participate in the Swiss EPD must comply with the certification requirements as laid down in the implementing provisions for the FLEHR. Such communities and, in particular, their gateways will be listed in a community portal index provided by the FOPH and therefore form a circle of trust by mutual recognition of their conformity related to data protection and data privacy. Furthermore, all required central services are also part of this circle of trust.
Notation of this term in the following text: **EPD circle of trust**

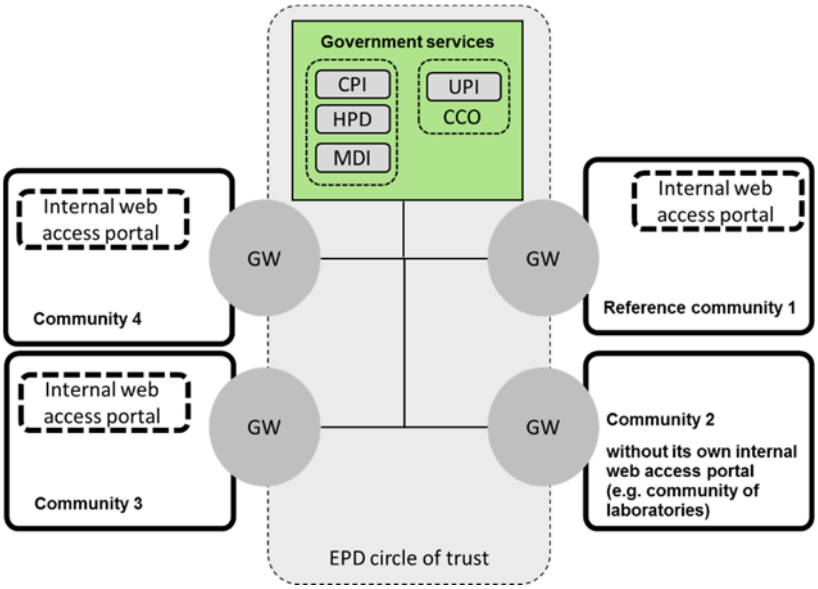


Figure 1: Swiss EPD circle of trust

Legend:

- GW: Gateway
- CPI: Community / Portal Index
- UPI: Unique Person Identification
- HPD: Healthcare Provider Directory
- MDI: Metadata Index-Service

1.1.3 Reference community

If a patient decides to open an EPD, she or he first chooses a community that manages all of his current consents and access right configurations to be used by other EPD users (in essence healthcare professionals) while accessing his personal EPD. Consents and access rights for one patient are managed by exactly one community in the EPD circle of trust.
Although the term home community is used by IHE in a slightly different way, the current specification states this consent and access right management community as reference community.
Cross-community accesses to documents within the EPD are only permitted when the initiating user gets permission by the access rights defined by the patient. Although cross-community accesses may occur between each community within the EPD circle of trust regardless whether it is the patient's reference community or not, the responding community must always apply the current access right settings managed by the reference community.
The patient may change his reference community at any time (for example, when moving to another residence).
Notation of this term in the following text: **referenceCommunity**

1.1.4 Patient Identifiers (EPD-PID, MPI-PID)

Communities in the EPD circle of trust use the national EPD patient identifier (EPD-PID) only for cross-community communication. The federal Central Compensation Office (CCO)[1] is the institution which issues EPD-PID's. CCO is the only institution which is allowed to correlate the Social Security Number (AVN13) with the EPD-PID. There is no correlation possible back from the EPD-PID to the Social Security Number. This is political intention in order to achieve highest possible patient privacy.
Within a community patients are identified by a MPI-PID which is managed by a community Master Patient Index (MPI). Primary Systems may correlate their local patient identifier with the MPI-PID. For

[1] http://www.zas.admin.ch/index.html

cross-community communication the gateways may correlate the MPI-ID to the EPD-PID.

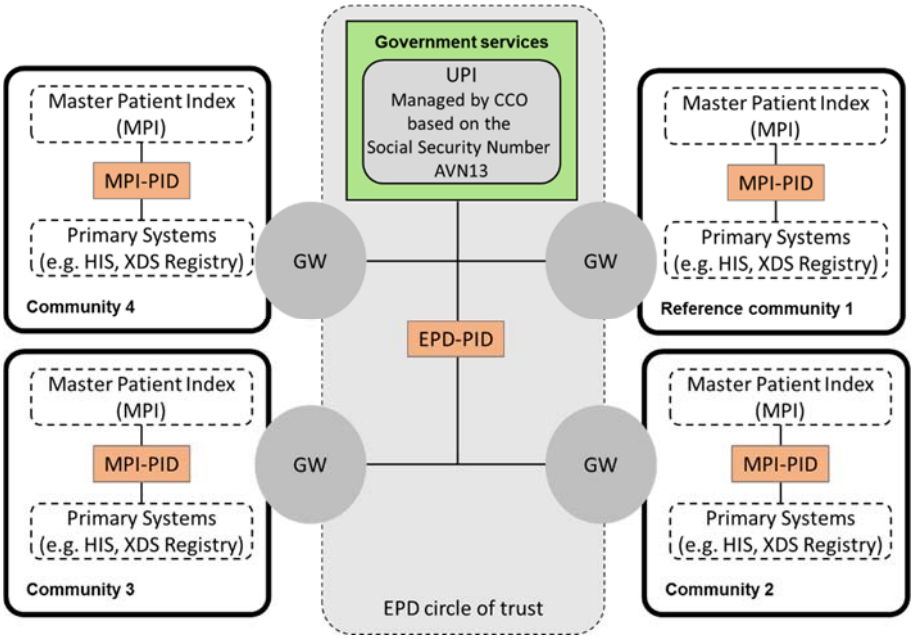


Figure 2 Swiss Patient Identifiers

1.1.5 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2 Volume 1 – Integration Profiles

2.1 Overview

The **Authorization Decision Request (ADR)** may be understood as a subsequent process to IHE XUA. XUA formulates the user's identity (SAML assertion) that is trying to access data through a corresponding transaction. ADR takes the information provided by the identity assertion of a transaction and formulates a decision request query by a description of the subject (who), action (how), resource (what) and environment (when). The response contains an access decision for each resource.

The **Privacy Policy Query (PPQ)**, however, may rather be understood similar to XDS transactions. A Policy Manager applies PPQ transactions to add, query, update and delete policies held by the Policy Repository. PPQ is the pre-requisite for Patient Portals to manipulate the policies, authorization decisions are finally based on. It is important to understand that PPQ transactions underlie the same access control mechanisms as XDS transactions do. Therefore XUA identity assertions MUST be provided, so that the Policy Repository can verify (through a subsequent ADR transaction) whether the access control mechanism allows the changes.

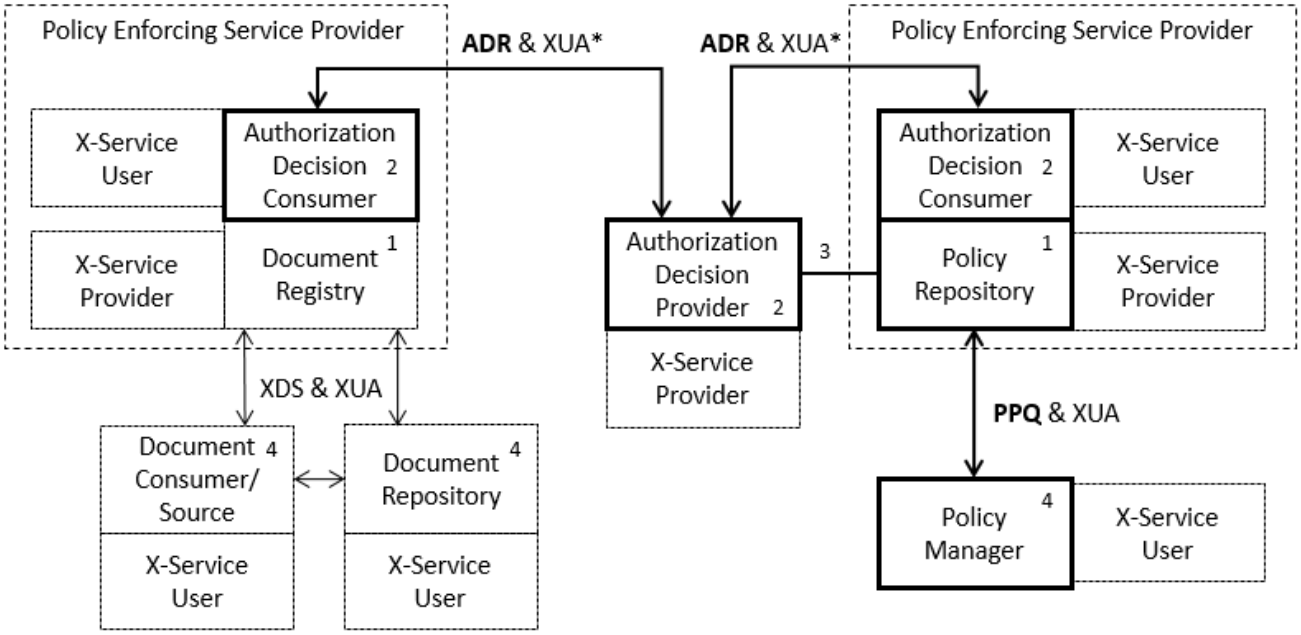


*Figure 3: ADR and PPQ Actors - shows the actors directly involved in the ADR and PPQ Profile and the relevant transactions between them. If needed for context, other actors that MAY be indirectly involved due to their participation in other related profiles are shown in dotted lines. Actors which have a mandatory grouping are shown in conjoined boxes. *) The ADR transaction MUST provide a XUA identity assertion of the current user mainly for auditing reasons.*

1. Document Registries, Repositories and Policy Repositories MUST be grouped with the ADR Authorization Decision Consumer and XUA X-Service Provider actors to become Policy Enforcing Service Providers.
2. ADR transactions are protected by XUA as well, which requires the Authorization Decision Consumer to be grouped with the X-Service User actor and the Authorization Decision Provider to be grouped with the X-Service Provider actor (marked with *)
3. The ADR Authorization Decision Provider SHOULD be grouped with a Policy Repository or requires privileged access to the policies stored by the Policy Repository.
4. A Policy Manager applies PPQ transactions to add, query, update and delete policies stored by the Policy Repository. Document Consumers apply XDS Registry Stored Query

transactions to retrieve document metadata. Document Repositories apply XDS Register Document Set transactions due to XDS Provide and Register transactions by a Document Source. All three are grouped with the XUA X-Service User Actor.

2.2 EPD XUA Requirements for XDS and PPQ

A SAML 2.0 **<Assertion>** is added to the WS-Security context of the SOAP Header of each transaction message to communicate entities (user identities) that initiated those transactions. This is a pre-requisite for subsequent Authorization Decision Query Requests.

```
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
  <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xs="http://www.w3.org/2001/XMLSchema" ID="_37d8092df99f08cd8435ac29a7062092"
    IssueInstant="2014-04-09T19:10:00.294Z" Version="2.0">
    <!--Identity Claims-->
  </saml2:Assertion>
</wsse:Security>
```

Listing 1: The WS Security context of the SOAP header with the SAML2 Assertion element. For simplicity the identity claims are not shown.

The EPD SAML 2.0 <Assertion> has the child elements **<Issuer>**, **<Signature>**, **<Subject>**, **<Conditions>, <AuthnStatement>** and **<AttributeStatement>**. The <AttributeStatement> element caries a number of attributes that reflect the identity claims being made.

The EPD requires the following details to be claimed within the assertion:

<Issuer> the system that issued the token and therefore confirms that the identified user was properly authenticated and that the attributes included in the token are accurate. For further details see [SAML 2.0].

```
<saml2:Issuer>urn:e-health-suisse:xua:gemeinschaft:ksa</saml2:Issuer>
```

<Signature> an X.509 signature by a trusted entity (XUA Assertion Provider) to guaranty the confidentiality of the claims being made and unaltered content of the assertion. For further details see [SAML 2.0].

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <ds:Reference URI="#_37d8092df99f08cd8435ac29a7062092">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xs"/>
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="value="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:DigestValue>NRrlqwGn8o9tO0DlkYbOaXNqlM0=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
 <ds:SignatureValue>dbBafjF2NPY0Y73uWztQvRpda5DOV8BrPYL5KlCx8yvnEBZ9TQrKnjwhcE=</ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate>
        <!-- X.509 Certificate -->
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
```

Listing 2: The Signature Element of the WS Security context providing the details of signature algorithm used. For simplicity the X.509 certificate is not shown.

<Subject> identifies the Requester Entity (Who is asking for access?). This element SHALL have the following SAML 2.0 **<NameID>** child element with the following attributes:

@Format=" urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" and **@NameQualifier="urn:e-health-suisse:epd-pid"** in case of a patient or **@NameQualifier="urn:gs1:gln"** in case of a professional or **@NameQualifier="urn:e-health-suisse:custodian-id"** in case of a custodian or guardian, who's been assigned to manage a patient's Health Record.
The Value of this element SHALL convey the subject identifier.

<Subject> SHALL have a second child element **<SubjectConfirmation>** with the following attribute:
@Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"

```
<saml2:Subject>
  <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
                NameQualifier="urn:e-health-suisse:gln">4567</saml2:NameID>
  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
</saml2:Subject>
```

Listing 3: Subject element of the SAML assertion providing the ID and the name qualifier of the requesting subject.

<Conditions> specifying a validity period (time stamps) to prevent "replay" of the assertion while attributes MAY have changed. The time period MUST be defined between a minimum of 5 seconds and a maximum of 10 minutes.
An audience restriction (urn:e-health-suisse:token-audience:all-communities) specifies the intended recipient or system the assertion SHALL be valid for.
The reuse of the token (signed SAML identity assertion) MAY be denied by

setting a <OneTimeUse> element. For further details see [SAML 2.0].

```
<saml2:Conditions NotBefore="2016-02-09T19:10:00.294Z" NotOnOrAfter="2016-02-09T19:15:00.294Z">
  <saml2:AudienceRestriction>
    <saml2:Audience>urn:e-health-suisse:token-audience:all-communities</saml2:Audience>
  </saml2:AudienceRestriction>
</saml2:Conditions>
```

Listing 4: The condition element of the SAML 2 assertion defining the assertion life time.

<AuthnStatement> specifying the authentication procedure by which the entity's identity (e.g. a user) was verified. For further details see [SAML 2.0].

```
<saml2:AuthnStatement AuthnInstant="2016-02-09T19:10:00.294Z">
  <saml2:AuthnContext>
<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
  </saml2:AuthnContext>
</saml2:AuthnStatement>
```

Listing 5: The authentication statement providing the authentication procedure used by the requesting system.

<AttributeStatement> identifies the Requester Entity's attributes / identity claims. There are six mandatory **<Attribute>** child elements as follows.
There SHALL be one <Attribute> element with the attribute:
@Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id"
The **<AttributeValue>** child element SHALL convey the subject's real world name as plain text as defined by IHE XUA.

There SHALL be one <Attribute> elements with the attribute:
@Name="urn:oasis:names:tc:xacml:2.0:subject:role"
The **<AttributeValue>** child element SHALL convey a coded value of the subject's **<Role>**. There are four roles to be distinguished within the EPD: "Patient(in)", "Behandelnde(r)", "Hilfsperson" and "Stellvertreter(in)".

There SHALL be one or more <Attribute> elements with the attribute:
@Name="urn:oasis:names:tc:xspa:1.0:subject:organization"
The **<AttributeValue>** child element SHALL convey a plain text the subject's organization is named by.

There SHALL be one or more <Attribute> elements with the attribute:
@Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id"
The **<AttributeValue>** child element SHALL convey the ID of the subject's organization or group that is identified by a GLN within the EPD's Healthcare Organizations Index (HOI). The value's syntax SHALL be a URN: urn:gs1:gln:*<GLN>,* e.g. urn:gs1:gln:7609999999999.

There SHALL be an <Attribute> element with the attribute:
@Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id"
The **<AttributeValue>** child SHALL convey the EPD-PID identifier of the patient's record the current transaction is related to.
(syntax as used in iti-18 XDSDocumentEntryPatientId)

.

There SHALL be an <Attribute> element with the attribute:
@Name=" urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"
The **<AttributeValue>** child element SHALL convey a coded value of the current transaction's **<PurposeOfUse>**. There are two values to be distinguished within the EPD: "Normalzugriff", "Notfallzugriff" (displayName).

```
<saml2:AttributeStatement>
  <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id">
    <saml2:AttributeValue>Hans Muster</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
    <saml2:AttributeValue>
      <Role xmlns="urn:hl7-org:v3" xs:type="CE“
            code=“1"
            codeSystem="2.16.756.5.30.1.127.3.10.xx.xx.xx"
            codeSystemName="eHealth Suisse EPD Akteure"
            displayName=“Patient(in)"/>
    </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization">
    <saml2:AttributeValue>Kantonspital Aarau</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">
    <saml2:AttributeValue>urn:e-health-suisse:gln:92375058</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id">
   <saml2:AttributeValue>8901^^^&amp;amp;2.16.756.5.30.1.127.3.10.x.xx&amp;amp;ISO</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
    <saml2:AttributeValue>
      <PurposeOfUse xmlns="urn:hl7-org:v3" xs:type="CE"
                    code=“1"
                    codeSystem="2.16.756.5.30.1.127.3.10.xx.xx.xx"
                    codeSystemName="eHealth Suisse Verwendungszweck"
                    displayName=“Normalzugriff"/>
    </saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

Listing 6: The SAML 2 attribute statement with the IHE XUA attribute claims.

2.3 Authorization Decision Query

This supplement defines new functionalities for XDS-based communities concerning the enforcement of access policies. They are applied to the clinical data stored by an XDS Document Registry, as well as to the access policies themselves, which are stored in a Policy Repository.

2.3.1 Motivation

The Document Registry, as the only system with knowledge of all clinical documents (and which only exists once) within communities (affinity domains), is generally thought of as an appropriate actor to enforce access rules on stored metadata. It is common that the Document Registry is inherently combined with the ability to make authorization decisions, which postulates access to the rules to be enforced and the ability to interpret them. As this is not necessarily given in all XDS environments, a separation of actors for decision making and enforcement, as well as the development of corresponding transactions greatly enhances interoperability. This is by no means a new idea, as the XACML standard as well as existing IHE profiles (SeR) envision the same concept and therefore will be adopted and adapted by ADR.
More generally, ADR enables a policy enforcing service provider (e.g. a Document Registry or a Policy Repository) to retrieve access decisions from an authority with access to the rules and the ability to interpret them.

2.3.2 Objectives and Constraints

The objective of the ADR Profile is the definition of a mechanism to request authorization decisions and convey the results between the actors "Authorization Decision Consumer" and "Authorization Decision Provider". Both are to be interpreted as specific implementations of PEP and PDP as defined by the XACML specification. There is a considerable overlap of concepts and use cases with the existing IHE Secure Retrieve (SeR) Profile. The following specification is based on IHE SeR, which was adapted to the needs of the actors and use cases of ADR. Transport, transaction types and content shall be based on the same standards and technologies as far as possible.
Two new actors and a new ADR-specific Authorization Decision Query transaction are being introduced. This profile describes how a Policy Enforcing Service Provider can request authorization decisions on certain resources and actions depending on user entities, a patient's record and other parameters allowed by the underlying standards.
Summarized, the constraints upon which this profile is developed are:

- The XACML data-flow model serves as the underlying processing model.
- There are Authorization Decision Providers acting as XACML PDPs with access to the policies and the capability to perform access decisions on.
- The policies are stored in a Policy Repository acting as XACML PAP.
- Policy enforcing service providers (e.g. Document Registries) act as XACML PEPs by implementing the Authorization Decision Consumer and the corresponding enforcement of a decision.
- The transactions between the profile's actors rely on SAML 2.0 profile of XACML v2.0.
- Policy enforcing service providers are grouped with a XUA X-Service Provider actor and therefore are capable of processing identities communicated in a SAML identity assertion.

2.3.3 Actors / Transactions

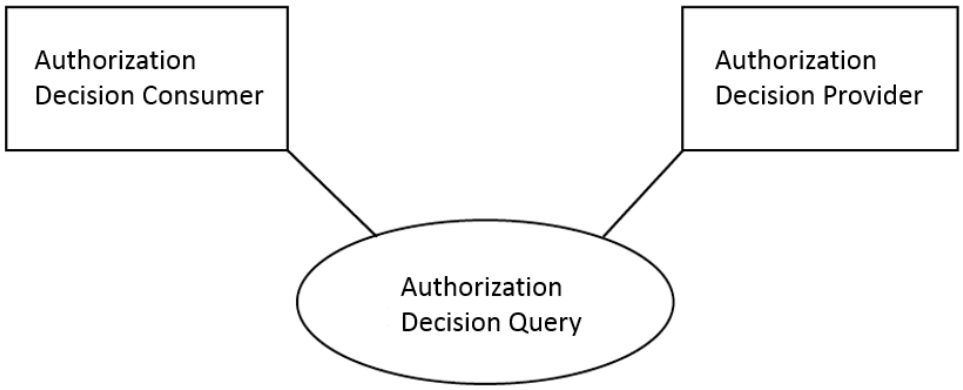


Figure 4: Diagram of actors involved in the ADR profile.

Actor:	Authorization Decision Provider
Role:	This actor accesses and interprets rules/policies and permits or denies access to resources.
Actor:	Authorization Decisions Consumer
Role:	This actor queries for authorization decisions.

Table 1 Actor Roles

2.4 Privacy Policy Query

This supplement defines new functionalities for XDS-based communities concerning the management of access policies in terms of updating or modifying policies as well as querying policies from and adding policies to a Policy Repository through a Policy Manager.

2.4.1 Motivation

The EPD defines the Policy Repository to act as XACML PAP that holds the access rules for the entire record as defined by the patient. Communities offering that service can be chosen by the patient to serve as the holder of that information (referenceCommunity). The community also provides a Patient Portal to allow the corresponding management of that information by the patient.
For the EPD, patients have extensive choices regarding their privacy preferences. There is a base rule stack, which defines a number of general access levels; the patient has a choice to grant to individual providers. A corresponding rule stack on top of the base rule stack MUST be allowed for the patient to be created, retrieved, manipulated and deleted. In addition to that, the patient MAY even define who has access not only to the record's documents but also to the patient's access rule stack including the ability to modify it.
The complexity and flexibility REQUIRED, can hardly be facilitated by existing standards. There are simpler approaches existing (e.g. IHE BPPC) to allow the expression of privacy choices by formulating consent to a set of fixed access policies (Allow publishing? Allow access during normal treatment? Allow break-the-glass?). However, allowing the patient to express specific rules for individual documents, providers and organizations requires a richer user experience and the ability to retrieve, change and delete individual rules. This implies using an API approach instead of a document-centric approach.

2.4.2 Objectives and Constraints

The objective of PPQ is the definition of actors and transactions to convey access policies from a Patient Portal to the referenceCommunity. Two new actors "Policy Manager" and "Policy Repository" are introduced. While the Policy Repository may be interpreted as a specific implementation of a XACML PAP, no analogy to the Policy Manager actor is defined in XACML. Therefore the Policy Manager is being introduced as an entirely new PPQ actor.
This profile describes how Policy Managers query, add, update and delete policies, allowing a Health

Record user to manage access rights according to the freedom of choice that was granted to the patient by Swiss regulations.
Constraints upon which this profile is developed are:

- The development of transactions between the profile's actors relies on SAML 2.0 and XACML SAML extension types, elements and protocols as specified in OASIS SAML 2.0 profile of XACML v2.0.
- The Policy Repository itself acts as a Policy Enforcing Service Provider being grouped with a XUA X-Service Provider actor. Therefore it is capable of processing identities communicated in a SAML identity assertion.
- The Policy Repository responds to PPQ Requests according to the result of ADR (transaction is allowed or not allowed to be performed).
- Respectively, Policy Managers are grouped with a XUA X-Service User to convey the current user's identity.

2.4.3 Actors / Transactions

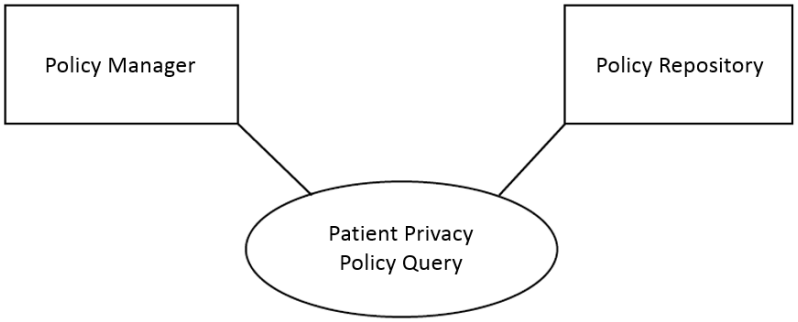


Figure 5: Actors involved in the PPQ profile.

Actor:	Policy Manager
Role:	This actor queries for existing policy sets, adds new policy sets, updates or deletes existing policy sets.
Actor:	Policy Repository
Role:	This actor acts as a XACML Policy Administration Point

Table 2: Actor Roles of the PPQ profile.

3 Volume 2 – Transactions

3.1 Authorization Decision Query

3.1.1 Scope

This transaction is used by the Authorization Decisions Consumer to query for authorization decisions, granted and managed by the Authorization Decisions Provider.
The Authorization Decisions Consumer asks for authorizations based on: the requester entity (**Subject**), the **Resources** available to be accessed by the Subject depending on the **Action** that was initiated, each completed by further context parameters.
This transaction is based on SOAP v1.2 exchange protocol and Synchronous Web services (See ITI TF-2x: Appendix V).

3.1.2 Referenced Standards

OASIS SOAP v1.2
OASIS Security Assertion Markup Language (SAML) v2.0
OASIS eXtensible Access Control Markup Language (XACML) v2.0
OASIS Multiple Resource Profile of XACML v2.0
OASIS SAML 2.0 profile of XACML v2.0
OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of SAML v2.0 for Healthcare Version 2.0 (not normative)

3.1.3 Interaction Diagram

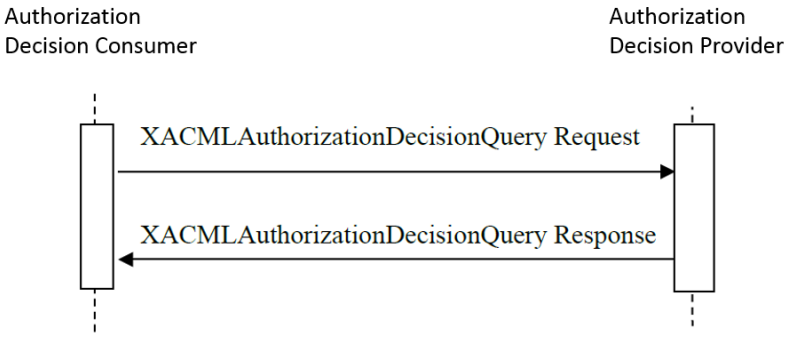


Figure 6: Sequence diagram of the XACMLAuthzDecisionQuery transaction of the ADR profile.

3.1.4 XACMLAuthzDecisionQuery Request

This message enables the Authorization Decisions Consumer to query the Authorization Decisions Provider for authorizations. This message relies on the SAML v2.0 extension for XACML and uses the element <XACMLAuthzDecisionQuery> to convey the Resource metadata, Subject identifier and Actions. The Authorization Decisions Consumer can ask for authorization regarding a number Resources in one query as the request message complies with the Multiple Resource Profile of XACML v2.0. Actors involved support XUA and use SAML identity assertions to identify entities (See ITI TF-1: 39.5 and 39.6). SAML attribute elements SHALL be mapped into XACML context attribute elements as defined in SAML 2.0 profile of XACML v2.0.

3.1.5 Trigger Events

The Authorization Decision Consumer of the EPD sends this message when it needs to verify whether there is an authorization to disclose specific Resources to an entity requesting them; e.g. to allow or deny access to and the manipulation of policies stored by a policy repository or to allow or deny access to document metadata stored in a Document Registry based on the entry's confidentiality code. In addition to that the Authorization Decision Consumer of the EPD sends this message when it needs to verify whether there is an authorization to persist specific Resources e.g. to allow or deny storage of document metadata in a Document Registry based on the entry's confidentiality code. The trigger events are:

- The grouped XDS Document Registry receiving a Registry Stored Query Request [ITI-18] and a Provide X-User Assertion [ITI-40] transaction, that identifies the specific requester entity within a SAML assertion, from an XDS Document Consumer;
- The grouped XDS Document Registry receiving a Register Document Set-b [ITI-42] and a Provide X-User Assertion [ITI-40] transaction, that identifies the specific requester entity within a SAML assertion, from an XDS Document Repository;
- The grouped PPQ Policy Repository receiving a Privacy Policy Query transaction (see this document) and a Provide X-User Assertion [ITI-40] transaction from a PPQ Policy Manager that identifies the specific requester entity within a SAML assertion.

3.1.6 Message Semantics

3.1.6.1 ADR due to XDS Registry Stored Query [ITI-18]

For the XDS Registry Stored Query related access decision enforcement, the EPD relies on the XDS Confidentiality Code within the document metadata to be accessed to represent a subset of the patient's health record. The Authorization Decisions Consumer MUST create one request to query for an access decision for each subset (rather than the actual document metadata objects), before providing the corresponding document metadata to a consumer. Therefore one of the attributes of each Resource within the Request must be a XDS confidentiality code defining the subset for an access decision to be made on (details below).

ADR due to XDS Register Document Set-b [ITI-42]

For the XDS Register Document Set related access decision enforcement, the EPD relies on the XDS Confidentiality Code within the document metadata to be stored in the patient's Health Record. The Authorization Decisions Consumer (Document Registry) MUST create one request to query for an access decision for each Confidentiality Code, before allowing the Register transaction to a Document Repository. One of the attributes of each Resource within the Request must be a XDS confidentiality code for an access decision to be made on (details below).

3.1.6.2 ADR due to PPQ

The EPD allows patients and their guardians to manage the patient's Health Record access rights. In addition to that, the patient may allow a professional to delegate his access rights to another professional if necessary.

In the case of ADR due to PPQ an access decision must be requested for each actual object (Resource) that access is being requested for (not a class of objects as it is the case for ADR due to XDS). Each Resource represents a policy set that's being queried, added, deleted or updated by a PPQ transaction. An access decision is to be requested for each of these Resources before the corresponding action can be granted (or has got to be denied, depending on the decision).

A professional may only delegate access rights to another professional not exceeding her or his own access level that was initially granted by the patient. The access level to be granted is encoded within the value of the referenced-policy-set attribute. Therefore, in case of ADR due to PPQ, one of the attributes of each Resource must be a referenced policy set (details below).

3.1.6.3 Semantics

The XACMLAuthzDecisionQuery Request message SHALL use SOAP v1.2 message encoding. The WS-Addressing Action header SHALL have this value:

urn:e-health-suisse:2015:policy-enforcement:AuthorizationDecisionRequest

The recipient of the Authorization Decision Query SHALL be identified by the WS-Addressing To header (URL of the endpoint).

A SAML 2.0 Identity Assertion SHALL be conveyed within the WS-Security Security header.

```
<soap:Envelope xmlns:soap=http://schemas.xmlsoap.org/soap/envelope/
        xmlns:wsa=http://www.w3.org/2005/08/addressing xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
        xmlns:wsse=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
        xmlns:ds=http://www.w3.org/2000/09/xmldsig# xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os"
        xmlns:xacml-samlp="urn:oasis:xacml:2.0:saml:protocol:schema:os"
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
        xmlns:epd="urn:e-health-suisse:2015:policy-administration"
        xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os" xmlns:hl7="urn:ihe-d:hl7-org:v3"
        xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/ http://schemas.xmlsoap.org/soap/envelope/
                http://www.w3.org/2005/08/addressing urn:e-health-suisse:2015:policy-administration
                epd-policy-administration-combined-schema-1.0-local.xsd ws-addr.xsd ">
  <soap:Header>
    <wsa:Action>urn:e-health-suisse:2015:policy-enforcement:AuthorizationDecisionRequest</wsa:Action>
    <wsa:MessageID>urn:uuid:e4bb38c7-e546-4bb1-8d68-2bccf783dfbf</wsa:MessageID>
    <wsa:To>https://e-health-suisse-adr-provider.ch</wsa:To>
    <wsse:Security>
      <saml:Assertion>
        <!--SAML Assertion as described above-->
      </saml:Assertion>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
   <!—ADR TRANSACTION PAY LOAD-->
  </soap:Body>
</soap:Envelope>
```

Listing 7: The SOAP envelope with the security header and the transaction payload of the ADR transactions. For better reading placeholder are used for the SAML assertions and the transaction payload.

The body of the message SHALL use an **<XACMLAuthzDecisionQuery>** element (defined in the SAML 2.0 Profile for XACML v2.0) to convey a <Request> with the Authorization Query parameters (Subject, Resource, Action, Environment). This element SHALL contain the following attribute:
@ReturnContext SHOULD be set to "**false**" because the content of the XACMLAuthzDecisionQuery Request is not needed within the Authorization Result.
@InputContextOnly SHALL be set to "**false**", as the Authorization Decision Provider may have further information and rules, other than the parameters included in the request, to determine a decision. This should not be restricted by the Authorization Decision Consumer.
This profile does not define further constraints for other attributes of this element (see OASIS SAML 2.0 profile of XACML v2.0 for details).

```
<soap:Body>
  <xacml-samlp:XACMLAuthzDecisionQuery InputContextOnly="false" ReturnContext="false"
  ID="_682fee8b-46c0-442a-8c54-fd9d656412fc" Version="2.0" IssueInstant="2016-02-09T09:30:10.5Z">
    <xacml-context:Request>
      <!--Request Parameters-->
    </xacml-context:Request>
  </xacml-samlp:XACMLAuthzDecisionQuery>
</soap:Body>
```

Listing 8: The SOAP body element for the XACMLAuthzDecisionQuery transaction. For better reading a placeholder is used for the request parameter.

The <XACMLAuthzDecisionQuery> element SHALL have only one child element **<Request>.** This element SHALL comply with OASIS Multiple Resource Profile of XACML v2.0. This element SHALL have the XACML child elements **<Subject>, <Resource>, <Action> and <Environment>**. <Request> and all subsequent elements, attributes and values comply to the namespace xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os". The namespace is left out of the following examples for better readability.

```
<soap:Body>
  <XACMLAuthzDecisionQuery>
    <Request>
      <Subject>
        <!--Attributes-->
      </Subject>
      <Resource>
        <!--Attributes-->
      </Resource>
      <Resource>
        <!--There can be more than one Resource-->
      </Resource>...
      <Action>
        <!--Attribute-->
      </Action>
      <Environment/>
    </Request>
  </XACMLAuthzDecisionQuery>
</soap:Body>
```

Listing 9: The schematic payload of the XACMLAuthzDecisionQuery request. For better reading placeholder are used for the XACML request elements.

<Subject> identifies the Requester Entity. It SHALL have at least the following **<Attribute>** child elements:

@AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" and **@DataType="http://www.w3.org/2001/XMLSchema#string"**.
The **<AttributeValue>** child element SHALL convey the subject identifier. This element SHALL have the same value of the /Subject/NameID element conveyed within the SAML assertion.

@AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id-qualifier" and **@DataType=" http://www.w3.org/2001/XMLSchema#string"**.
The **<AttributeValue>** child element SHALL convey the subject ID qualifier. This element SHALL have the same value as the /Subject/NameID/@NameQualifier conveyed within the SAML assertion, e.g. **urn:e-health-suisse:epd-pid** in case of a patient or guardian or **urn:gs1:gln** in case of a professional or auxiliary person.

@AttributeId="urn:ihe:iti:xca:2010:homeCommunityId" and **@DataType="http://www.w3.org/2001/XMLSchema#anyURI"**.
The **<AttributeValue>** child element SHALL convey the home community id. This value is not necessarily conveyed within the XUA SAML assertion. It SHALL be set to the OID of the Authorization Decision Consumer's community.

@AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role" and **@DataType="urn:hl7-org:v3#CV"**.
The **<AttributeValue>** child element SHALL convey the coded value for the subject's role. This element SHALL have the same value as the

/AttributeStatement/Attribute[@name="urn:oasis:names:tc:xacml:2.0:subject:role"]/AttributeValue conveyed within the SAML assertion.

@AttributeId="urn:oasis:names:tc:xacml:2.0:subject:organization-id" and **@DataType=" http://www.w3.org/2001/XMLSchema#anyURI"**.
The **<AttributeValue>** child element SHALL convey the organization identifier. This element SHALL have the same value as the organization-id conveyed within the SAML assertion.

@AttributeId="urn:oasis:names:tc:xacml:2.0:subject:purposeofuse" and **@DataType="urn:hl7-org:v3#CV"**.
The **<AttributeValue>** child element SHALL convey the coded value for the subject's purpose of use. This element SHALL have the same value of the <AttributeStatement>/<Attribute>/<AttributeValue> element **@PurposeOfUse** conveyed within the SAML assertion.

```
<Request>
  <Subject>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
               DataType="http://www.w3.org/2001/XMLSchema#string">
      <Attribute>4567</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id-qualifier"
               DataType="http://www.w3.org/2001/XMLSchema#string">
      <AttributeValue> urn:e-health-suisse:epd-pid</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:ihe:iti:xca:2010:homeCommunityId"
               DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <AttributeValue>1.2.756.113619.20.2.6.1</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role“
               DataType="urn:hl7-org:v3#CV">
      <AttributeValue>
        <hl7:CodedValue code=“1" codeSystem="2.999.8" displayName=“Patient(in)"/>
      </AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:subject:organization-id"
               DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <Attribute Value>urn:e-health-suisse:gln:92375058</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:subject:purposeofuse"
               DataType="urn:hl7-org:v3#CV">
      <AttributeValue>
        <hl7:CodedValue code="1" codeSystem=" 2.16.756.5.30.1.xxx" displayName=“Normalzugriff"/>
      </AttributeValue>
    </Attribute>
</Subject>
  <Resource/>
  <Action/>
  <Environment/>
</Request>
```

Listing 10: Example of the subject attributes elements of the XACMLAuthzDecisionQuery request.

<Resource> identifies the object (ADR due to PPQ) or class of objects (ADR due to XDS) an Authorization Decision is requested for. It SHALL at least have the following **<Attribute>** child elements. The Authorization Decisions Provider MAY ignore any attribute not defined in this specification.

@AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" and **@DataType="http://www.w3.org/2001/XMLSchema#anyURI"**.
The **<AttributeValue>** child element SHALL convey the resource identifier.

For ADR due to XDS [ITI-18] and [ITI-42] there are always exactly four Resources to be identified, each representing a class of documents: useful, medical, sensitive and confidential documents. The value MUST be constructed dynamically containing the patient's national identifier extension that was conveyed in the SAML assertion of the XDS transaction identifying the resource (resource-id). The four resource identifiers for ADR due to XDS are:
urn:e-health-suisse:2015:epd-subset:4567:useful,
urn:e-health-suisse:2015:epd-subset:4567:medical,
urn:e-health-suisse:2015:epd-subset:4567:sensitive and
urn:e-health-suisse:2015:epd-subset:4567:confidential with 4567 as an example value of the patient ID.

For ADR due to PPQ an Authorization Decision MUST be requested for each object itself, not a class of objects. In that case the value is the uuid of a Policy Set the Entity (Subject) is asking access for by a PPQ query, add, update or delete policy, e.g.:
c969c7cd-9fe9-4fdc-83c5-a7b5118922a3.
Therefore, for ADR due to PPQ, there is not a fixed number of <Resource>s (with corresponding Resource IDs) to be specified within the request.

@AttributeId="urn:e-health-suisse:2015:epd-pid" and **@DataType="urn:hl7-org:v3#II"**.
The **<AttributeValue>** child element SHALL convey the patient's national identifier that was conveyed in the SAML assertion of the XDS transaction identifying the resource (resource-id).

For ADR due to XDS each Resource element MUST also contain the actual confidentiality code corresponding to the resource-id as another attribute:
@AttributeId="urn:ihe:iti:xds-b:2007:confidentiality-code" and **DataType="urn:hl7-org:v3#CV"**.
The **<AttributeValue>** child element SHALL convey a confidentiality code, e.g. **<hl7:CodedValue code="2" codeSystem="2.999.1" displayName="useful data"/>**.

Example for one of the four Resource elements in case of ADR due to XDS [ITI-18]/[ITI-42]:

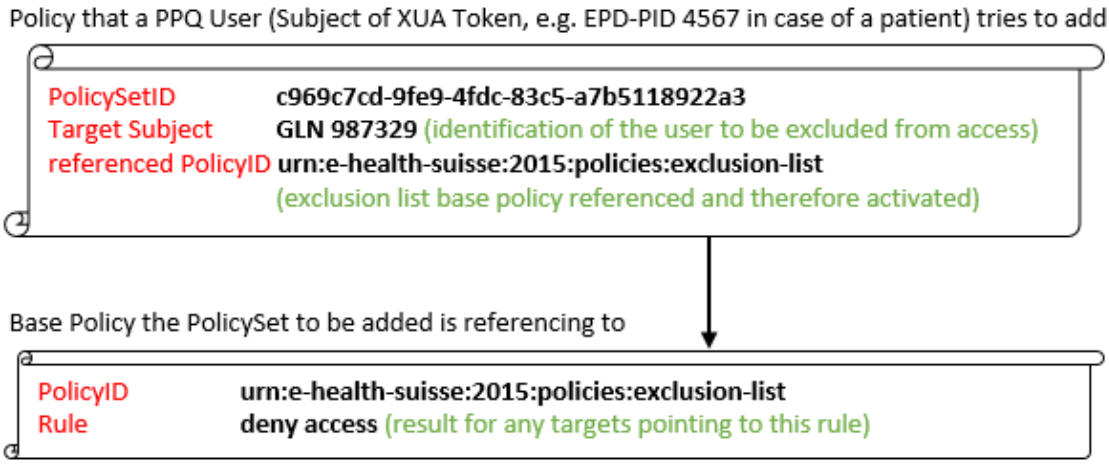
```
<Request>
  <Subject/>
  <Resource>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
               DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <AttributeValue>urn:e-health-suisse:2015:epd-subset:8901:useful</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:e-health-suisse:2015:epd-pid"
               DataType="urn:hl7-org:v3#II">
      <AttributeValue><hl7:InstanceIdentifier root="2.999.1" extension="8901"/></AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:ihe:iti:xds-b:2007:confidentiality-code"
               DataType="urn:hl7-org:v3#CV">
      <AttributeValue>
        <hl7:CodedValue code="2" codeSystem="2.999.2" displayName="useful data"/>
      </AttributeValue>
    </Attribute>
  </Resource>
  <Resource>
    <!-- resource element for medical documents corresponding to the example above -->
  </Resource>
  <Resource>
    <!-- resource elements for sensitive documents corresponding to the example above -->
  </Resource>
  <Resource>
    <!-- resource elements for confidential documents corresponding to the example above -->
  </Resource>
  <Action/>
  <Environment/>
</Request>
```

Listing 11: Example of the resource attributes of the XACMLAuthzDecisionQuery request payload. For better reading the part for one confidentiality code is shown in detail, while for the other confidentiality codes placeholders are used.

For ADR due to PPQ each Resource element MUST also contain the **referenced** policy **within** the policy set to be potentially returned, added, updated or deleted (according to the first resource attribute).
@AttributeId="urn:e-health-suisse:2015:policy-attributes:referenced-policy-set" and **DataType="urn:hl7-org:v3#CV"**.
The **<AttributeValue>** child element SHALL convey the Policy Identifier that is being referenced within the Policy Set to be queried, added, updated or deleted, e.g. **urn:e-health-suisse:2015:policies:exclusion-list**.

The following example is to clarify this requirement:
If a user (e.g. a patient) tries to add a policy set with ID c969c7cd-9fe9-4fdc-83c5-a7b5118922a3 (as in @AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id") that adds somebody (e.g. GLN 7609999999999) to the exclusion list, the policy set will contain a reference to another policy from the base configuration, which will have the policy set ID urn:e-health-suisse:2015:policies:exclusion-list. That's the value to be included within the Resource attribute @AttributeId="urn:e-health-suisse:2015:policy-attributes:referenced-policy-set".

An illustration of the usecase:



Correspondingly, the Resource element of an ADR due to PPQ transaction (to verify if the PPQ user 4567 may be allowed to perform this transaction) SHALL be constructed as in the following example:

```
<Request>
  <Subject/>
  <Resource>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id“
               DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <AttributeValue>c969c7cd-9fe9-4fdc-83c5-a7b5118922a3</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:e-health-suisse:2015:epd-pid“
               DataType="urn:hl7-org:v3#II">
      <AttributeValue><hl7:InstanceIdentifier root="2.999.1" extension="4567"/></AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:e-health-suisse:2015:policy-attributes:referenced-policy-set"
               DataType="urn:hl7-org:v3#CV">
      <AttributeValue>urn:e-health-suisse:2015:policies:exclusion-list</AttributeValue>
    </Attribute>
  </Resource>
  <Resource>
    <!—further resource elements-->
  </Resource>
  <Action/>
  <Environment/>
</Request>
```

Listing 12: Example of resource attributes of the XACMLAuthzDecisionQuery request payload for ADR due to PPQ to request an authorization decision for access to the patient's policy configuration.

<Action> identifies the transaction being performed by the Requester Entity. The <Action> element SHALL have one **<Attribute>** child element:

@AttributeId="urn:oasis:names:tc:xacml:1.0:action-id" and **@DataType="http://www.w3.org/2001/XMLSchema#anyURI"**.
The **<AttributeValue>** child element SHALL convey the action identifier:
urn:e-health-suisse:2015:policy-administration:PolicyQuery or
urn:e-health-suisse:2015:policy-administration:AddPolicy or
urn:e-health-suisse:2015:policy-administration:UpdatePolicy or
urn:e-health-suisse:2015:policy-administration:DeletePolicy for ADR due to PPQ or
urn:e-health-suisse:2015:action:RegistryStoredQuery for ADR due to XDS ITI-18 or
urn:e-health-suisse:2015:action:RegisterDocumentSet for ADR due to XDS ITI-42.

```
<Request>
  <Subject/>
  <Resource/>
  <Action>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action-id"
               DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <AttributeValue>urn:e-health-suisse:2015:policy-administration:AddPolicy</AttributeValue>
    </Attribute>
  </Action>
  <Environment/>
</Request>
```

Listing 13: Example of the action setting of XACMLAuthzDecisionQuery request for ADR due to PPQ.

<Environment> The EPD does not specify any <Environment> parameters within the XACMLAuthzDecisionQuery. Therefore this child element MAY be empty: **<Environment />**. The Authorization Decision Provider MAY ignore any attribute in this section when arriving at an authorization decision. However, there is a constraint to the use of <Environment> in case of inputContextOnly of <XACMLAuthzDecisionQuery> was set to true. In that case, current time and date MUST be provided as attributes of <Environment>.

3.1.7 Expected Actions

The Authorization Decisions Provider SHALL return Authorization Decisions that match the XACML Query parameters according to the rules defined in XACML policies.

The Authorization Decision Provider SHALL produce a XACMLAuthzDecisionQuery Response message that conveys the results of the evaluation of the patient's policies against the request. One result for each Resource SHALL be included in the response message.

3.1.8 XACMLAuthzDecisionQuery Response

The XACMLAuthzDecisionQuery Response message is created by the Authorization Decisions Provider in response to the XACMLAuthzDecisionQuery Request. This message conveys to the Authorization Decisions Consumer the results of the evaluation made by the Authorization Decisions Provider. For each Resource specified within the Request message, the Authorization Decisions Provider provides an Authorization Result that SHALL be used by the Authorization Decisions Consumer to determine which of the requested objects are to be returned or transactions to be allowed in response to the corresponding initial transactions. This message relies on OASIS SAML 2.0 profile of XACML v2.0 protocol standard. Authorization Results are conveyed using the XACMLAuthzDecisionStatement.

3.1.9 Trigger Events

This message is created by the Authorization Decisions Provider after the evaluation of the XACMLAuthzDecisionQuery Request message. The Authorization Decision Provider MUST only return Authorization Decisions applicable to the request.

3.1.10 Message Semantics

The XACMLAuthzDecisionQuery Response message is based on OASIS SAML 2.0 profile of XACML v2.0.
The WS-Addressing Action header of the SOAP message SHALL be:
urn:e-health-suisse:2015:policy-enforcement:XACMLAuthzDecisionQueryResponse

As defined in OASIS SAML 2.0 profile of XACML v2.0, the XACML Authorization Statement is conveyed within a SAML v2.0 Assertion. The Assertion does not need to be signed. In case of all Resources resulting in a decision of "Indeterminate" (details below), the SAML /Status/**StatusCode** of the Assertion shall be the same as the /Result/Status/StatusCode/@Value of the Response: urn:e-health-suisse:2015:error:not-holder-of-patient-policies. Otherwise the SAML /Status/**StatusCode** of the Assertion SHALL be supplied as defined in section 7.3.1 of OASIS SAML 2.0 profile of XACML v2.0.
The **<Issuer>** of the Authorization Assertion MUST identify the Authorization Decisions Provider. For the EPD this ID is specified to be the home community ID of the Authorization Decision Provider community encoded as an URN, e.g.
<saml:Issuer NameQualifier="urn:e-health-suisse:community-index">urn:oid:2.99</saml:Issuer>.

```
<soap:Body>
  <saml:Assertion
   xmlns:xacml-samlp="urn:oasis:xacml:2.0:saml:protocol:schema:os"
   xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
   xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os" xmlns:hl7="urn:ihe-d:hl7-org:v3"
   xsi:schemaLocation="urn:oasis:xacml:2.0:saml:assertion:schema:os access_control-xacml-2.0-saml-assertion-schema-os.xsd
   urn:ihe-d:hl7-org:v3 ihe-d-xacml-hl7-datatypes-base-1.0.xsd" ID="_79f6b857-f5ad-4b38-bebe-ef51aa9949b8"
   Version="2.0" IssueInstant="2016-02-05T09:30:10.5Z">
    <saml:Issuer NameQualifier="urn:e-health-suisse:community-index">urn:oid:2.999.1.1</saml:Issuer>
    <saml:Status>
      <samlp:StatusCode>urn:oasis:names:tc:SAML:2.0:status:Success</samlp:StatusCode>
    </saml:Status>
    <saml:Statement xsi:type="xacml-saml:XACMLAuthzDecisionStatementType">
    <xacml-context:Response>
        <!--Decision Result per Resource-->
      </xacml-context:Response>
    </saml:Statement>
  </saml:Assertion>
</soap:Body>
```

Listing 14: Schematic payload of the XACMLAuthzDecisionQuery response. For better reading the

details of the response is suppressed and shown in the listings below.
As specified in the OASIS multiple resource profile of XACML v2.0, the XACML **<Response>** element SHALL contain a **<Result>** element for each **<Resource>** element contained within the XACMLAuthzDecisionQuery Request message. Each <Result> element SHALL contain a @**ResourceId** attribute that identifies which Resource an Access Decision belongs to. A child element **<Decision>** holds the actual decision value.
In case of the decision code of a Result equaling to "Deny", "Permit" or "NotApplicable", the /Result/Status/**StatusCode**/@Value attribute SHALL equal to "urn:oasis:names:tc:xacml:1.0:status:ok". In case of "Indeterminate" it SHALL equal to "urn:e-health-suisse:2015:error:not-holder-of-patient-policies".
<Response> and all subsequent elements, attributes and values comply to the namespace xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os". The namespace is left out of the following examples for better reading purposes.

```
<Response>
  <Result ResourceId="e693657c-50be-46a6-bdcd-05269147f357">
    <Decision>Deny</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  <Result ResourceId="1c9fa73c-2b9c-41b2-a814-f9164e073c15">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  <Result ResourceId="c969c7cd-9fe9-4fdc-83c5-a7b5118922a3">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
</Response>
```

Listing 15: Example for a response to an ADR due to PPQ request.

```
<Response>
  <Result ResourceId="urn:e-health-suisse:2015:epd-subset:4567:useful">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  <Result ResourceId="urn:e-health-suisse:2015:epd-subset:4567:medical">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  <Result ResourceId="urn:e-health-suisse:2015:epd-subset:4567:sensitive">
    <Decision>NotApplicable</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
  <Result ResourceId="urn:e-health-suisse:2015:epd-subset:4567:confidential">
    <Decision>NotApplicable</Decision>
   <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
</Response>
```

Listing 16: Example for a Response to an ADR due to XDS message if 4567 was the patient ID (EPD-PID) of the Health Record to be accessed.

As defined in the XACML v2.0 standard, there are four possible values associated with the **<Decision>**. The Authorization Decisions Provider shall use these values as described below:

- **Permit**: if the evaluation was successful and the Subject is authorized to perform the Action on the Resource;
- **Deny:** if the evaluation was successful and the Subject is explicitly not authorized to perform the Action on the Resource.
- **NotApplicable**: if the evaluation was successful, but the Subject is not authorized to perform the Action on the Resource. E.g. a Permit decision can be determined on the Resource "useful data", but no permit or deny decision can be determined for the other resources in the request. The decision code for the other resources MUST be NotApplicable.
- **Indeterminate**: if the evaluation succeeded, but access to the requested Resource is not managed by the Authorization Decisions Manager, or if the evaluation failed. The EPD specifically defines this decision code to be returned, if access rights for a given patient are not managed in the associated Policy Repository and therefore cannot be determined by the Authorization Decision Provider. To distinguish between those two cases, clients may evaluate the /Result/Status/StatusCode/@Value attribute, which has to equal "urn:e-health-suisse:2015:error:not-holder-of-patient-policies" if the Policy Repository is not responsible for holding the given patient policies.

```
<Response>
  <Result ResourceId="urn:e-health-suisse:2015:epd-subset:4567:useful">
    <Decision>Indeterminate</Decision>
    <Status>
      <StatusCode Value="urn:e-health-suisse:2015:error:not-holder-of-patient-policies"/>
      <StatusMessage>Gemeinschaft ist nicht die Stammgemeinschaft des Patienten</StatusMessage>
    </Status>
  </Result>
  <Result ResourceId="urn:e-health-suisse:2015:epd-subset:4567:medical">
    <Decision>Indeterminate</Decision>
    <Status>
      <StatusCode Value="urn:e-health-suisse:2015:error:not-holder-of-patient-policies"/>
      <StatusMessage>Gemeinschaft ist nicht die Stammgemeinschaft des Patienten</StatusMessage>
    </Status>
  </Result>
  <Result ResourceId="urn:e-health-suisse:2015:epd-subset:4567:sensitive">
    <Decision>Indeterminate</Decision>
    <Status>
      <StatusCode Value="urn:e-health-suisse:2015:error:not-holder-of-patient-policies"/>
      <StatusMessage>Gemeinschaft ist nicht die Stammgemeinschaft des Patienten</StatusMessage>
    </Status>
  </Result>
  <Result ResourceId="urn:e-health-suisse:2015:epd-subset:4567:confidential">
    <Decision>Indeterminate</Decision>
    <Status>
      <StatusCode Value="urn:e-health-suisse:2015:error:not-holder-of-patient-policies"/>
      <StatusMessage>Gemeinschaft ist nicht die Stammgemeinschaft des Patienten</StatusMessage>
    </Status>
  </Result>
</Response>
```

Listing 17: The response to a XACMLAuthzDecisionQuery in the case when the patient's policies are not known in the requested community, i.e. when the requested community is not the patients referenceCommunity.

3.1.11 Expected Actions

When the Policy Enforcing Service Provider receives a XACMLAuthzDecisionQuery Response, it SHALL enforce the decision results according to the following EPD policy.

If a **Deny** or **NotApplicable** decision is returned, the

- XDS Document Registry SHALL not disclose the related document metadata in response to ITI-18;
- XDS Document Registry SHALL not store any document metadata from a submission set containing a document that has a confidentiality code for which such a decision was returned and return a XDS registration failure to the XDS Document Repository in response to ITI-42;
- PPQ Policy Repository SHALL not allow the initial PPQ transaction, respectively not return the policy data or make the requested changes to the policies.

If a **Permit** decision is returned, the

- XDS Document Registry SHALL disclose the document metadata with the given confidentiality code in response to ITI-18;
- XDS Document Registry SHALL perform the initiated transaction for a submission set containing documents with a corresponding confidentiality code as long as all of the documents of a submission set have a confidentiality code that was permitted by the ADR Response (otherwise see "Deny or NotApplicable" above);
- Policy Repository shall perform the initiated transactions, respectively return the policy data that has been queried for.

If **Indeterminate** is returned, the

- XDS Document Registry MUST request a decision from another Authorization Decisions Provider (XADR as defined below). If there is no Authorization Decisions Provider that returns Deny, NotApplicable or Permit, then the Document Registry SHALL not disclose any document metadata in response to ITI-18 or not perform the ITI-42 transaction respectively.
- PPQ Policy Repository SHALL not allow the initial PPQ transaction, respectively not return the policy data or make the requested changes to the policies.

3.1.12 Enforcement of XDS Retrieve Document Set transactions

The Retrieve of a document MUST be enforced according to the access rights formulated by the patient. If the document metadata of a document cannot be accessed by a user, a Retrieve of the corresponding document MUST be denied by the Document Repository. To implement this functionality, it is recommended for the Document Repositories to initialize a XDS Registry Stored Query [ITI-18] GetDocuments ObjectRef), combined with the XUA Identity Token provided by the Document Consumer [ITI-40], before supplying the document to the Consumer. If the corresponding Document Id is included in the XDS Registry Stored Query Response, the Document SHALL be supplied to the Document Source. If the corresponding Document Id is not included in the XDS Registry Query Response, the Document SHALL NOT be supplied to the Document Source.
The IHE SeR Profile may provide further guidance on the enforcement of access rights concerning the XDS Retrieve Document Set transaction.

3.1.13 Security Considerations

The Authorization Decisions Query transaction requires TLS communication between actors involved. This transaction mandates the creation of Authorizations associated at least with the Requester Entity and with the document metadata (confidentiality code) requested. If additional parameters need to be associated to the authorization, then the same parameters SHALL be provided within the Authorization Decisions Query transaction.

3.1.14 Authorization Decisions Consumer Audit Message

	Field Name	**Opt**	**Value Constraints**
Event	EventID	M	EV (110112, DCM,"Query")
	EventActionCode	M	E = Execute
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ADR", "e-health-suisse", "Authorization Decisions Query")
Source (Authorization Decisions Consumer) (1)			
Destination (Authorization Decisions Consumer) (1)			
Query Parameters (1..n)			
Requester Entity (1)			
Authorization Result (1..n)			

Source: AuditMessage/ ActiveParticipant	*UserID*	*U*	*not specialized*
	AlternativeUserID	MC	the process ID as used within the local operating system in the local system of logs
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	EV (110153, DCM, "Source")
	NetworkAccessPointTypeCode	U	"1" for machine (DNS) name "2" for IP address
	NetworkAccessPointID	U	The machine name or IP address, as specified in DICOM PS 3.15 A.5.3.

Destination: AuditMessage/ ActiveParticipant (1)	UserID	M	Authorization Decisions Provider SOAP URI
	AlternativeUserID	U	the process ID as used within the local operating system in the local system of logs
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	EV (110152, DCM, "Destination")
	NetworkAccessPointTypeCode	U	"1" for machine (DNS) name "2" for IP address
	NetworkAccessPointID	U	The machine name or IP address, as specified in DICOM PS 3.15 A.5.3.

Requester Entity: AuditMessage/ ParticipantObjectIdentification (1)	ParticipantObjectTypeCode	M	"1" (person)
	ParticipantObjectTypeCodeRole	M	"11" (security user entity)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("ADR", "e-health-suisse", "Authorization Decisions Query")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The Requester Entity (identified in the Attribute with AttributeId

			urn:oasis:names:tc:xacml:1.0:subject:subject-id)
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

Query Parameters: AuditMessage/ ParticipantObjectIdentification (1..n)	ParticipantObjectTypeCode	M	"2" (SYSTEM)
	ParticipantObjectTypeCodeRole	M	"24" (query)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("ADR", "e-health-suisse", "Authorization Decisions Query")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	*M*	*not specialized*
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	M	Resource-ID
	ParticipantObjectDetail	*U*	*not specialized*

Authorization Result: AuditMessage/ ParticipantObjectIdentification (1..n)	ParticipantObjectTypeCode	M	**"**2" (SYSTEM)
	ParticipantObjectTypeCodeRole	M	"13" (security resource)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("ADR", "e-health-suisse", "Authorization Decisions Query")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	Resource-ID
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	M	Decision Code (Permit, Deny, NotApplicable, Indeterminate)

3.1.15 Authorization Decisions Provider Audit Message

	Field Name	**Opt**	**Value Constraints**
Event	EventID	M	EV (110112, DCM,"Query")
	EventActionCode	M	E = Execute
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("ADR", "e-health-suisse", "Authorization Decisions Query")
Source (Authorization Decisions Provider) (1)			
Destination (Authorization Decisions Provider) (1)			
Query Parameters (1..n)			
Requester Entity (1)			
Authorization Result (1..n)			

Source: AuditMessage/ ActiveParticipant	*UserID*	*U*	*not specialized*
	AlternativeUserID	MC	the process ID as used within the local operating system in the local system of logs
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	EV (110153, DCM, "Source")
	NetworkAccessPointTypeCode	U	"1" for machine (DNS) name "2" for IP address
	NetworkAccessPointID	U	The machine name or IP address, as specified in DICOM PS 3.15 A.5.3.

Destination: AuditMessage/ ActiveParticipant (1)	UserID	M	Authorization Decisions Provider SOAP URI
	AlternativeUserID	U	the process ID as used within the local operating system in the local system of logs
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	EV (110152, DCM, "Destination")
	NetworkAccessPointTypeCode	U	"1" for machine (DNS) name "2" for IP address
	NetworkAccessPointID	U	The machine name or IP address, as specified in DICOM PS 3.15 A.5.3.

Requester Entity: AuditMessage/ ParticipantObjectIdentification (1)	ParticipantObjectTypeCode	M	"1" (person)
	ParticipantObjectTypeCodeRole	M	"11" (security user entity)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("ADR", "e-health-suisse", "Authorization Decisions Query")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The Requester Entity (identified in the Attribute with AttributeId urn:oasis:names:tc:xacml: 1.0:subject:subject-id)
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

Query Parameters: AuditMessage/ ParticipantObjectIdentification (1..n)	ParticipantObjectTypeCode	M	"2" (SYSTEM)
	ParticipantObjectTypeCodeRole	M	"24" (query)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("ADR", "e-health-suisse", "Authorization Decisions Query")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	*M*	*not specialized*
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	M	Resource-ID
	ParticipantObjectDetail	*U*	*not specialized*

Authorization Result: AuditMessage/ ParticipantObjectIdentification (1..n)	ParticipantObjectTypeCode	M	**"**2" (SYSTEM)
	ParticipantObjectTypeCodeRole	M	"13" (security resource)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("ADR", "e-health-suisse", "Authorization Decisions Query")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	Resource-ID
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	M	Decision Code (Permit, Deny, NotApplicable, Indeterminate)

3.2 Cross-Community Authorization Decision Request (XADR)

Within the EPD, the patient's Health Record access rights are to be stored within the patient's referenceCommunity only. However, each XDS Document Registry MUST act as Policy Enforcing Service Provider, even if the patient's Health Record access rights are not stored within the same community.
That means, any Authorization Decision Consumer grouped with a XDS Document Registry SHALL ask each Authorization Decision Provider, even outside their home community, until a response includes a decision code other than NotApplicable. The XADR request follows the same specification as ADR above. Only the service endpoint of an XADR Authorization Decision Provider will be outside of the community of the Authorization Decision Consumer. There may be strategies to be implemented to reduce the number of necessary service calls, which are out of scope of this specification.
For the Authorization Decision Consumer, grouped with a PPC Policy Repository, this is not a requirement, as patient access rights are always managed by a community specific Policy Manager. In that case, the Authorization Decision Provider is always grouped with the Policy Repository of the Policy Managers community, and therefore is the only source of an ADR due to PPC access decision.

3.3 Privacy Policy Query (PPQ)

3.3.1 Scope

These transactions are used by the Policy Manager to add, query, update or delete authorization policies (respectively XACML policy sets) stored in a Policy Repository.
This transaction is based on SOAP v1.2 exchange protocol and Synchronous Web services (See ITI TF-2x: Appendix V).

3.3.2 Referenced Standards

OASIS SOAP v1.2
OASIS Security Assertion Markup Language (SAML) v2.0
OASIS SAML 2.0 profile of XACML v2.0
OASIS eXtensible Access Control Markup Language (XACML) v2.0
OASIS Multiple Resource Profile of XACML v2.0

3.3.3 Interaction Diagrams

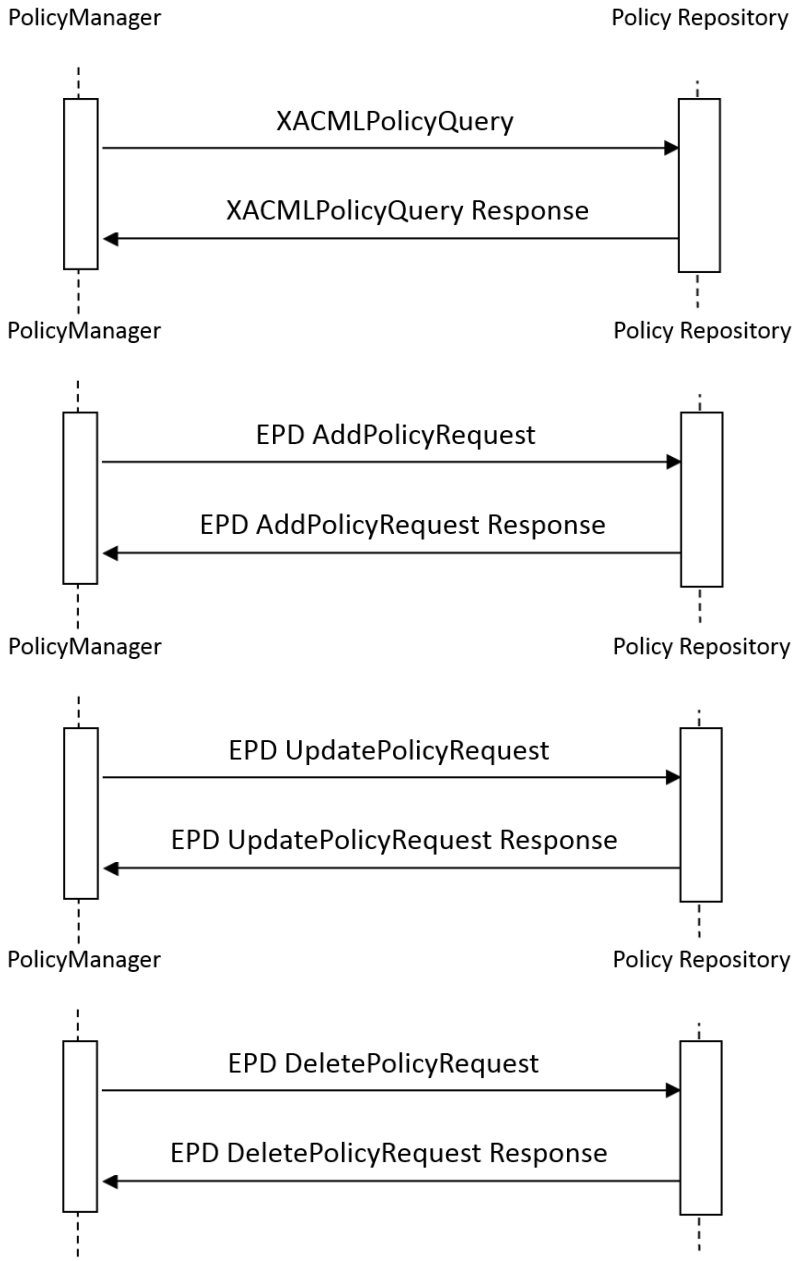


Figure 7: Sequence diagrams for the transactions of the PPQ profile to query, add, update and remove elements of the patient's privacy policy.

3.3.4 Message Semantics SOAP

PPQ Request messages SHALL use SOAP v1.2 message encoding.
The Addressing Action header of the SOAP message SHALL be:
urn:e-health-suisse:2015:policy-administration:PolicyQuery or
urn:e-health-suisse:2015:policy-administration:AddPolicy or
urn:e-health-suisse:2015:policy-administration:UpdatePolicy or
urn:e-health-suisse:2015:policy-administration:DeletePolicy, depending on the corresponding trigger event.
The recipient of the PPQ Request SHALL be identified by the WS-Addressing To header (URL of the endpoint).
A SAML 2.0 Identity Assertion SHALL be conveyed within the WS-Security Security header.

```
<soap:Envelope xmlns:soap=http://schemas.xmlsoap.org/soap/envelope/
               xmlns:wsa=http://www.w3.org/2005/08/addressing xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
               xmlns:wsse=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
               xmlns:ds=http://www.w3.org/2000/09/xmldsig# xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os"
               xmlns:xacml-samlp="urn:oasis:xacml:2.0:saml:protocol:schema:os"
               xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
               xmlns:epd="urn:e-health-suisse:2015:policy-administration"
               xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os" xmlns:hl7="urn:ihe-d:hl7-org:v3"
               xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/ http://schemas.xmlsoap.org/soap/envelope/
                                   http://www.w3.org/2005/08/addressing urn:e-health-suisse:2015:policy-administration
                                   epd-policy-administration-combined-schema-1.0-local.xsd ws-addr.xsd ">
  <soap:Header>
    <wsa:Action>urn:e-health-suisse:2015:policy-administration:PolicyQuery</wsa:Action><!--or-->
    <wsa:Action>urn:e-health-suisse:2015:policy-administration:AddPolicy</wsa:Action><!--or-->
    <wsa:Action>urn:e-health-suisse:2015:policy-administration:UpdatePolicy</wsa:Action><!--or-->
    <wsa:Action>urn:e-health-suisse:2015:policy-administration:DeletePolicy</wsa:Action>
    <wsa:MessageID>urn:uuid:feafcab1-1f9d-4d46-8321-8af925f55f13</wsa:MessageID>
    <wsa:To>urn:e-health-suisse:2015:actor:EpdPolicyRepository</wsa:To>
    <wsse:Security>
      <saml:Assertion>
        <!--SAML Assertion as described above-->
      </saml:Assertion>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    <!—PPQ TRANSACTION PAY LOAD-->
  </soap:Body>
</soap:Envelope>
```

Listing 18: The SOAP envelope with the security header, the SAML assertions and the transaction payload of the PPQ request. For better reading placeholder are used for the SAML assertions and the transaction payload.

PPQ Response messages SHALL use SOAP v1.2 message encoding.
The Addressing Action header of the SOAP message SHALL be:
urn:e-health-suisse:2015:policy-administration:PolicyQueryResponse or
urn:e-health-suisse:2015:policy-administration:AddPolicyResponse or
urn:e-health-suisse:2015:policy-administration:UpdatePolicyResponse or
urn:e-health-suisse:2015:policy-administration:DeletePolicyResponse, depending on the corresponding trigger event.
The recipient of the PPQ Response SHALL be identified by the WS-Addressing To header (URL of the endpoint).

```
<soap:Envelope xmlns:soap=http://schemas.xmlsoap.org/soap/envelope/
        xmlns:wsa=http://www.w3.org/2005/08/addressing xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
        xmlns:wsse=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
        xmlns:ds=http://www.w3.org/2000/09/xmldsig# xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os"
        xmlns:xacml-samlp="urn:oasis:xacml:2.0:saml:protocol:schema:os"
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
        xmlns:epd="urn:e-health-suisse:2015:policy-administration"
        xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os" xmlns:hl7="urn:ihe-d:hl7-org:v3"
        xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/ http://schemas.xmlsoap.org/soap/envelope/
                http://www.w3.org/2005/08/addressing urn:e-health-suisse:2015:policy-administration
                epd-policy-administration-combined-schema-1.0-local.xsd ws-addr.xsd ">
  <soap:Header>
   <wsa:Action>urn:e-health-suisse:2015:policy-administration:PolicyQueryResponse</wsa:Action><!--or-->
   <wsa:Action>urn:e-health-suisse:2015:policy-administration:AddPolicyResponse</wsa:Action><!--or-->
   <wsa:Action>urn:e-health-suisse:2015:policy-administration:UpdatePolicyResponse</wsa:Action><!--or-->
   <wsa:Action>urn:e-health-suisse:2015:policy-administration:DeletePolicyResponse</wsa:Action>
   <wsa:MessageID>urn:uuid:03010066-ba69-43d9-82b1-bb740f8c9a79</wsa:MessageID>
    <wsa:To>urn:e-health-suisse:2015:actor:EpdPolicyManager</wsa:To>
  </soap:Header>
  <soap:Body>
   <!—PPQ RESPONSE PAY LOAD-->
  </soap:Body>
</soap:Envelope>
```

Listing 19: The SOAP envelope with the transaction payload of the PPQ response. For better reading a placeholder is used the response payload.

3.3.5 XACMLPolicyQuery

This message enables the Policy Manager to query the Policy Repository for existing policies of a patient.
This message relies on SAML 2.0 profile of XACML v2.0.
Actors involved support XUA and use SAML identity assertions to identify current user entities for subsequent access enforcement.

3.3.6 Trigger Events

The Policy Manager sends this message when it needs to retrieve existing XACML policies or policy sets of a patient stored by a Policy Repository (of the patient's referenceCommunity).

3.3.7 Message Semantics

This message relies on a SAML v2.0 extension protocol element <xacml-samlp:XACMLPolicyQuery> (as specified in OASIS SAML 2.0 profile of XACML v2.0 to convey a **<Request>**, constructed by the XACML 2.0 policy schema. Following the XACML syntax, the Policy Manager asks for XACML Policies and Policy Sets that match a top-level **<Target>** constructed by a number of **<Resources>**. For the EPD, the patient identified by a patient ID (EPD-PID) is included as a Resource Attribute to be queried for (all policies matching that Resource SHALL be returned if allowed). The Policy Manager MAY query for single Policies too. In that case a Policy ID is required as the match target of the query.

```
<soap:Body>
  <xacml-samlp:XACMLPolicyQuery ID="357cf1d7-d87a-45f5-95ab-e91cbf68a7ad" Version="2.0"
                                IssueInstant=" 2016-02-09T09:30:10.5Z ">
   <xacml-context:Request>
    <xacml:Target>
      <xacml:Resources>
        <xacml:Resource>
          <xacml:ResourceMatch MatchId="urn:hl7-org:v3:function:II-equal">
            <xacml:AttributeValue DataType="urn:hl7-org:v3#II">
              <hl7:InstanceIdentifier root="2.999.1" extension="4567"/>
            </xacml:AttributeValue>
            <xacml:ResourceAttributeDesignator DataType="urn:hl7-org:v3#II"
                                               AttributeId="urn:ihe:iti:xds-b:2007:patient-id"/>
          </xacml:ResourceMatch>
        </xacml:Resource>
      </xacml:Resources>
    </xacml:Target>
   </xacml-context:Request>
  </xacml-samlp:XACMLPolicyQuery>
</soap:Body>
```

Listing 20: Example for the SOAP body element of a XACMLPolicyQuery payload with the XACML syntax to match all patient privacy policies of a specific patient, identified by the patient id.

3.3.8 Expected Actions

The Policy Repository SHALL return all XACML Policies or Policy Sets that match a specific Resource Attribute within their top-level <Target> element.

3.3.9 ACMLPolicyQuery Response

The XACMLPolicyQuery Response message is created by the Policy Repository in response to the XACMLPolicyQuery Request. In conformance to SAML 2.0 profile of XACML v2.0, the Policy Repository SHALL produce a SAML Assertion response message that conveys the resulting Policies and Policy Sets within a Policy Statement.

3.3.10 Trigger Events

This message is created by the Policy Repository after the evaluation of a XACMLPolicyQuery Request message. The Policy Repository identifies Policy Sets applicable to be returned to the requester.

3.3.11 Message Semantics

The **XACMLPolicy <Assertion>** as specified in OASIS SAML 2.0 Profile of XACML v2.0, is conveyed within a XACMLPolicy **<Response>**. The Assertion does not need to be signed.
The **<Issuer>** of the Assertion MUST identify the Policy Repository. For the EPD this ID is specified to be the home community ID of the Authorization Decision Provider community encoded as an URN, e.g.
<saml:Issuer NameQualifier="urn:e-health-suisse:community-index">urn:oid:2.99</saml:Issuer>. The SAML **StatusCode** of the /Assertion/Status of the Response SHALL be conveyed as defined in OASIS SAML 2.0 Profile of XACML v2.0, Section 7.3.2.

```
<soap:Body>
  <samlp:Response ID="4v7a68d0-5d67-557e-def4-8e5858676abc2" Version="2.0"
                  IssueInstant=" 2016-02-09T09:30:10.5Z ">
    <saml:Assertion ID="3b5a66d0-5d86-477e-afc4-8e561084edc9" Version="2.0"
                  IssueInstant=" 2016-02-09T09:30:10.5Z ">
      <saml:Issuer NameQualifier="urn:e-health-suisse:community-index">urn:oid:2.999.1</saml:Issuer>
      <saml:Status>
        <samlp:StatusCode>urn:oasis:names:tc:SAML:2.0:status:Success</samlp:StatusCode>
      </saml:Status>
      <saml:Statement xsi:type="xacml-saml:XACMLPolicyStatementType">
        <!—XACML Policy-->
      </saml:Statement>
    </saml:Assertion>
  </samlp:Response>
</soap:Body>
```

Listing 21: Structure of the SOAP body element of the response to a XACMLPolicyQuery. A placeholder is used for the XACML policies returned by the Policy Repository.

3.3.12 EPD AddPolicyRequest and EPD UpdatePolicyRequest

This message enables the Policy Manager to add or update XACML policies, respectively existing XACML Policy Sets of a patient.
This message relies on SAML 2.0 Profile of XACML v2.0.
Actors involved support XUA and use SAML identity assertions to identify current user entities for subsequent access enforcement.

3.3.13 Trigger Events

The Policy Manager sends these messages when it needs to add new or update existing patient-specific policy sets stored within the Policy Repository (of a patient's referenceCommunity).

3.3.14 Message Semantics

This message relies on an EPD specific transaction schema (epd-policy-administration-combined-schema-1.0-local.xsd) as the SAML 2.0 profile of XACML v2.0 does not provide a transaction type and schema REQUIRED by these requests. It uses the element **<AddPolicyRequest>** or **<UpdatePolicyRequest>** to identify the transaction and convey the request.
Otherwise it relies on the very same specification and concepts as the XACMLPolicyQuery Response message does. XACML Policies or Policy Sets to be added or updated are conveyed using a SAML **<Statement>** of type **XACMLPolicyStatementType** within a XACML Policy SAML **<Assertion>** as specified in OASIS SAML 2.0 profile of XACML v2.0. The Assertion does not need to be signed. The **<Issuer>** of the Assertion SHALL identify the Policy Manager. For the EPD this ID is specified to be the home community ID of the Authorization Decision Provider community encoded as an URN, e.g. **<saml:Issuer NameQualifier="urn:e-health-suisse:community-index">urn:oid:2.98</saml:Issuer>.**

```
<soap:Body>
  <epd:AddPolicyRequest> <!--or-->
  <epd:UpdatePolicyRequest>
    <saml:Assertion ID="_3b5a66d0-5d86-477e-afc4-8e561084edc9" Version="2.0"
                    IssueInstant="2016-02-09T09:30:10.5Z">
      <saml:Issuer NameQualifier="urn:e-health-suisse:community-index">urn:oid:2.98</saml:Issuer>
      <saml:Statement xsi:type="xacml-saml:XACMLPolicyStatementType">
        <!—XACML Policy-->
      </saml:Statement>
    </saml:Assertion>
  </epd:AddPolicyRequest> <!--or-->
  </epd:UpdatePolicyRequest>
</soap:Body>
```

Listing 22: Structure of the SOAP body element of the response to an AddPolicyRequest, with the policy to be conveyed injected in the Statement as denoted by the placeholder.

3.3.15 Expected Actions

The Policy Repository SHALL return a status according to the success or failure of the transaction as defined below.

3.3.16 EPD AddPolicyRequest Response and EPD UpdatePolicyRequest Response

The EPD AddPolicyRequest Response or EPD UpdatePolicyRequest Response message is created by the Policy Repository in response to the EPD AddPolicyRequest or EPD UpdatePolicyRequest message.
An EPD specific transaction EPD PolicyRepositoryResponse is applied to report a general success or failure code. A soap fault MUST be reported back to the Policy Manager in case an EPD UpdatePolicyRequest cannot be executed due to unknown Policy or Policy Set IDs.

3.3.17 Trigger Events

This message is created by the Policy Repository after the EPD AddPolicyRequest or EPD UpdatePolicyRequest have been executed or refused to be executed.

3.3.18 Message Semantics

The EPD specific transaction **<PolicyRepositoryResponse>** conveys a status **urn:e-health-suisse:2015:response-status:success** or **urn:e-health-suisse:2015:response-status:failure**.

```
<soap:Body>
  <epd:PolicyRepositoryResponse status="urn:e-health-suisse:2015:response-status:success"/>
</soap:Body>
```

```
<soap:Body>
  <epd:PolicyRepositoryResponse status="urn:e-health-suisse:2015:response-status:failure"/>
</soap:Body>
```

Listing 23: Status element of the response to a request to add or to update a policy.

In case of an update failure due to unknown Policy Set IDs a soap **<Fault>** with a **<faultcode>** value **epd-policy-administration:UnknownPolicySetId** is to be returned to the Policy Manager.

```
<soap:Body>
  <soap:Fault>
    <faultcode>epd-policy-administration:UnknownPolicySetId</faultcode>
    <faultstring>The PolicySet with the given PolicySet ID does not exist</faultstring>
  </soap:Fault>
</soap:Body>
```

Listing 24: The soap fault element with error message in the case of an failure of the update request.

3.3.19 EPD DeletePolicyRequest

This message enables the Policy Manager to delete XACML Policies or Policy Sets from a Policy Repository.
This message relies on SAML 2.0 profile of XACML v2.0.
Actors involved support XUA and use SAML identity assertions to identify current user entities for subsequent access enforcement (See ITI TF-1: 39.5 and 39.6).

3.3.20 Trigger Events

The Policy Manager sends these messages when it needs to delete existing patient-specific policy sets stored within the Policy Repository (of a patient's referenceCommunity).

3.3.21 Message Semantics

This message relies on an EPD specific transaction schema (epd-policy-administration-combined-schema-1.0-local.xsd) as the SAML 2.0 profile of XACML does not provide a transaction type and schema REQUIRED by this requests. It uses the element **<DeletePolicyRequest>** to identify the transaction and convey the request.
Otherwise it relies on the same specification and concepts as the XACMLPolicyQuery Response message, EPD AddPolicyRequest and EPD UpdatePolicyRequest do. However, there is no Statement type specified to convey the information needed by this transaction. Policies or Policy Sets to be deleted are to be identified by a corresponding ID that is to be conveyed using an EPD specific SAML **<Statement>** of type **XACMLPolicySetIdReferenceStatementType** (as defined in epd-policy-administration-combined-schema-1.0-local.xsd) within a XACML Policy SAML **<Assertion>**. The Assertion does not need to be signed.
The **<Issuer>** of the Assertion SHALL identify the Policy Manager. For the EPD this ID is specified to be the home community ID of the Authorization Decision Provider community encoded as an URN, e.g.
<saml:Issuer NameQualifier="urn:e-health-suisse:community-index">urn:oid:2.98</saml:Issuer>.

```
<soap:Body>
  <epd:DeletePolicyRequest>
    <saml:Assertion ID="_3b5a66d0-5d86-477e-afc4-8e561084edc9" Version="2.0"
                    IssueInstant="2016-02-09T09:30:10.5Z">
      <saml:Issuer NameQualifier="urn:e-health-suisse:community-index">urn:oid:2.98</saml:Issuer>
      <saml:Statement xsi:type="epd:XACMLPolicySetIdReferenceStatementType">
        <xacml:PolicySetIdReference>10a3f268-d9d6-4772-b908-9d8521161</xacml:PolicySetIdReference>
      </saml:Statement>
    </saml:Assertion>
  </epd:DeletePolicyRequest>
</soap:Body>
```

Listing 25: Example of the SOAP body for a EPD DeletePolicyRequest, where the policy set to be removed from the patients policy configuration is referenced by ID.

3.3.22 Expected Actions

The Policy Repository SHALL return a status according to the success or failure of the transaction as defined below.

3.3.23 EPD DeletePolicyRequest Response

The EPD DeletePolicyRequest Response message is created by the Policy Repository in response to the EPD DeletePolicyRequest.
An EPD specific transaction EPD PolicyRepositoryResponse is applied to report a general success or failure code. A soap fault MUST be reported back to the Policy Manager in case an EPD DeletePolicyRequest cannot be executed due to unknown Policy or Policy Set IDs.

3.3.24 Trigger Events

This message is created by the Policy Repository after the EPD DeletePolicyRequest or have been executed or refused to be executed.

3.3.25 Message Semantics

The EPD specific transaction **<PolicyRepositoryResponse>** conveys the status **urn:e-health-suisse:2015:response-status:success** or **urn:e-health-suisse:2015:response-status:failure**.

```
<soap:Body>
  <epd:PolicyRepositoryResponse status="urn:e-health-suisse:2015:response-status:success"/>
</soap:Body>
```

```
<soap:Body>
  <epd:PolicyRepositoryResponse status="urn:e-health-suisse:2015:response-status:failure"/>
</soap:Body>
```

Listing 26: Status element of the response to a request to add or to update a policy.

In case of an update failure due to unknown Policy Set IDs a soap **<Fault>** with a **<faultcode>** value **epd-policy-administration:UnknownPolicySetId** is to be returned to the Policy Manager.

```
<soap:Body>
  <soap:Fault>
    <faultcode>epd-policy-administration:UnknownPolicySetId</faultcode>
    <faultstring>The PolicySet with the given PolicySet ID does not exist</faultstring>
  </soap:Fault>
</soap:Body>
```

Listing 27: The soap fault element with error message in the case of a failure of the delete request.

3.3.26 Security Considerations

Relevant Security Considerations are defined in ITI TF-1: 39.5. The Privacy Policy Query transactions require TLS communication between actors involved. Relevant XDS Affinity Domain Security background is discussed in the XDS Security Considerations Section (see ITI TF-1: 10.7). The Actors involved SHALL record audit events according to the following:

3.3.27 Policy Manager Audit Message

	Field Name	**Opt**	**Value Constraints**
Event	EventID	M	EV (110112, DCM,"Query")
	EventActionCode	M	E = Execute
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("PPQ", "e-health-suisse", "Privacy Policy Query Policy Query") *EV*("PPQ", "e-health-suisse", *"Privacy Policy Query Add Policy")* *EV*("PPQ", "e-health-suisse", *"Privacy Policy Query Update Policy")* *EV*("PPQ", "e-health-suisse", *"Privacy Policy Query Delete Policy")*
Source (Policy Manager) (1)			
Human Requestor (0..n)			
Destination (Document Registry) (1)			
Audit Source (Document Consumer) (1)			
Patient (0..1)			
Query Parameters(1..n)			

Source: AuditMessage/ ActiveParticipant	*UserID*	*U*	*not specialized*
	AlternativeUserID	M	the process ID as used within the local operating system in the local system of logs
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	EV (110153, DCM, "Source")
	NetworkAccessPointTypeCode	U	"1" for machine (DNS) name "2" for IP address
	NetworkAccessPointID	U	The machine name or IP address.

Human Requestor (if known) AuditMessage/ ActiveParticipant	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	NA	
	NetworkAccessPointID	NA	

Destination AuditMessage/ ActiveParticipant	UserID	M	SOAP endpoint URI.
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	U	not specialized
	RoleIDCode	U	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address.

Audit Source AuditMessage/ AuditSourceIdentification	*AlternativeUserID*	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*

Patient (AuditMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCode	M	"1" (person)
	ParticipantObjectTypeCodeRole	M	"11" (patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	*not specialized*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

Query Parameters: AuditMessage/ ParticipantObjectIdentification (1..n)	ParticipantObjectTypeCode	M	"2" (SYSTEM)
	ParticipantObjectTypeCodeRole	M	"24" (query)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("PPQ", "e-health-suisse", "Privacy Policy Query Policy Query") *EV*("PPQ", "e-health-suisse", *"Privacy Policy Query Add Policy")* *EV*("PPQ", "e-health-suisse", *"Privacy Policy Query Update Policy")* *EV*("PPQ", "e-health-suisse", *"Privacy Policy Query Delete Policy")*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	*M*	*not specialized*
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	M	PolicySetId (PatientId for query all policies of a patient)
	ParticipantObjectDetail	*U*	*not specialized*

3.3.28 Policy Repository Audit Message

	Field Name	**Opt**	**Value Constraints**
Event	EventID	M	EV (110112, DCM,"Query")
	EventActionCode	M	E = Execute
	EventDateTime	*M*	*not specialized*
	EventOutcomeIndicator	*M*	*not specialized*
	EventTypeCode	M	EV("PPQ", "e-health-suisse", "Privacy Policy Query Policy Query") *EV*("PPQ", "e-health-suisse", *"Privacy Policy Query Add Policy")* *EV*("PPQ", "e-health-suisse", *"Privacy Policy Query Update Policy")* *EV*("PPQ", "e-health-suisse", *"Privacy Policy Query Delete Policy")*
Source (Policy Manager) (1)			
Destination (Policy Repository) (1)			
Audit Source (Policy Repository) (1)			
Patient (0..1)			
Query Parameters (1..n)			

Source: AuditMessage/ ActiveParticipant	UserID	*M*	*not specialized*
	AlternativeUserID	U	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	EV (110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name "2" for IP address
	NetworkAccessPointID	U	The machine name or IP address.

Destination: AuditMessage/ ActiveParticipant	UserID	M	SOAP endpoint URI.
	AlternativeUserID	M	the process ID as used within the local operating system in the local system of logs
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	EV (110152, DCM, "Destination")
	NetworkAccessPointTypeCode	U	"1" for machine (DNS) name "2" for IP address
	NetworkAccessPointID	U	The machine name or IP address.

Audit Source AuditMessage/ AuditSourceIdentification	*AlternativeUserID*	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*

Patient (AuditMessage/ ParticipantObjectIdentification)	ParticipantObjectTypeCode	M	"1" (person)
	ParticipantObjectTypeCodeRole	M	"1" (patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	*not specialized*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

Query Parameters: AuditMessage/ ParticipantObjectIdentification	ParticipantObjectTypeCode	M	"2" (SYSTEM)
	ParticipantObjectTypeCodeRole	M	"24" (query)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV("PPQ", "e-health-suisse", "Privacy Policy Query Policy Query") *EV*("PPQ", "e-health-suisse", *"Privacy Policy Query Add Policy")* *EV*("PPQ", "e-health-suisse", *"Privacy Policy Query Update Policy")* *EV*("PPQ", "e-health-suisse", *"Privacy Policy Query Delete Policy")*
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	*M*	*not specialized*
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	M	PolicySetId (PatientId for query all policies of a patient)
	ParticipantObjectDetail	*U*	*not specialized*

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI

Office fédéral de la santé publique OFSP
Unité de direction Politique de la santé

RS 816.11.n / Annexe 8 de l'ordonnance du DFI du … sur le dossier électronique du patient

Prescriptions sur la protection des moyens d'identification

Protection Profile for Electronic Means and their Authentication Procedures

Version: 1.0 22.03.2016

Entrée en vigueur: …

Table of Contents

PP Introduction

The Swiss Federal Law on Electronic Health Records (FLEHR) requires a strong authentication of identity for patients and healthcare professionals in order to access the Swiss Electronic Health Record (EHR). The Federal Council sets the requirements in relation to electronic identities and the issuing process for Electronic Identification Means (EIM) in detail. In this regard, EIM are used to identify patients and healthcare professionals to access the Swiss national electronic health record (EHR) via an access portal that is operated by communities (association of health professionals) and reference communities (communities with additional responsibilities related to the establishment of an account for the Electronic Patient Record). To assure a high confidence in the claimed identity of patients and healthcare professionals, the related processes for instantiation and issuance of identification means such as identity proofing and verification or credential issuance have to comply with the requirements for the level of assurance 3 as defined in ISO/IEC 29115:2013

The Protection Profile for Electronic Identification Means and their Authentication Procedures is based on the Regulations on the Electronic Patient Record (EPDV). It defines a set of requirements that are expected to be fulfilled by all products that can perform electronic identification and authentication to access the Swiss national EHR. The evaluation of EIM according this protection profile is part of the certification process of communities and reference communities, respectively.

1.1 PP Reference

Title:	Protection Profile for Electronic Identification Means and their Authentication Procedures
Version:	1.0
Date:	23.03.2016
Issuer:	Swiss Federal Office of Public Health
Evaluation Assurance Level	The assurance level for this PP is EAL2
CC Version	V3.1 Revision 4

1.2 TOE Overview

This protection profile defines the security objectives and requirements for EIM including their authentication procedures required to access the Swiss national EHR.

1.2.1 TOE definition

The Target of Evaluation (TOE) addressed by this protection profile comprises the components that are relevant to instantiate as an EIM towards relying parties (RP) in the EPDV context, namely it provides the following:

- An Identity Provider (IdP) for identification and authentication of registered users.
- Web services / middleware / internet visible access portal for authentication provided by IdP.
- Web service / middleware to create secure channel between IdP and service provider (i.e. community portal for patients and healthcare professionals) provided by IdP.
- Web service / middleware provided by service provider (i.e. community portal for patients and healthcare professionals) to receive authorization response from secure channel from IdP.
- Devices of multiple variety (e.g. smartcard, mobile devices) carrying tokens (e.g. application on mobile device) and/or credentials (e.g. public and secret key material, authentication credentials).
- Secure handover of randomized and time limited session from service provider to device (e. g. secure browser redirect or equivalent level)

1.2.2 TOE Usage

Electronic identification means comprises one or more token that are secured by a device. Each token may hold a credential, that is used by the IdP to authenticate the user's identity based on possession and control of the corresponding token. Figure 1 shows the steps required to authenticate patients and healthcare processionals to an access portal of communities.

In the first step, the holder of the token authenticates himself to the IdP (1) which provides a defined interface for that purpose. Specifically, this means an IdP-initiated approach where the IdP refers to service provider or relying party and, thus, the claimant may choose a specific context (2). In the next step, the IdP verifies the credentials of that user and after successful verification, the IdP transmits a proof of identity to the access providing system of the (reference-) community (3). The connection between IdP and service provider (SP) has to be established via secure channel. This channel shall also be used for initial notification of an approved patient's identity to the reference community of the patient. Although the IdP authorizes patients and healthcare professionals in order to grant access to the EHR, fine-grained permission control is left to the reference community.

To access the EHR, the session has to be handed over from the service provider to the IdP or the user's device (3,4). Afterwards, the user has access via the interface to the services authorized for this user in the (reference-) community.

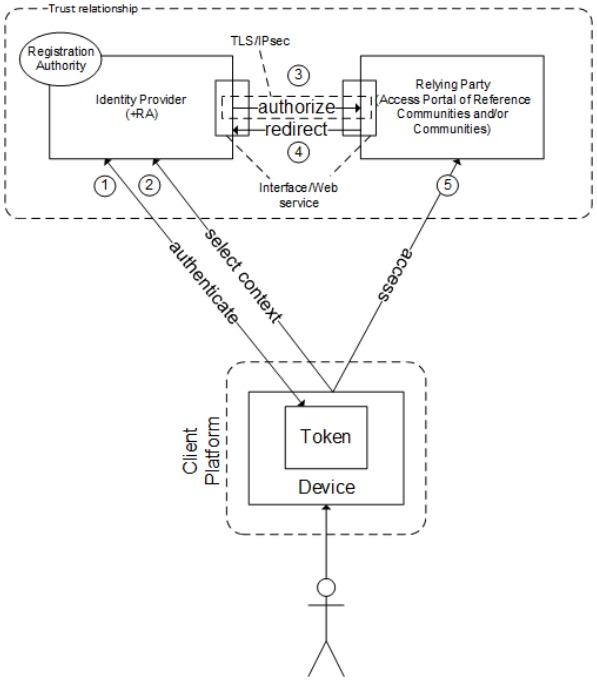


Figure 1 Usage of the TOE

1.3 Operational Environment

EIM have to be compliant with a specific level of assurance (LoA 3) as defined by ISO/IEC 29115:2013 [9]. It is assumed that EIM meet all necessary requirements related to enrolment, credential management and entity authentication such that there is a high confidence in the claimed or asserted identity of patients and healthcare professionals being allowed to access the EHR.

1.4 Physical Protection of the TOE

The physical protection is mainly provided by the TOE environment. This specifically covers the following scenarios:

- Access to the TOE infrastructure is not sufficiently restricted and the attacker gains unauthorized access to the server environment.
- The device is stolen and manipulated an attacker.

1.5 Assets

The assets to be protected by the TOE are data listed in Table 1. Assets of the TOE are divided into TSF and User data and the security services provided by the TOE as defined above. The data assets known to the TOE environment like public keys shall be protected by the TOE environment as well.

TSF data / User Data	Data	Description
User data	Device / Token with secret/public credential	A device that carries a secret/public credential of an individual user • Disseminated beforehand in a rollout process • Activation data or password is only known to the user Note that the device could be of multiple variety (e. g. Chipcard, Handheld-Device, Harddisk).
User data	Activation data for token	An activation secret for the token.
User data	Credential for web portal	A credential that is used for additional login into the access portal of the reference community.
User data	Secret and private credential of the user (on token)	The token stores secret and private credential of a user to authenticate the user has to be stored in a confidential and integrity protected way by the TOE.
User data	Reference of user credential	The IdP stores reference of the credential of a user to authenticate the user has to be stored in a confidential and integrity protected way by the TOE.
User data	Token output / authenticator	Authentication data that is transferred from the Token to the IdP Raw or transformed, e.g. in form of a cryptographic expression
User data	Identification Data	A unique tuple that identifies a user e.g. GLN, given birthname, birthdate, etc.
TSF data	Cryptographic Key Material for Channels	All cryptographic key material that is used to establish secure channels for communication between parts of the TOE or between the TOE and other trusted components as well as the browser.
TSF data	Claimant ID	A unique ID provided by the IdP to identify the claimant unanimously.
TSF data	Assertion Data	Any SAML assertion defined and generated by the TOE.

Table 1 Assets of the TOE divided into TSF and User data.

1.6 External Entities and Subjects

This protection profile considers the following subjects and external entities:

Entity	Description
User	A patient, a patient's representative, a Healthcare professional or an authorized supportive persons with access to the EDP, i.e. that have a identification token beforehand.
Trusted Users	Administrators, Operators and Security Information Officers that have privileged access rights to the EIM platform.
Temporary privileged users	Users that might have temporary privileged access rights, e.g. developers, support persons and auditors.
Test users and functional users	Technical users that might exist for management of the platform.
Attacker	A human, or a process acting on his behalf, located outside the TOE. The main goal of the attacker is to access or modify security relevant data.
Service Provider (Relying Party)	Data storage and infrastructure on (reference-) community site that is connected to the EIM and provides the access control for identified users (authorization control in accordance with the regulation). Additionally a secure channel exists between the (reference-) community infrastructure and the EIM.
RA (Registration Authority)	A trusted entity that establishes and vouches for the identity of a Subscriber/Claimant to an IdP. The RA may be an integral part of an IdP, or it may be independent of an IdP, but it has a relationship to the IdP(s).
IdP (Identity Service Provider)	A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The IdP may encompass Registration Authorities and verifiers that it operates. An IdP may be an independent third party, or may issue credentials for its own use.
Subscriber/Claimant	A user after successful identification and registration.
Client_Platform	The platform environment from which the user requests an identification process at the IdP. (e.g. for a user's PC with browser for redirect to the community access portal and a connected mobile device with the token).
Service desk	Portal within the IdP for user help and revocation requests

Table 2 External Entities and Subjects

2 Conformance Claims

- This PP has been developed using Version 3.1 R4 [1], [2], [3] of Common Criteria [CC].
- This PP does not claim conformance to any other PP.
- This PP requires strict conformance of any PP/ST to this PP.

This PP claims an assurance package EAL2 as defined in [CC] Part 3 for product certification.

3 Security Problem Definition

The Security Problem Definition is the part of a PP, which describes

- Assumptions on security relevant properties and behavior of the TOE's environment;
- Organizational security policies, which describe overall security requirements defined by the organization in charge of the overall system including the TOE. In particular this may include legal regulations, standards and technical specifications;
- Threats against the assets, which shall be averted by the TOE together with its environment.

3.1 Assumptions

Assumption	**Description**
A.Personal	It is assumed that background verification checks on all candidates for employment, contractors, and third party developers are carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. It is assumed that all employees and contractors understand their information security responsibilities, are authorized and trained for the roles for which they are considered and are aware of information security threats. Healthcare professionals and patients are assumed to always act with care and read the existing guidance documentation of the corresponding part of TOE. It is assumed, that holders of devices/tokens and other computing platforms keep secret activation/authentication data confidential, ensuring that it is not divulged to any other parties and avoid keeping a record on paper, in a software file or on a hand-held device, unless this can be stored securely and the method of storing has been approved.
A.AccessManagement	An Access Management is in place to control the allocation of access rights for authorized user access and to prevent unauthorized access to information systems and physical premises.
A.Physical	It is assumed, that the components of the TOE except for the enrolled device/token are operated in a secure area and protected against physical manipulations.
A.Monitoring	It is assumed, that information processing systems on the service providing part of the TOE are monitored and user activities, physical access to secure areas, exceptions, and information security events are recorded to ensure that information system problems are identified.

	It is assumed that the clocks of all relevant information processing systems are synchronized with an agreed accurate time source.
A.Malware	It is assumed, that that information processing systems on the service providing part of the TOE and its computing environment is protected against malware based on a malware detection and repair system service and information security awareness is introduced and practiced. It is also assumed, that a vulnerability management to prevent exploitation of technical vulnerabilities is established and maintained.
A.ClientPlatform	It is assumed, that the computing environment on which a part of the TOE is installed or interacts and has access to the services provided by the TOE, is protected against malware, its components have a current patch status and is not used in the administrator mode. It is assumed, that this computing environment is a general home-type environment. This means low physical security measures.
A.Identification	It is assumed that the claimant is carefully identified and well informed concerning practicing security awareness.
A.CredentialHandling	It is assumed that a mechanism to ensure that a credential is provided to the correct entity or an authorized representative is implemented. It is assumed that procedures ensure that a credential or means to generate a credential are only activated, if it is under the control of the intended entity. Therefore the device/token is protected against unauthorized access with activation data only known to the claimant. In the case of revocation due to compromise or loss of device/token, it is assumed, that the claimant informs immediately the service desk of the IdP through appropriate channels.
A.TrustedCommunityEndpoint	It is assumed, that the community provides a trusted endpoint for defined secure communication with the IdP.

Table 3 Assumptions

3.2 Organizational Security Policies (P)

The TOE and/or its environment shall comply with the following Organizational Security Policies (P) as security rules, procedures, practices, or guidelines imposed by an organization upon its operation.

Policy	Description
P.Audit	The security relevant events (internal to the TOE or due to the communication flows) shall be recorded and maintained and reviewed. The audit trail analysis is executed in order to hold the authorized users accountable for their actions and to trace attack attempts from networks. At minimum, the following items should be logged: - user IDs - dates, times, and details of key events - terminal identity - records of successful and rejected system access attempts - changes to system configuration - use of privileges network addresses and protocols
P.Crypto	State of the art recommended cryptographic functions shall be used to perform all cryptographic operations (e.g. NIST or other applicable guidance and recommendations). At least the following or stronger cryptographic algorithms shall be used: - SHA-2 - AES: n ≥ 256 - RSA: n ≥2048 - ECDSA: n ≥ 224
P.AccessRights	A defined management of admission to TOE and network resources shall be established that grants authenticated users access to specific resources based on policies and permission levels, assigned to users or user groups. The access control shall include an authentication, which proves the identity of the user or client entity attempting to log in. Administrative privileges allow users the right to make any and all changes on the TOE, including setting up accounts for other users and change SFR specific settings. The allocation and use of system administration privileges shall be more restricted and controlled.
P.Hardening	A defined policy for hardening the TOE shall be established and processes shall be implemented for securing the systems within the TOE by reducing its vulnerability. To achieve this, an effective vulnerability and patch management shall be established, unnecessary software shall be removed, unnecessary services shall disabled or removed and access rights and access to resources shall be strongly restricted and controlled.
P.Assertion	SAML-Token has to comply with the specification given in section 6.3. The IdP information processing system shall contain a component to generate unique reference identifiers. A time restricted SAML-Token issued by the IdP shall be digitally signed with an enhanced signature by a certified certificate service provider.
P.TrustedCommunityEndpoint	A trusted community endpoint for the secure communication between the IdP and the Community shall be established as defined in section 6.3.

Table 4 Description of the organizational security policies the TOE and its environment shall comply with

3.3 Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the assets protected by the TOE and the method of OE's use in the operational environment. The threats described in chapter 10.3 of the ISO/IEC 29115 are fully covered and extended by the following threats.

Threat	**Assets/ Security Goals / Adverse Action / Attacker**
T.CompromiseToken/Credential Compromise of a device/token and their credentials	Asset: Secret and private credential of the claimants device/token Security goal: The TOE and therefore all assets of the TOE Adverse action: Exposition of credential stored on a device/token - An attacker causes a IdP to create a credential based on a fictitious subscriber/claimant - An attacker alters information as it passes from the enrolment process to the credential creation process. - An attacker obtains a credential that does not belong to him and by masquerading as the rightful claimant causes the IdP to activate the credential. - An attacker has access to secret credentials stored on a device/token of a registered claimant with a weak credential protection mechanism and is therefore able to export or copy these secret credentials. Subsequently he is able to use these secret credentials for masquerading the rightful claimant (direct use or duplication of the token). - An attacker has either direct access to the activation data by breaking a weak protection mechanism or he can apply analytical methods outside the authentication mechanism (offline guessing) supported by a weak protection mechanism of the device/token. - An attacker can capture activation data or credentials by sending disguised malware as applications (e.g. keystroke logging software), which can be stored on a device. - The dissemination of revocation information is not timely leading to a threat of device/token with revoked credentials still being able to authenticate before the IdP updates the latest revocation information. Attacker: An Attacker alters information during the enrolment process of a device/token or gains access to a credential of a registered claimant and impersonates him or her either by credential tampering, credential disclosure, credential duplication, delayed credential revocation or offline guessing.
T.Token/CredentialTheft	Asset: Secret and private credential of the claimants device/token Security goal: The TOE and therefore all assets of the TOE

	Adverse action: A device/token that generates or contains credentials is stolen by an attacker Attacker: If an attacker also knows the activation data or has direct access to the activation data by breaking a weak protection mechanism or can apply analytical methods outside the authentication mechanism (offline guessing) favored by a weak protection mechanism of the device/token, he gain an authenticated access to the TOE and therefore all assets of the TOE.
T.WebPlatformAttacks	Asset: The TOE and therefore all assets of the TOE. Security goal: Confidentiality and integrity of the assets. Adverse action:. - Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities. - Cross-Site-Scripting (XSS) flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the claimant's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites. - A Cross-Site Request Forgery attack (CSRF) forces a logged-on claimant's browser to send a forged HTTP request, including the claimant's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the claimant's browser to generate requests the vulnerable application thinks are legitimate requests from the claimant. - Injection flaws, such as SQL, OS-Command-Shell, XPATH and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization. - Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect claimants to phishing or malware sites, or use forwards to access unauthorized pages. - Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

	Attacker: - Not correctly implemented authentication and session managements allow an attacker either capture or bypass the authentication methods that are used by a web application. He is able to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users identities (Unencrypted connections, predictable login credentials, vulnerable and unprotected session handling, no or too long timeouts, etc.) - An attacker can inject untrusted snippets of JavaScript into an application without validation. This JavaScript is then executed by the claimant who is visiting the target site. There are 3 primary types: In Reflected XSS, an attacker sends the claimant a link to the target application through email, social media, etc. This link has a script embedded within it which executes when visiting the target site. In Stored XSS, the attacker is able to plant a persistent script in the target website which will execute when anyone visits it. With DOM Based XSS, no HTTP request is required, the script is injected as a result of modifying the DOM of the target site in the client side code in the claimant's browser and is then executed. - Cross-Site Request Forgery (CSRF) is a web application vulnerability that makes it possible for an attacker to force a claimant to unknowingly perform actions while they are logged into an application. Attackers commonly use CSRF attacks to target sites such as cloud storage, social media, banking and on-line shopping, because of the user information and actions available in these applications. - All injection attacks involve allowing untrusted or manipulated requests, commands, or queries to be executed by a web application. An attacker wants to perform SQL inject they could write a SQL query to replace or concatenate an existing query used by the application, using specific characters like to bypass the existing query-logic. For an OS commanding injection an attacker can include a shell command within their injection using specific characters to include attacker's commands. Each attack could be tailored to the attacker's goal, the target server's infrastructure, and which inputs can bypass the application's existing logic. XPATH is the query language used to parse and extract specific data out of XML documents, and by injecting malicious input into an XPATH query, an attacker can alter the logic of the query. This attack is known as XPATH injection. - Applications that redirect after a successful authentication to another location by sending a redirect header to the client in an HTTP/HTTPS response, an attacker can without proper validation redirect claimants to phishing or malware sites, or use forwards to access unauthorized pages. - The web application needs to verify the request at the UI level, as well as the backend function level. An attacker will ignore the UI and a forge requests that access unauthorized functionality.

T.SpoofingAndMasquerading	Asset: The TOE and therefore all assets of the TOE. Security goal: The confidentiality and integrity of the assets. Adverse action: Spoofing and masquerading refer to situations in which an attacker impersonates another entity in order to launch attacks against network hosts, steal data, spread malware or bypass access controls. This may be done by making use of the credential(s) of an entity or otherwise posing as an entity (e.g. by forging a credential). Attacker: An attacker impersonates an entity spoofs one or more biometric characteristics that matches the pattern of the entity (by creating a “gummy” finger, recording voice, etc.) IP spoofing attacks can be used to overload targets with traffic or bypassing IP address-based authentication, when trust relationships between machines on a network and internal systems are in place. Such spoofing attacks impersonate machines with access permissions and bypass trust-based network security measures. An attacker spoofs a MAC address by having its device broadcast a MAC address that belongs to another device that has permissions on a particular network. In a DNS server spoofing attack, an attacker is able to modify the DNS server in order to reroute a specific domain name to a different IP address. This attack can also be used to masquerade a legitimate IdP with an attackers IdP or masquerade a legitimate software publisher responsible for downloading on-line software applications and/or updates by a faked downloading service.
T.SessionHijacking	Asset: Credentials, Session-IDs and other user data Security goal: The confidentiality and integrity of the assets Adverse action: An Attacker is able to intercept successful authentication exchange transactions between the claimant and the IdP and to steal or predict valid session data to gain compromised/unauthorized access to the web portal of the service provider. Without effective countermeasures, such attacks could be successfully performed using methods like Session Sniffing, Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc), Man-in-the-middle attacks, Man-in-the-browser attacks. Attacker: An Attacker is able to take over an already authenticated session by eavesdropping on or predicting the value of authentication data used to mark HTTP/HTTPS requests sent by the claimant to the IdP and subsequently gain compromised/unauthorized access to the web portal of the service provider. An attacker logs into a vulnerable application, establishing a valid

	session ID that will be used to trap the claimant. He then convinces the claimant to log into the same application, using the same session ID, giving the attacker access to the claimants account through this active session.
T.OnlineGuessing	Asset: User credentials Security goal: The confidentiality of assets Adverse action: An Attacker performs repeated logon trials by guessing possible values of the token authenticator. Attacker: An Attacker navigates to a web page and attempts to log in using brute force methods based on specific dictionaries.
T.ReplayAttack	Asset: Credentials, authentication exchange data Security goal: The confidentiality of assets Adverse action: An Attacker is able to replay previously captured messages (between a legitimate Claimant and an IdP) to authenticate as that Claimant to the IdP. Attacker: An Attacker captures a Claimant's credential or session IDs from an actual authentication session, and replays it to the IdP to gain access at a later time.
T.Eavesdropping	Asset: Credentials, authentication exchange data and other user data Security goal: The confidentiality of communication channels and assets of the TOE Adverse action: An Attacker listens passively to the authentication transaction to capture information which can be used in a subsequent active attack to masquerade as the Claimant. A way to achieve this, the attacker positions himself in between the Claimant and the IdP, so that he can intercept the content of the authentication protocol messages. The Attacker typically impersonates the IdP to the Claimant and simultaneously impersonates the Claimant to the IdP. Conducting an active exchange with both parties simultaneously may allow the Attacker to use authentication messages sent by one legitimate party to successfully authenticate to the other. Attacker: An Attacker captures the transmission credentials or Session IDs

	from a Claimant to a IdP.
T.Configuration	Asset: The TOE and therefore all assets of the TOE. Security Goal: Confidentiality and integrity of the assets. Adverse action: An unauthenticated or authenticated attacker might exploit a weakness resulting from a wrong configuration setting, incomplete deployment or not up-to-dated software (libraries, frameworks, and other software modules, almost always running with full privileges) of TSF components of the TOE (applications, frameworks, application servers, web servers, database servers and platforms) Attacker: An unauthenticated or authenticated attacker is able to exploit a weakness by wrong configuration setting, incomplete deployment or not up-to-dated software to expose confidential information about user data or TSF data.
T.DoS	Asset: The TOE and therefore all assets of the TOE. (The availability of the TOE). Security goal: The Denial of Service (DoS) attack is focused on making TSF components of the TOE (site, application, server) unavailable for the purpose there were designed. Adverse action: An attacker is able to manipulate network packets, programming, logical, or resources handling vulnerabilities, etc. Attacker: An (unauthenticated) attacker is able to start a DoS attack on the external interfaces of the TOE (namely browser interface and web service) so that a service receives a very large number of requests and may cease to be available to legitimate users. An (unauthenticated) attacker is also able to stop a service, if a programming vulnerability is exploited or to slow down using too much service handles.

Table 5 Threats

4 Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment.

4.1 Security Objectives for the TOE

This section describes the security objectives for the TOE and addresses the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE. The security objectives describe the protection of the primary assets as User Data and the secondary assets as TOE security functions data (TSF data) against threats identified in TOE environment.

O.Integrity	The TOE shall protect against either intentional or accidental violation of user and TSF data integrity (the property that data has not been altered in an unauthorized manner) or violation of system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).
O.Confidentiality	The TOE shall protect user and TSF data against intentional or accidental attempts to perform unauthorized access. The TOE shall protect confidentiality of user and TSF data in storage, during processing and while in transit.
O.Availability	The TOE shall ensure the availability of services provided by the TOE and the TSF to authorized users (e.g. the IdP is unavailable to subscribers as a consequence of a DoS attack or insufficient scalability).
O.Accountability	The TOE shall trace all actions of an entity uniquely to that entity. The TOE shall record user activities, exceptions, and information security events and shall keep these for an agreed period to assist in future investigations and in access control monitoring.
O.Authentication	Towards the service provider: All messages between IdP and their relaying parties shall be digitally signed to guarantee the authenticity and validity shall be time limited. Towards the client platform: The TOE shall provide either a token with two or more authentication factors (multifactor token) or a combination of a single-factor token and at least another token transmitted on a separate channel for authentication. The factors shall comply with the requirements of ISO 29115.
O.Secure_Communication	The TOE shall support secure communication for protection of the confidentiality and the integrity of the user data and TSF data received or transmitted. Further nonces, challenges or timeliness shall be used for freshness of each transaction.
O.Cryptographic_Functions	The TOE shall provide means to encrypt and decrypt user data and TSF data to maintain confidentiality, integrity and accountability and allow for detection of modification of user data that is transmitted within or outside of the TOE.
O.Access_Control	The TOE shall enable access control on all objects under the control of the TOE (e.g. assets) as well as the TSF and ensure authorized use while preventing unauthorized use.

4.2 Security Objectives for the operational environment

This section describes security objectives that the TOE should address in the operational environment to solve problems with regard to the threats and organizational security policies defined as the security problems. In addition, the security objectives stated herein shall all be derived from the assumptions.

OE.HR-Security	Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy. A written and signed agreement is mandatory as part of contractual obligation for employees, contractors and third party users. Conditions of their employment contract shall state their and the organization's responsibilities for information security. All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures as relevant for their job function. Responsibilities and defined processes shall be in place to ensure an employee's, contractor's or third party user's exit from the organization and that the return of all assets and the removal of all access rights are completed. The following controls shall be fulfilled: [ISO/IEC 27001:2013][8]: A.7 Human resource security
OE.Access_ManagementSystem	Secure Operation of the TOE requires an access-management-system for which an access control policy shall be established, documented and reviewed based on business and information security requirements. Access to systems and applications shall be restricted in accordance with the access control policy. A formal user registration and de-registration process shall be implemented to enable assignment of access rights. The allocation and use of privileged access rights shall be restricted and controlled. Password management systems shall be interactive and shall ensure strong passwords. The following controls shall be applied and fulfilled: - [ISO/IEC 27001:2013]: A.9 Access Control
OE. SecureAreas and Equipment	Critical or sensitive information processing facilities of the IdP shall be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They shall be physically protected from unauthorized access, damage and loss including safeguard supporting facilities, such as the electrical supply and cabling infrastructure. The following controls shall be applied and fulfilled: - [ISO/IEC 27001:2013]: A.11 Physical and environmental security
OE.Configuration and ChangeManagement	In order to ensure the integrity of information processing systems of the IdP, there shall be established strict controls over the implementation of changes. Formal change

	control procedures shall be enforced. They should ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained. Defined policies and configuration procedures or systems shall be established to keep control of all implemented software as well as the system documentation. The following controls shall be applied and fulfilled: - [ISO/IEC 27001:2013]: A.12.1.2 Change management - [ISO/IEC 27001:2013]: A.12.5 Control of operational software
OE.Malware and Vulnerability Management	The information processing systems of the IdP shall be protected against malicious code and based on malware code detection, security awareness, and appropriate system access and change management controls. Information resources to be used to identify relevant technical vulnerabilities and to maintain awareness have to be defined and made available. When a potential technical vulnerability has been identified, associated risks shall be identified and the following actions shall be taken: - patching the vulnerable systems or - turning off services or capabilities related to the vulnerability - adapting or adding access controls, e.g. firewalls - increased monitoring to detect actual attacks - raising awareness of the vulnerability The following controls shall be applied and fulfilled: - [ISO/IEC 27001:2013]: A.12.2 Protection from malware - [ISO/IEC 27001:2013]: A.12.6 Technical vulnerability management
OE.Logging and Monitoring	The information processing systems of the IdP shall be monitored and information security events shall be recorded. Operator logs and fault logging shall be used to ensure information system problems are identified. Logging facilities and log information should be protected against tampering and unauthorized access. The clocks of all relevant information processing systems shall be synchronized with an accepted Swiss time source to ensure the accuracy of audit logs. The following controls shall be applied and fulfilled: - [ISO/IEC 27001:2013]: A.12.4 Logging and monitoring
OE.Network Security	A policy concerning the use of networks and network services shall exist and implemented. All authentication methods with respect to the security requirements used to control access by remote users shall be defined and documented. Groups of information services, users, and information processing systems in the IdP shall be segregated on networks. Routing controls shall be implemented for networks to ensure that information processing systems connections and information flows do not breach the access control policies. The following controls shall be applied and fulfilled:

	- [ISO/IEC 27001:2013]: A.13.1 Network security management
OE.Identification and IdentityManagement	Secure Operation of the TOE requires the following steps taken beforehand regarding an Identification- and Identity-Management-System: 1. Before a claimant (subscriber) enters into a contractual relationship with a Registration Authority [RA], he shall be informed of the precise terms and conditions by the RA regarding the use of the device/token. 2. The RA shall perform all identity proofing in accordance with the published identity proofing policy and ensure, that subscribers are properly identified and registered. 3. The RA shall accept requests with qualified digital signatures for claimants possessing valid certificates. 4. The RA shall record the signed agreement with the claimant (subscriber). 5. Records with the actions of the RAs and IdPs, shall be stored in corresponding event journals. 6. Communications between the RA and the IdP shall be authenticated and secure. 7. If external RAs are used, a documented process for validating and authorising external registration authorities respecting the information security requirements shall be implemented. 8. The IdP shall provide a policy for managing the identity information lifecycle 9. Processes to maintain the accuracy of the identity information and controls to verify policies, regulations, business requirements and to improve processes shall be established by the IdP. 10. Policies to specify the conditions and procedures to archive identity information shall be established by the IdP. 11. The IdP shall provide policies to specify the conditions and procedures to initiate deletion of identity information. The following controls shall be fulfilled: - [ISO/IEC 29115:2013]: 10.1 Threats to, and controls for, the enrolment phase - [ISO/IEC 24760-2:2015][10]: 6.2 Access policy for identity information - [ISO/IEC 24760-2:2015]: 6.3.1 Policy for identity information life cycle - [ISO/IEC 24760-2:2015]: 6.3.2 Conditions and procedure to maintain identity information - [ISO/IEC 24760-2:2015]: 6.3.5 Identity information quality and compliance - [ISO/IEC 24760-2:2015]: 6.3.6 Archiving information - [ISO/IEC 24760-2:2015]: 6.3.7 Terminating and deleting identity information
OE.Credential Management	1. The IDP shall establish procedures to ensure that the individual who receives the device/token is the same individual who participated in the registration procedure. 2. For issuing a device/token, procedures shall be established, which allow the subscriber to authenticate

	the IdP as the source of the delivered device/token and to check its integrity. 3. The IdP shall revoke a device/token based on a unique identifying attribute in a token or in a credential (e.g. serial number) within a specific time period as defined by a corresponding policy or immediately, when stolen or compromised. An on-line revocation/status checking availability shall be implemented and maintained as well as a web site, on which revocation requests can be submitted in an authenticated manner (security questions, out-of-band notification, etc.) by the claimants. The following controls shall be applied and fulfilled: - [ISO/IEC 29115:2013]: 10.2 Threats to, and controls for, the credential management phase
OE.Operations Security	To ensure correct and secure operations of information processing systems, the IdP shall also implement, maintain and control processes according to the following security controls of the ISO/IEC 27001 Standard: - [ISO/IEC 27001:2013]: A. 12.3 Backup - [ISO/IEC 27001:2013]: A.14.2.1 Secure development policy - [ISO/IEC 27001:2013]: A.14.2.5 Secure system engineering principles - [ISO/IEC 27001:2013]: A.15 Supplier relationships - [ISO/IEC 27001:2013]: A.16 Information security incident management - [ISO/IEC 27001:2013]: A.18.1.3 Protection of records - [ISO/IEC 27001:2013]: A.18.1.4 Privacy and protection of personally identifiable information - [ISO/IEC 27001:2013]: A. 18.2.2 Compliance with security policies and standards
OE.User Security Awareness	1. The RA shall inform the claimant/subscriber through an agreement to submit accurate and complete information to the legal requirements according EPDV, particularly within the registration process. 2. The RA shall inform the claimant/subscriber through an agreement to protect his device/token and furthermore to: - use the device/token only for authentication and in accordance with any other limitations notified to the claimant/subscriber - exercise care to prevent unauthorised use of its device/token 3. The RA shall inform the claimant/subscriber through an agreement and to notify the IdP without any reasonable delay, if any of the following events should occur before the end of the validity period: - the claimant's device/token has been lost, stolen or potentially compromised - control over the claimant's device/token has been lost due to a compromised activation data or other reasons. 4. Claimants shall be aware to communicate revocation requests through protected and authenticated channels with an appropriate user authentication and validation (security questions, out-of-band notification,

	etc.). 5. The RA shall made aware the claimant/subscriber of his responsibilities for maintaining effective access controls, particularly regarding the use of his activation data. 6. The RA shall made aware, that the claimant/subscriber shall keep his computing environment on which the part of the TOE is installed or interacts integer. To achieve this requirement, an anti-virus and personal firewall shall be installed and kept up to date. The entire computing environment shall be updated with the last patches und security updates. The claimant shall be aware and extremely cautious when downloading and/or running executable content such as programs, scripts, macros, add-ons, apps, etc. in order to prevent attacks on the integrity of the computing environment.

Table 6 Security Objectives for the operational environment

4.3 Security Objectives rationale

This chapter describes rationales for the effectiveness of the security objectives stated above for individual parameters of the security problem definition.

4.3.1 Overview

	O.Integrity	O.Confidentiality	O.Availability	O.Accountability	O.Authentication	O.Secure_Communication	O.Cryptographic_Functions	O.Access_Control	OE.HR-Security	OE.Access_ManagementSystem	OE. SecureAreas and Equipment	OE.Configuration and ChangeManagement	OE.Malware and Vulnerability Management	OE.Logging and Monitoring	OE.Network Security	OE.Identification and IdentityManagement	OE.Credential Management	OE.Operations Security	OE.User Security Awareness
P.Audit	X	X		X										X					
P.Crypto	X	X				X	X								X				
P.AccessRights		X			X			X		X									
P.Hardening													X						
T.CompromiseToken/Credential	X	X			X	X	X												X
T.Token/CredentialTheft								X									X		X
T.WebPlatformAttacks						X						X	X	X	X				

	O.Integrity	O.Confidentiality	O.Availability	O.Accountability	O.Authentication	O.Secure_Communication	O.Cryptographic_Functions	O.Access_Control	OE.HR-Security	OE.Access_ManagementSystem	OE. SecureAreas and Equipment	OE.Configuration and ChangeManagement	OE.Malware and Vulnerability Management	OE.Logging and Monitoring	OE.Network Security	OE.Identification and IdentityManagement	OE.Credential Management	OE.Operations Security	OE.User Security Awareness
T.SpoofingAndMasquerading	X	X		X	X	X								X					
T.SessionHijacking	X	X				X									X				
T.Online_Guessing				X	X									X					
T.ReplayAttack				X		X								X					
T.Eavesdropping		X				X									X				
T.Configuration									X			X							
T.DoS			X									X	X		X				
A.Personal																			
A.AcccessManagement																			
A.Physical																			
A.Monitoring														X					
A.Malware													X						
A.Identification																X			
A.Credential Handling																	X		
A.SystemOperation																		X	
A.Client_Platform																			X

Table 7 Rationale for the security objectives

4.3.2 Countering the threats

4.3.2.1 **T.CompromiseToken/Credential**

The threat **T.CompromiseToken/Credential** addresses all compromises of a device/token and their credentials meaning that an attacker gains access to a credential of a registered claimant and impersonates him or her either by credential tampering, credential disclosure, credential duplication, delayed credential revocation or offline guessing.

The protection against this threat is mainly achieved by the security objectives **O.Integrity** by ensuring TSF data integrity, **O.Confidentiality** by ensuring that TSF Data has not been altered in an unauthorized manner, **O.Authentication** by ensuring authenticity and a strong authentication with regard to the client platform, **O.Secure_Communication** by protection of confidentiality and integrity of the received and transmitted user and TSF data and **O.Cryptographic_Functions** by encryption of TSF and User data of the TOE. Furthermore, the security objective for the operational environment **OE.User Security Awareness** shall ensure that the claimant/subscriber is aware of his responsibilities for maintaining effective access controls and obligations with regard to stolen, lost or compromised devices/tokens.

4.3.2.2 **T.Token/CredentialTheft**

The threat **T.Token/CredentialTheft** describes the situation where the token or device has been stolen by an attacker. The attacker then gains access to the TSF data for instance by knowing the activation data and therefore gains access to the TOE.

This threat is countered by the security objectives **O.Access_Control** and the objectives for the TOE environment **OE.Credential Management** and **OE.User Security Awareness**. The objective **O.Access_Control** sets the requirements to prevent unauthorized use by the establishment of access control of all objects under the control of the TOE and the TSF. The objective for the TOE environment **OE.Credential Management** shall ensure secure issuing procedures regarding the device and token and procedures for immediate revocation of stolen or lost devices/tokens.

4.3.2.3 **T.WebPlatformAttacks**

The threat **T.WebPlatformAttacks** addresses incorrect or faulty implementation of application functions related to authentication and session management that allows an attacker to compromise passwords, keys or session tokens by using exploits such as Cross-Site-Scripting, Cross-Site Request Forgery attacks or Injection exploits.

The protection against this threat is achieved by the security objectives **O.Secure_Communication** and the objectives for the TOEs environment **OE.Configuration and ChangeManagement**, **OE.Malware and Vulnerability Management** and **OE.Network Security**. The objective **OE.Malware and Vulnerability Management** ensures that information processing systems are protected against malicious code and that appropriate measures such as malware code detection are in place beside appropriate system access and change management controls. The objective **OE.Network Security** counters this threat by ensuring the security of information in networks and the protection of connected services from unauthorized access. The objective **OE.Configuration and ChangeManagement** counters this threat by ensuring that security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.

4.3.2.4 T.SpoofingAndMasquerading

The threat **T.SpoofingAndMasquerading** refers to situations in which an attacker impersonates another entity in order to launch attacks against network hosts, steal data, spread malware or bypass access controls. This may be done by making use of the credential(s) of an entity or otherwise posing as an entity (e.g. by forging a credential).

The protection against this threat is mainly achieved by the security objectives **O.Integrity**, **O.Confidentiality**, **O.Accountability**, **O.Authentication**, **O.Secure_Communication** and the objective for the TOE environment **OE.Logging and Monitoring**. The objectives **O.Integrity** and **O.Confidentiality** shall ensure that TSF data has not been accessed or altered in an unauthorized manner such that the attacker will not be able to masquerade as the owner of the token/device. The objective **O.Accountability** shall ensure that all actions of an entity specifically to establish future investigations and access control monitoring. The objective **O.Authentication** requires any message to be digitally signed and **O.Secure_Communication** that secure communication is supported by the TOE. The objective **OE.Logging and Monitoring** further requires logs and fault logging to ensure information that system problems are identified.

4.3.2.5 T.SessionHijacking

The threat **T.SessionHijacking** addresses the situation where an attacker is able to intercept successful authentication exchange transactions between the claimant and the IdP and to steal or predict valid session data to gain compromised/unauthorized access to the web portal of the service provider.

The protection against this threat is achieved by the security objectives **O.Integrity**, **O.Confidentiality**, **O.Secure_Communication** providing integrity secured, confidential secure channels between the trusted entities. Further it is ensured by the objective for the TOE environment **OE.Network Security**.

4.3.2.6 **T.Online_Guessing**

The threat **T.Online_Guessing** addresses guessing of the token authenticator for instance by using brute force methods based on specific dictionaries.

The protection of this threat is achieved by the objectives **O.Accountability**, ensuring unique tracing of all actions to an entity and **O.Authentication** requiring use of a multi-authentication factor token and supportively the objective for the TOE environment **OE.Logging and Monitoring**.

4.3.2.7 T.ReplayAttack

The threat **T.ReplayAttack** addresses replaying of previously captured messages between the claimant and the IdP in order to authenticate as that claimant.

The protection of this threat is achieved by the security objectives **O.Accountability**, **O.Secure_Communication**, specifically providing nonces or challenges to prove the freshness of the transaction and supportively the objective for the TOE environment **OE.Logging and Monitoring**.

4.3.2.8 **T.Eavesdropping**

The threat **T.Eavesdropping** addresses passively listening to authentication transactions and to capture information that can be used in a subsequent active attack to masquerade as the claimant.

The protection of this threat is achieved by the security objectives **O.Confidentiality**, **O.Secure_Communication**, specifically encrypting all communication appropriately and supportively the objective for the TOE environment **OE.Network Security**.

4.3.2.9 **T.Configuration**

The threat **T.Configuration** addresses exploiting of weaknesses resulting from a wrong configuration setting, incomplete deployment or not up-to-date software of TSF

The protection of this threat is achieved by the security objectives for the TOE environment **OE.HR-Security** and **OE.Configuration and ChangeManagement**.

4.3.2.10 **T.DoS**

The threat **T.DoS** addresses denial of service attacks focussing on TSF in order to make them unavailable.

The protection of this threat is achieved by the security objectives **O.Availability** and the objectives for the TOE environment **OE.Configuration and ChangeManagement**, **OE.Malware and Vulnerability Management** and **OE.Network Security**.

5 Security Requirements

5.1 Overview

The CC allows several operations to be performed on functional components: refinement, selection, assignment, and iteration are defined in chapter C.4 of part 1 of the CC. Each of these operations is used in this PP.

The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is (1) denoted by the word “refinement” in a footnote and the added/changed words are in bold text, or (2) included in text as underlined text and marked by a footnote. In cases where words from a CC requirement were deleted, a separate attachment indicates
10 the words that were removed.

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are italicized.

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are italicized.

20 **5.2 Security Functional Requirements for the TOE**

This section on security functional requirements (SFR) for the TOE is divided into sub-section following the main security functionality.

5.2.1 Security audit automatic response (FAU_ARP)

FAU_ARP.1 Security alarms

FIA_ARP.1.1	The TSF shall take [one or more of the following actions: audible alarm, SNMP trap, log, email with or without attachments, page to a pager, SMS, visual alert to notify the administrator’s designated personnel and generate an audit record] upon detection of a potential security violation.
Hierarchical to:	No other components.
Dependencies:	**FAU_SAA.1 Potential violation analysis**
Application note:	This requirement applies only for the IdP. Additionally, the security alarms have to be integrated in the monitoring processes of the computing environment of the TOE.

5.2.2 Audit Data Generation (FAU_GEN)

FAU_GEN.1 Audit Generation

FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified[1] level of audit; and

c) *Auditable events listed in the table below:*[2]

Event	Additional Details	Entity
Any event	- Time the event (e.g. request) received	IdP Activity Log
Authenticated successful	- Remote logname/identity - IP address - Claimant ID, if the request was authenticated - First line of request. - Final status. - Size of response in bytes. - Referrer header field	IdP Activity Log
Authenticated unsuccessful	- Remote logname/identity - IP address - First line of request. - Final status. - Size of response in bytes. - Referrer header field	IdP Activity Log
Logged in successful	- Name of the Trusted User, Temporary privileged user - Name and role of the operator	IdP Activity Log
Logged out successful	- Name of the Trusted User, Temporary privileged user - Name and role of the operator	IdP Activity Log
Logon failure	- Name of the Trusted User, Temporary privileged user - Name and role of the operator	IdP Activity Log
Creation of a new claimant	- n/a	IdP Activity Log
Deletion of a claimant	- n/a	IdP Activity Log
Locking of a claimant	- n/a	IdP Activity Log
Successful and rejected	- Name of the subject and	IdP Activity

[1] [selection, choose one of: minimum,basic, detailed, not specified]

[2] [assignment: other specifically defined auditable events]

data and other resource access attempts if applicable	the resources	Log
Changes to system configuration	- Name of the Trusted User - Name and role of the operator	IdP Activity Log
Privileged actions (e.g. password change)	- Name of the Trusted User, Temporary privileged user - Name and role of the operator	IdP Activity Log
Use of system utilities and applications	- Name of the subject and the resources	IdP Activity Log
Alarms raised by the access control system	- Entity	IdP Activity Log
Activation and de-activation of protection systems	- Name of the Trusted User - Name and role of the operator	IdP Activity Log
Incidents	- Source - Number of changes - Analysis – list of suspicious actions - Event Tree: process, file, registry and network events - Timeline: timeline of suspicious actions - Geography: suspected locations of suspicious events - Configuration: host system identification details, running applications, service handles, processes, threads	IdP Incidents Alerts

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP, additional details specified below:[3]

- files accessed (if applicable)
- programs/utilities used
- use of privileged accounts, e.g. supervisor, root, administrator;

[3] [assignment: other audit relevant information]

- system start-up and stop;
- I/O device/connector attachment/detachment;
- failed or rejected user actions;
- failed or rejected actions involving data and other resources;
- access policy violations and notification
- console alerts or messages;
- system log exceptions;
- network management alarms;
- alarms raised by the access control system;
- changes to, or attempts to change, system security settings and controls

Hierarchical to: No other components.

Dependencies: **FPT_STM.1 Reliable time stamps**

Application note: These requirements apply only to the IdP and shall be integrated into the logging and monitoring concept of the computing environment of the TOE.

5.2.3 Security audit analysis (FAU_SAA)

FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of defined auditable events given in the following table[4] known to indicate a potential security violation

b) none[5].

No.	Operation	Potential violation analysis list
1	Authentication	Claimant ID mismatch
2		Authentication attempt with revoked claimant ID
3		Authenticator Token mismatch
4		Authentication error
5		Communication channel not trusted or broken
6		Communication channel with weak encryption
7		Enumerating of access portal
8		DoS-Attack on access portal
9		System alerts
10		Certificate validation and path failures

[4] [assignment: subset of definedauditable events]

[5] [assignment: any other rules]

11		Assertion scheme mismatch
12		Digital signature verification failure

Hierarchical to: No other components.

Dependencies: **FAU_GEN.1 Audit Generation**

Application note: These requirements apply only to the IdP and shall be integrated into the operation security concept of the computing environment of the TOE

5.2.4 Security audit review (FAU_SAR)

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide Trusted Users and/or Temporary privileged users[6] with the capability to read incident reports and the IdP Activity Log[7] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for user to interpret the information.

Hierarchical to: No other components.

Dependencies: **FAU_GEN.1 Audit Generation**

Application note: These requirements apply only on the IdP and shall be integrated into the logging and monitoring concept of the computing environment of the TOE.

5.2.5 Security audit event storage (FAU_STG)

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_ STG.1.2 The TSF shall be able to prevent[8] unauthorized modifications to the stored audit records in the audit trail.

Hierarchical to: No other components.

Dependencies: **FAU_GEN.1 Audit Generation**

Application note: These requirements apply only to the IdP and shall be integrated into the operation security concept of the computing environment of the TOE

[6] [assignment: authorised users]

[7] [assignment: list of audit information]

[8] [selection, choose one of: prevent, detect]

5.2.6 Management of security attributes (FMT_MSA)

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1	The TSF shall enforce the access control SFP[9] to restrict the ability to query, delete[10] the security attributes Reference of the user credential, Claimant ID, Identification Data[11] to Trusted User[12].
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Application note:	

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1	The TSF shall enforce the access control SFP[13] to provide restrictive[14] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the Security Information Officers[15] to specify alternative initial values to override the default values when an object or information is created.
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Application note:	

[9] [assignment: access control SFP(s), information flow control SFP(s)]

[10] [selection: change_default, query, modify, delete, [assignment: other operations]]

[11] [assignment: list of security attributes]

[12] [assignment: the authorised identified roles]

[13][assignment: access control SFP, information flow control SFP]

[14] [selection, choose one of: restrictive, permissive, [assignment: other property]]

[15] [assignment: the authorised identified roles]

5.2.7 Access control functions (FDP_ACF)

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1	The TSF shall enforce the access control SFP[16] to objects based on the following: User, Trusted User, Temporary privileged users, User data, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes[17].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: Authenticated successful, Authenticated unsuccessful, Logged in successful, Logged out successful, Logon failure, Creation of a new claimant, Deletion of a claimant, Locking of a claimant, Successful and rejected data and other resource access attempts if applicable[18].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[19].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[20].
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
Application note:	These requirements apply only to the IdP and shall be integrated into the access management system of the computing environment of the TOE.

5.2.8 Access control policy (FDP_ACC)

FDP_ACC.1 Subset access control

FDP_ACC.1.1	The TSF shall enforce the access control SFP[21] on User, Trusted User, Temporary privileged users, User data and operations among subjects and objects

[16] [assignment: access control SFP]

[17] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

[18] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

[19] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[20] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

[21] [assignment: access control SFP]

covered by the SFP[22].

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

Application note:

5.2.9 Inter-TSF TSF data consistency (FPT_TDC)

FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_TDC.1.1 The TSF shall provide the capability to consistently interpret Assertion Data[23] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use OASIS Security Assertion Markup Language (SAML) V2.0[24] when interpreting the TSF data from another trusted IT product.

Hierarchical to: No other components.

Dependencies: No dependencies.

Application note:

5.2.10 Import from outside of the TOE (FDP_ITC)

FDP_ITC.2 Import of user data with security attributes

FDP_ITC.2.1 The TSF shall enforce the access control SFP(s)[25] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none[26].

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or

[22] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

[23] [assignment: list of TSF data types]

[24] [assignment: list of interpretation rules to be applied by the TSF]

[25] [assignment: access control SFP(s) and/or information flow control SFP(s)]

[26] [assignment: additional importation control rules]

FTP_TRP.1 Trusted path]
FPT_TDC.1 Inter-TSF basic TSF data consistency

Application note:

5.2.11 Cryptographic key management (FCS_CKM)

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [defined by the following standards: ETSI TS 102 176-1 [5], NIST Special Publication 800-133 [6], NIST Special Publication 800-56A, NIST Special Publication 800-56B [7][27] and specified cryptographic key sizes [asymmetric (RSA): 2048 - 4096 Bit, elliptic curve (EC): n ≥ 224, symmetric: ≥ 256 bits, any key sizes of algorithms providing comparable cryptographic strength][28] that meet the following: none[29].

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

Application note:

FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall perform import the user data with security[30] in accordance with a specified cryptographic key access method import through a secure channel[31] that meets the following: GlobalPlatform Card Specification v.2.3 [14], TLSv1.2 [11], other secure means with defined descriptions[32].

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security
attributes, or
FDP_ITC.2 Import of user data with security
attributes, or

[27] [assignment:cryptographic key generation algorithm]

[28] [assignment: cryptographic key sizes]

[29] [assignment: list of standards]

[30] [assignment: type of cryptographic key access]

[31] [assignment: cryptographic key access method]

[32] [assignment: list of standards]

FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

Application note:

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physically overwriting the keys with random numbers[33] that meets the following: none[34].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Application note:	The key destruction method shall be applied on volatile key fragments after a cryptographic operation for authentication purposes. This requirement shall not be applied on libraries for standard communication security applications (e.g. TLS, IPsec).

5.2.12 Cryptographic operation (FCS_COP)

FCS_COP.1(1) Cryptographic operation (Symmetric Key Cryptographic Operation)

FCS_COP.1.1(1)	The TSF shall perform data encryption and decryption operations[35] in accordance with a specified cryptographic algorithm AES[36] with a cryptographic key size 256 bits[37] that meets the following: none[38].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or

[33] [assignment: cryptographic key destruction method]

[34] [assignment: list of standards]

[35] [assignment: list of cryptographic operations]

[36] [assignment: cryptographic algorithm]

[37] [assignment: cryptographic key sizes]

[38] [assignment: list of standards]

FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1(2) Cryptographic operation (Asymmetric Key operations)

FCS_COP.1.1(2)	The TSF shall perform data encryption and decryption[39] in accordance with a specified cryptographic algorithm RSA, Diffie-Hellman, ElGamal, EC and comparable algorithms[40] and cryptographic key size 2048 - 4096 Bit, n ≥ 224[41] that meet the following: PKCS#1 v1.5, PKCS#1 v2.1[42].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Application note:	Additionally to the listed cryptographic algorithms, other algorithms are admitted if they provide comparable cryptographic strength.

FCS_COP.1(3) Cryptographic operation (HASH function)

FCS_COP.1.1	The TSF shall perform a HASH operation[43] in accordance with a specified cryptographic algorithm [SHA-256, SHA-512[44]] with a cryptographic key size none[45] that meets the following: FIPS PUB 180-3[46].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

[39] [assignment: list of cryptographic operations]

[40] [assignment: cryptographic algorithm]

[41] [assignment: cryptographic key sizes]

[42] [assignment: list of standards]

[43] [assignment: list of cryptographic operations]

[44] [assignment: cryptographic algorithm]

[45] [assignment: cryptographic key sizes]

[46] [assignment: list of standards]

FCS_CKM.4 Cryptographic key destruction

Application note:

5.2.13 Authentication failures (FIA_AFL)

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 / IdP	The TSF shall detect when an administrator configurable positive integer within the range of 1 - 20[47] unsuccessful authentication attempts occur related to authentication on the IdP portal or system[48].
FIA_AFL.1.1 / Device/Token	The TSF shall detect when a certain number of[49] unsuccessful authentication attempts occur related to RAD/Activation (5 attempts are allowed) and PUK (authentication (10 attempts are allowed) if provided[50].
FIA_AFL.1.2 / IdP	When the defined number of unsuccessful authentication attempts has been met or surpassed[51], the TSF shall display warning message, stop the function of user authentication for 10 minutes and generate audit data to the event[52].
FIA_AFL.1.2 / Device/Token	When the defined number of unsuccessful authentication attempts has been met or surpassed[53], the TSF shall block the RAD/Activation[54].
Hierarchical to:	No other components.
Dependencies:	**FIA_UID.1 Timing of identification**

Application note:

5.2.14 User authentication (FIA_UAU)

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1	The TSF shall allow all functions allowed to be performed by the non authenticated user according to the defined authentication sequence with corresponding secure authentication process states[55] on behalf of the user to be performed before the user is authenticated.

[47] [selection: [assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]]

[48] [assignment: list of authentication events]

[49] [selection: [assignment: positive integer number], an administrator configurable positive integer with-in[assignment: range of acceptable values]]

[50] [assignment: list of authentication events]

[51] [selection: met, surpassed]

[52] [assignment: list of actions]

[53] [selection: met, surpassed]

[54] [assignment: list of actions]

[55] [assignment: list of TSF mediated actions]

FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Hierarchical to:	No other components.
Dependencies:	**FIA_UID.1 Timing of identification**
Application note:	

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Hierarchical to:	FIA_UAU.1 Timing of authentication.
Dependencies:	**FIA_UID.1 Timing of identification**
Application note:	

FIA_UAU.3 Unforgeable authentication

FIA_UAU.3.1	The TSF shall *detect and prevent* use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2	The TSF shall detect and prevent[56] use of authentication data that has been copied from any other user of the TSF.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1	The TSF shall provide at least a 2-factor authentication mechanism using a combination of the following possible authentication components: a) Username and Passphrase or activation data, b) Software/Hardware token verification data, c) Biometric credentials[57] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the following rules: The TOE first verifies the first one authentication component and then verifies the second one authentication component. If each verification of the two chosen

[56] [selection: detect, prevent]

[57] [assignment: list of multiple authentication mechanisms]

	authentication components has been successfully performed, further TSF-mediated actions are allowed.[58]
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	These SFRs refer to the ability for one of many authentication schemes to be specified, and to the ability for the TSF to authenticate a claimant based on the data passed through any of these schemes. The access web portal of the IdP use an authenticated secure channel to protect authentication/verification data transactions based on TLS 1.2 with at least one server-side certificate authentication.

FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1	The TSF shall provide only obscured feedback[59] to the user while the authentication is in progress.
Hierarchical to:	No other components.
Dependencies:	**FIA_UID.1 Timing of identification**
Application note:	Obscured feedback implies the TSF does not produce a visible display of any authentication data entered by a user, such as through a keyboard or another entering device (e.g., echo the password). It is acceptable that some indication of progress be returned instead.

5.2.15 User identification (FIA_UID)

FIA_UID.1 Timing of identification

FIA_UID.1.1	The TSF shall allow access to the public web portal of the IdP (restricted to the functions and resources accessible to the subscriber/claimant according to the access control policy assigned for that purpose)[60] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	

[58] [assignment: rules describing how the multiple authentication mechanisms provide authentication]

[59] [assignment: list of feedback]

[60] [assignment: list of TSF-mediated actions]

5.2.16 Management of functions in TSF (FMT_MOF)

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1	The TSF shall restrict the ability to modify the behavior of, enable, disable[61] the functions according to table under FMT_SMF.1 {a ..o}[62] to [Administrators, Operators].
FMT_MOF.1.2	The TSF shall restrict the ability to enable, disable[63] the functions according to table under FMT_SMF.1 {p ..q}[64] to Subscriber/Claimant[65].
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Application note:	

5.2.17 Revocation (FMT_REV)

FMT_REV.1 Revocation

FMT_REV.1.1	The TSF shall restrict the ability to revoke security attributes[66] associated with the users[67] under the control of the TSF to the authorized claimants[68].
FMT_REV.1.2	The TSF shall enforce rules a) The TSF shall revoke immediately the authentication associated with security b) The authorized claimant can revoke the authentication processes activated by the subscriber/claimant and the registration authority[69].
Hierarchical to:	No other components.
Dependencies:	**FMT_SMR.1 Security roles**
Application note:	The IdP has to make available a revocation service using the ocsp protocol

[61] [selection: determine the behaviour

of, disable, enable, modify the behaviour of]

[62] [assignment: list of functions]

[63] [selection: determine the behaviour

of, disable, enable, modify the behaviour of]

[64] [assignment: list of functions]

[65] [assignment: the authorised identified roles]

[66] [assignment: list of security attributes]

[67] [selection: users, subjects, objects, [assignment: other additional resources]]

[68] [assignment: the authorised identified roles]

[69] [assignment: specification of revocation rules]

5.2.18 Security management roles (FMT_SMR)

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- Administrators,
- Operators,
- Maintenances,
- Claimant,
- and further authorized roles (e.g. supervisors)[70]

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Hierarchical to: No other components.

Dependencies: **FIA_UID.1 Timing of identification**

Application note:

5.2.19 Specification of Management Functions (FMT_SMF)

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [71]

	Management Function	**Entity**
a)	Management of Security Attributes Objects and credentials	IdP Device/Token
b)	Management of Claimant Security Attributes	IdP
c)	Management of Authentication Data	IdP
d)	Management of Audit Trail	IdP
e)	Management of Audited Events	IdP
f)	Management of TOE Access Banner	IdP
g)	Management of Role Definitions, including Role Hierarchies and constraints	IdP
h)	Management of access control and its policy	IdP
i)	Management of TOE configuration data	IdP
j)	Management of cryptographic network protocols	IdP
k)	Management of cryptographic keys	IdP
l)	Management of digital certificates	IdP
m)	Management of identification and authentication policy	IdP
n)	Management of identity	IdP
o)	Management of session services	IdP
p)	Management of device/token	Device/Token
q)	Management Reference authentication data [RAD]	Device/Token

Hierarchical to: No other components.

Dependencies: No dependencies.

[70] [assignment: the authorised identified roles]

[71] [assignment: list of management functions to be provided by the TSF]

Application note:

5.2.20 Replay detection (FPT_RPL)

FPT_RPL.1 Replay detection

FPT_RPL.1.1	The TSF shall detect replay for the following entities: TSF data and security attributes[72].
FPT_RPL.1.2	The TSF shall perform reject data; and audit event[73] when replay is detected.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	

5.2.21 Time stamps (FPT_STM)

FPT_STM.1 Reliable time stamps

FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	These requirements apply only on the IdP and shall be integrated into the logging and monitoring concept of the computing environment of the TOE.

5.2.22 Limitation on scope of selectable attributes (FTA_LSA)

FTA_LSA.1 Limitation on scope of selectable attributes

FTA_LSA.1.1	The TSF shall restrict the scope of the session security attributes cookies, session-IDs[74], based on user identity, originating location, time of access[75].
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	

5.2.23 Confidentiality of exported TSF data (FTP_ITC)

FTP_ITC.1 Inter-TSF confidentiality transmission

FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

[72] [assignment: list of identified entities]

[73] [assignment: list of specific actions]

[74] [assignment: session security attributes]

[75] [assignment: attributes]

FTP_ITC.1.2	The TSF shall permit the TSF[76] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for secure communication of assertions and user data.[77]
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application note:	This is to protect the transmission between the IdP and the associated RP.The TSF shall only use TLS 1.2 (RFC 5246 [11]) or IPsec with IKEv2 (RFC 4301 [12], RFC 7296 [13]).

[76] [selection: the TSF, another trusted IT product]

[77] [assignment: list of functions for which a trusted channel is required].

5.3 Security Requirements Rationale

	O.Integrity	Q.Confidentiality	O.Availability	O.Accontability	O.Authentication	O.Secure_Com-munication	O.Crypto-graphic_Func-tions	O.Access_Con-trol	OE.HR_Security	OE.Acces_Man-agementSystem	OE.SecureAreas and Equipment	OE.Configration *and* ChangeManage-	OE.Malware and velnerability Managemenet	OE.Logging and Monitorung	OE.Netswork Security	OE.Identification and IdentityMan-agement	OE.Credential Management	OE.Operations Security	OE.User responsibilities
FAU_ARP.1			X	X															
FAU_GEN.1			X	X															
FAU_SAA.1			X	X															
FAU_SAR.1	X		X	X															
FAU_STG.1	X		X																
FCS_CKM.1							X												
FCS_CKM.3		X			X	X	X	X											
FCS_CKM.4		X					X												
FCS_COP.1		X				X	X												
FDP_ACC.1				X			X	X											
FDP_ACF.1				X				X											
FDP_ITC.2	X	X				X		X											
FIA_AFL.1			X		X		X	X											
FIA_UAU.1				X	X		X	X											
FIA_UAU.2					X			X											
FIA_UAU.3	X				X			X											
FIA_UAU.5					X			X											
FIA_UAU.7		X			X			X											
FIA_UID.1				X	X	X		X											
FMT_MSA.1					X		X	X											

	O.Integrity	Q.Confidentiality	O.Availability	O.Accontability	O.Authentication	O.Secure_Com-munication	O.Crypto-graphic_Func-tions	O.Access_Con-trol	OE.HR_Security	OE.Acces_Man-agementSystem	OE.SecureAreas and Equipment	OE.Configration *and* ChangeManage-	OE.Malware and velnerability Managemenet	OE.Logging and Monitorung	OE.Netswork Security	OE.Identification and IdentityMan-agement	OE.Credential Management	OE.Operations Security	OE.User responsibilities
FMT_MSA.3					X		X	X											
FMT_MOF.1								X											
FMT_REV.1	X		X	X	X			X											
FMT_SMF.1				X	X	X	X	X											
FPT_RPL.1			X	X	X	X													
FTA_LSA.1	X				X	X	(X)	X											
FTP_ITC.1	X	X			X	X	X												
FPT_TDC.1	X			X															
FMT_SMR.1				X	X			X											
FPT_STM.1	X			X															

5.4 Security Assurance Requirements Rationale

The Evaluation Assurance Level for this Protection Profile is **EAL2**.
The reason for choosing assurance level EAL 2 is that this Protection Profile shall provide reasonable assurance for auditing the Electronic Means of Identification in the context of the Federal Act on Electronic Health Records and its regulations.

6 Appendix

6.1 Mapping from English to German/French terms

Term	German	French
Reference community	Stammgemeinschaft	Communauté de référence
Community	Gemeinschaft	Communauté
Healthcare professional	Gesundheitsfachperson	Professionnel de la santé
Electronic identification means	Identifikationsmittel	Moyen d'identification
Regulation on the Electronic Patient Record	Verordnung über das elektronische Patientendossier	Ordonnance sur le dossier électronique du patient
Claimant	Anspruchsberechtigter	Ayant droit
Token	Identifizierungsmerkmal	Caractéristiques d'identification
Credential	Berechtigungsnachweis	Référence d'authentification
Federal Act on Electronic Health Records	Bundesgesetz über das elektronische Patientendossier	Loi fédérale sur le dossier électronique du patient

6.2 Tables

6.3 References

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; Version 3.1, Revision 3, Final, July 2009

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; Version 3.1, Revision 3, Final, July 2009, CCMB-2009-07-002

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; Version 3.1, Revision 3, Final, July 2009, CCMB-2009-07-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 3, Final, July 2009, CCMB-2009-07-004

[5] ETSI TS 102 176-1 V2.0.0 (2007-11): Electronic Signatures and Infrastructures (ESI);

Algorithms and Parameters for Secure Electronic Signatures;

Part 1: Hash functions and asymmetric algorithms

[6] NIST Special Publication 800-133: Recommendation for Cryptographic Key Generation

[7] NIST Special Publication 800-56B: Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography

[8] ISO/IEC 27001:2013: Information technology -- Security techniques -- Information security management systems – Requirements

[9] ISO/IEC 29115:2013: Information technology -- Security techniques -- Entity authentication assurance framework

[10] ISO/IEC 24760-2:2015: Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements

[11] RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2

[12] RFC 4301: Security Architecture for the Internet Protocol

[13] RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)

[14] GlobalPlatform Card Specification Version 2.3, Public Release October 2015, Document Reference: GPC_SPE_034

6.4 SAML Specification

Note: The specification will be drafted during or subsequently to appraisal.