Totalrevision ZertES: Übersicht über die eingereichten Stellungnahmen

Allgemeine Bemerkungen	**Wer**?
Grundsätzlich begrüssen wir die Stossrichtung der Gesetzesrevision, insbesondere die Schaffung einer neuen Form der elektronischen Signaturfür juristische Personen und Behörden. Dass die bisherige qualifizierte elektronische Signatur nur natürlichen Personen zugänglich ist, hat sich für den elektronischen Verkehr in Wirtschaft und Verwaltung, insbesondere für Massengeschäfte, als hinderlich erwiesen. Ebenfallsbegrüsst wird, dass das neue sogenannte «geregelte Zertifikat» nicht nur für die elektronische Signatur, sondern auch etwa für die sichere Authentifizierung von Kommunikationspartnern eingesetzt werden kann. Diese Neuerung entspricht den heutigen Gepflogenheiten im elektronischen Geschäftsverkehr, wo neben dem Austausch von Willenserklärungen via E-Mail vor allem auch die Geschäftsabwicklung via Webdiensten und -Portalen eine zentrale Rolle spielt. Im Übrigen begrüssen wir grundsätzlich auch die vorgeschlagenen terminologischen Vereinfachungen und Bereinigungen, erlauben uns aber den Hinweis, dass das Gesetz nach wie vor äusserst «techniklastig» formuliert und deshalb selbst für Fachleute teilweise nur schwer verständlich ist. Im Übrigen hängt der konkrete Nutzen digitaler Signaturen und Zertifikate massgeblich davon ab, in wie vielen und welchen Bereichen sie künftig eingesetzt werden können. Diese Fragen sind nicht Gegenstand der vorliegenden Revision des ZertES, das nur die Qualität gewisser Zertifizierungsprodukte und die Pflichten der Anbieter solcher Produkte regelt. Bedeutung und Rechtswirkungen digitaler Signaturen und Zertifikate sind in den entsprechenden Sachgesetzen zu regeln. In diesem Zusammenhang wird derzeit vom EJPD der gesetzgeberische Handlungsbedarf im Bereich der elektronischen Signatur abgeklärt. Ein entsprechender Vorschlag für das weitere Vorgehen wird offenbar bis Ende 2012 zuhanden des Bundesrates erwartet. Vor diesem Hintergrund fragt es sich, warum die Revision ZertES bereits jetzt isoliert und nicht später zusammen mit der geplanten Revision der Sachgesetzgebung erfolgen soll.	ZH
Der Kanton Bern begrüsst die Schaffung einer weiteren elektronischen Signatur, die auch von juristischen Personen und Behörden erstellt werden kann. Die an weniger strenge Voraussetzungen geknüpfte Möglichkeit der digitalen Unterzeichnung von Dokumenten entspricht einem Bedürfnis und stärkt den elektronischen Geschäftsverkehr. Sie vereinfacht nicht zuletzt auch den Informationsaustausch im Verkehr mit Behörden (z.B. Gerichten oder Registerbehörden) und hat daher das Potential zu vielen zweckmässigen Einsatz- und Anwendungsmöglichkeiten. Allerdings stellt sich die Frage, ob die für die neue Signaturkategorie gewählte Bezeichnung «geregelt» wirklich passend ist. Möglicherweise liesse sich der eher nichtssagende Begriff durch eine treffendere Umschreibung ersetzen. Der Gegenstand der unterbreiteten Revisionsvorlage ist technisch und anspruchsvoll. Das wirkt sich zwangsläufig auf die Gesetzessprache aus. Dennoch stellt sich im vorliegenden Fall die Frage, ob es nicht möglich gewesen wäre, den Erlass sprachlich einfacher zu redigieren. Das neue Gesetz ist für eine fachfremde Person kaum mehr verständlich. Das dürfte auch mit dem hohen Grad an Differenzierungen zusammenhängen, den es mit sich bringt. Wir gehen davon aus, dass die Revisionsvorlage direkte Auswirkungen auf den in weiten Teilen bundesrechtlich vorgeschriebenen elektronischen Geschäftsverkehr der kantonalen Behörden mit ihren Kundinnen und Kunden haben wird. So ist zu vermuten, dass die Neuerungen, Anpassungen und Modifikationen bei den Einrichtungen und Applikationen für den elektronischen Geschäftsverkehr auslösen werden. Neben den Anpassungen der bestehenden Applikationen und Systeme ist dem massiv zunehmenden Mobilitätsbedürfnis der Benutzer in der Revision und in der späteren Ausführung Rechnung zu tragen. Dementsprechend wichtig wäre es zu er-	BE

fahren, wie der Bund die Folgen der Gesetzesrevision für die kantonalen Behörden einschätzt. Eine fundierte Beurteilung der Auswirkungen ist insbesondere auch deshalb nötig, weil der bereits erwähnte hohe Grad an Technizität die Folgeschätzungen zusätzlich erschwert.	
Wir begrüssen die Überarbeitung dieses Gesetzes. Der Entwurf zum Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und andererAnwendungen digitaler Zertifikate (ZertES) enthält viele wertvolle Erweiterungen des heutigen Bundesgesetzes und behält die wichtigen und richtigen Punkte des geltenden Rechts bei. Insbesondere die Erweiterung des Anwendungsbereiches auf juristische Personen und Behörden macht Sinn.	LU
Der Regierungsrat des Kantons Schwyz begrüsst grundsätzlich die geplante Revision. Unsere Stellungnahmen und Vorschläge beziehen sich auf verschiedene relevante Aspekte, welche im Zusammenhang mit der Regelung von Zertifizierungsdiensten im Bereich der elektronischen Signatur zu beachten sind. Die Vorlage regelt einen Bereich, der für die Zukunft der Arbeitsweise der Steuerverwaltung sowie der Verwaltung generell von Bedeutung sein wird. Allerdings betrifft die Vorlage Punkte auf einer noch zu „entfernten“ Ebene (Zulassungen usw.). Aus steuerlicher Sicht sieht man derzeit noch keinen Anlass, sich zur Gesetzesvorlage zu äussern. Aus Sicht des möglichen Nutzens im Bereich Grundbuch und Vermessung wird die Ergänzung der elektronischen Signatur um den Bereich der juristischen Personen und Behörden sowie die Bereinigung bei den Begriffen begrüsst. Insbesondere bei Behörden – wie Grundbuchämtern – wird die Ergänzung mit der geregelten elektronischen Signatur eine Vereinfachung hinsichtlich automatisiert erstellter Grundbuchauszüge bringen. Zudem kann dies auch ein Thema bei automatisiert erstellten Katasterauszügen im Bereich der amtlichen Vermessung sein.	SZ
Die Einführung einer „geregelten elektronischen Signatur, welche auch von juristischen Personen und Behörden genutzt werden kann ist zu begrüssen. Es wird sich zeigen, ob mit dieser neuen Grundlage die elektronische Signatur „massengeschäftstauglich“ wird und sich im Geschaftsverkehr stärker durchsetzen kann. Im Übrigen gehen wird davon aus, dass die Revision keine Kostenfolgen für die Kantone haben wird.	OW
Gleich wie beim heute geltenden ZertES bleibt es ein wichtiges Ziel des Gesetzesentwurfes, ein breites Angebot an sicheren Zertifizierungsdiensten zu fördern. Ausgehend von diesem Ziel ist aus Sicht des Datenschutzes nicht nur die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift von Bedeutung, sondern auch (oder gerade) die hierbei zu Grunde liegende Technologie und deren Förderung. Kryptographische Verfahren gewährleisten Vertraulichkeit, Integrität und Authentizität beim elektronischen Geschäftsverkehr. Sie dienen damit zentralen Anliegen des Datenschutzes. Die rasante technologische Entwicklung führt nicht nur im Bereich der Kryptographie zu immer neueren und sicheren Verfahren, sondern eröffnet auch potenziellen Angreifern immer neue Möglichkeiten, vorhandene Verschlüsselungen oder Sicherheitsmechanismen aufzubrechen oder zu umgehen. Im Bereich der Kryptographie muss die Forschung deshalb laufend mögliche Angriffe antizipieren und wirksame Gegenmassnahmen entwickeln. Wir regen an, die Forschung und Entwicklung im Bericht der Kryptographie gezielt zu fördern und eine entsprechende Bestimmung in den Gesetzesentwurf aufzunehmen.	NW
Wir begrüssen die Stossrichtung der Revision grundsätzlich. Die angestrebten gesetzlichen Veränderungen verbessern die Handhabung von Zertifikaten und fördern deren Einsatz.	GL

Wir sind mit den Zielen der Revision einverstanden und begrüssen die Ergänzung des Gesetzes um Lösungen, welche auch von juristischen Personen und Behörden im geschäftlichen Einsatz genutzt werden können. Aus Sicht der Informatik sehen wir keine Hindernisse für deren Umsetzung. Wichtig ist auch die Delegation der Kompetenzen.	ZG
Nous soutenons ce projet. En outre, la nouvelle loi s'étend de la signature électronique à toute forme de certificat numérique. Cela inclut donc les certificats SSL et autres certificats, qui ont des usages, mais également des implications différentes. L'utilisation de certificats pour le chiffrement, par exemple, n'est pas abordée dans la loi. Les usages de certificats "machine" pour des sites web sécurisés en SSL distribués sur du Cloud sont en contradiction avec la loi qui impose la "garantie que la clef est unique", alors qu'en pratique les clefs privées sont dupliquées ds que ion fait de la haute disponibilité.	FR
Wir begrüssen die mit der vorliegenden Revision verfolgten Ziele. Die Einführung der sogenannten geregelten elektronischen Signatur, die (anders als die qualifizierte elektronische Signatur) auch von juristischen Personen und Behörden genutzt werden kann, erachten wir als eine sinnvolle und praktikable Neuerung. Konsequent und ebenso begrüssenswert ist, dass nebst der elektronischen Signatur auch die sichere Authentifikation mit Zertifizierungsdienste-Produkten gesetzlich geregelt werden soll. Das neue geregelte Unternehmens- oder Behördenzertifikat sehen wir im Zusammenhang von Massengeschäften als weiteres klares und wirksames Instrument für den sicheren Rechts- und Geschäftsverkehr. Damit lässt sich auf kostengünstige Weise eine wesentliche Verbesserung der Nachvollziehbarkeit und Sicherheit namentlich des Mailverkehrs zwischen Behörden und Privaten bzw. anderen Behörden erreichen. Schliesslich betrachten wir es als sinnvoll, im Rahmen der Revision terminologische Bereinigungen und Vereinfachungen bei der Regelung der elektronischen Signatur in den verschiedenen Gesetzen und Verordnungen herbeizuführen.	SO
In grundsätzlicher Hinsicht können wir Ihnen mitteilen, dass wir die vorgelegte Revision begrüssen. Insbesondere unterstützen wir die Bestrebungen, die elektronische Signatur für Unternehmen und Behörden zugänglich zu machen. Auch die weiteren Revisionspunkte wie die gesetzliche Regelung der sicheren Authentifikation mit Zertifizierungsdienste-Produkten, die Einführung eines Zeitstempels in der von Ihnen vorgeschlagenen Form bei qualifizierten Zertifikaten sowie die terminologischen Bereinigungen in den verschiedenen Gesetzen sind aus unserer Sicht nicht zu beanstanden. Nach wie vor unbefriedigend ist sodann die Situation der elektronischen Signatur im Zusammenhang mit den natürlichen Personen für die Steuerbehörden. Die damit zusammenhängenden Kosten für das Ausstellen von Zertifikaten und die Tatsache, dass diese zuerst bei einem Anbieter beschafft werden müssen, haben zur Folge, dass die elektronische Signatur bei den Bürgern und Bürgerinnen kaum genutzt wird und wenig verbreitet ist. Dies hat unseres Erachtens Auswirkungen auf den weiteren Ausbau und die Weiterentwicklung vonE-Government Dienstleistungen. An dieser Situation hat die Einführung der SuisselD nichts geändert und es ist zu erwarten, dass auch die vorliegende Gesetzesrevision in dieser Beziehung keine Änderung bringen wird. Vielmehr werden Bestrebungen in den Kantonen zu nehmen, für bestimmte Behördengeschäfte wie das Ausfüllen der Steuererklärung im Internet oder der Zugriff auf das Steuerkonto, welche einen besonders hohen Grad an Authentizität, Persönlichkeitsschutz, 1 Informationsschutz und Integrität erfordern, durch gesetzliche Regelung andere Verfahren als die qualifizierte elektronische Signatur einzusetzen, welche den Bürger oder die Bürgerin authentifiziert.	BS

Wir danken Ihnen für die Einladung zur Stellungnahme und teilen mit, dass der Regierungsrat des Kantons Basel-Landschaft das Revisionsvorhaben befürwortet. Die Absicht des Bundesrats, die Anwendung der elektronischen Signatur für juristische Personen und Behörden zu vereinfachen, wird von uns unterstützt.	BL
Wir begrüssen den Vorschlag, den Anwendungsbereich für die elektronische Signatur praxistauglicher zu gestalten und durch Einführung der «geregelten elektronischen Signatur» den Benutzerkreis auch auf juristische Personen und Behörden auszudehnen. Die gesetzliche Regelung einer sicheren Authentifikation ist ebenfalls von zentraler Bedeutung. Es sind für uns keine Gründe ersichtlich, der elektronischen Signatur nicht einen Zeitstempel, zumindest als fakultative Option, beizufügen.	SH
Die Totalrevision des Bundesgesetzes über die elektronische Signatur wird vom Regierungsrat grundsätzlich begrüsst, insbesondere die Stossrichtung, die elektronische Signatur praxistauglicher zu machen. Obwohl die Möglichkeit für elektronische Eingaben im Zivil- und Strafverfahren seit 1. Januar 2011 gegeben ist, hat der elektronische Rechtsverkehr in Appenzell Ausserrhoden – im Einklang mit dem gesamtschweizerischen Trend – noch nicht Fuss gefasst. Es wird sich zeigen, ob die vorgeschlagenen Verbesserungen der Rahmenbedingungen die Verfahrensparteien dazu bringen werden, von dieser Möglichkeit Gebrauch zu machen. Die Qualität der Gesetzgebung des elektronischen Rechtsverkehrs ist bereits jetzt auf einem ausreichend hohen Niveau, die Gefässe stehen zur Anwendung bereit. Definitiv wird die Qualität der Gesetzgebung allerdings erst beurteilt werden können, wenn damit gearbeitet wird. Es ist davon auszugehen, dass dies in nicht allzu langer Zeit der Fall sein wird, da die Erfahrung in anderen Ländern wie beispielsweise Österreich zeigt, dass der elektronische Rechtsverkehr durchaus eine effiziente Alternative zum Postversand sein kann. Bis dies auch in der Schweiz wahrgenommen wird macht es wohl keinen Sinn, weitere Revisionen an den Rechtsgrundlagen vorzunehmen. Es ist eher unwahrscheinlich, dass die Verfahrensparteien mit blossen Feineinstellungen der technischen Rahmenbedingungen dazu gebracht werden können, auf den elektronischen Rechtsverkehr umzusteigen. Dies ist vielmehr eine Frage der Gewohnheit, welche zu ändern erfahrungsgemäss eine gewisse Zeit in Anspruch nimmt.	AR
Sind mit der Vorlage einverstanden. Wir gehen aber davon aus, dass die Thematik UID in die Gesetzesrevision einfliessen wird, geht es doch bei der UID um den sicheren Austausch von Informationen in administrativen und statistischen Prozessen.	AI
Mit der beabsichtigten Revision des Bundesgesetzes vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) wird als Ergänzung zur bisherigen qualifizierten Signatur, die nur natürlichen Personen zugänglich ist, eine weitere geregelte elektronische Signatur definiert, die auch von juristischen Personen und Behörden erstellt werden kann. Zudem werden die gesetzlichen Grundlagen geschaffen, durch welche nebst der elektronischen Signatur auch die sichere Authentifikation mit Zertifizierungsdienste Produkten geregelt wird. Schliesslich soll eine terminologische Bereinigung und Vereinfachung bei der Regelung der elektronischen Signatur in den verschiedenen Bundeserlassen herbeigeführt werden. Zusätzlich wird geprüft, ob neu allenfalls ein Zeitstempel obligatorischer Bestandteil der qualifizierten elektronischen Signatur sein soll. Der Regierungsrat des Kantons Aargau begrüsst die Zielsetzung der vorliegenden Gesetzesrevision, die Anforderungen für die Anerkennung elektronischer Signaturen im Hinblick auf deren Verbreitung und im Vergleich zur eigenhändigen Unterschrift alltagstauglicher zu machen.	AG

Wir danken Ihnen für die Möglichkeit, uns zum Entwurf für die Totalrevision des Bundesgesetzes vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES; SR 943.03) äussern zu können und teilen Ihnen mit, dass wir mit der Vorlage grundsätzlich einverstanden sind. Bezüglich der technischen und organisatorischen Umsetzung ergeben sich jedoch Fragen, die in der entsprechenden Ausführungsverordnung noch geklärt werden müssen. So wäre in jener Verordnung beispielsweise zu präzisieren, wie der kontrollierte Beschaffungsprozess erfolgt, welche Möglichkeiten zur Personalisierung von Firmenschlüsseln existieren, wie sich die Integrität bei der Prüfung eines Dokuments darstellt, welche Massnahmen betreffend Missbrauch vorhanden sind und wie vorzugehen ist, wenn die Zeichnungsberechtigung in einer Firma mit „Kollektivunterschrift zu zweien“ geregelt ist.	TG
Lo scrivente Consiglio condivide appieno l'impostazione dell'avamprogetto di legge posto in consultazione, rilevando in particolare che le novità che si intendono introdurre con la revisione della Legge fédérale del 19 dicembre 2003 sui servizi di certificazione nel campo della firma elettronica è di sicuro interesse per l'economia, i servizi amministrativi e per le autorità giudiziarie. Come visto, l'attuale firma elettronica qualificata è accessibile unicamente aile persone fisiche, ragione per cui un'autorità puô farvi capo solamente facendo intestare il relative certificate qualificato ad une spécifiée funzionarie. Queste pone dei limiti impertanti alla diffusiene della firma elettronica. La nueva legge permetterà per contre ad ogni singola autprità di essere titelare di una firma elettronica regolamentata e del relative certificate e di agire quindi in mode tetalmente autonome. Il Consiglio di State, corne dette, condivide l'impostazione deil'avamprogetto, segnala tuttavia che dal punto di vista della tecnica legislativa, l'abbreviazione proposta (FiEle), oltre ad essere una parola di sensé compiuto in italiano che non ha nulla a che vedere con la firma elettronica, non è conforme cen gli standard. Le abbreviazieni LFEI (Legge fédérale sulla firma elettronica) e LSCFE (Legge fédérale sui servizi ci certificazione nel campo della firma elettronica e di altre applicazieni di certificati digitali) sembrano più appropriate. Ci permettiame infine di rilevare che nel titele della Sezione 4 si è insinuato un piccelo errore nel termine "certificati".	TI
Le Conseil d'Etat vaudois a pris connaissance de la révision de la loi sur la signature électronique. Il vous remercie de l'avoir consulté. De manière générale, il apparaît que cette révision de la loi fédérale répond à une volonté unanime exprimée par les différentes instances concernées. Cette révision présente en effet l'avantage de combler les lacunes qui survinrent dès l'adoption de la présente loi, sans remise en cause fondamentale des règles préétablies. La volonté de simplifier les termes de la présente loi, ainsi que du cadre légal corollaire, constitue une avancée notable dans la mesure où l'application de ce texte suscitait de nombreuses interrogations et incertitudes. Enfin, le gouvernement vaudois se réjouit de l'intégration de la notion d'authentification sûre via des produits de certification, qui intervient en clarification des interrogations en la matière ; en effet, il ressort de l'usage que l'emploi de termes ou solutions trop précises se révèle parfois un obstacle restrictif dans l'étendue des outils à portée. Néanmoins, si le gouvernement vaudois est conscient de la difficulté de légiférer en matière technologique du fait de la nature dynamique de ce domaine, il se doit de constater que les modifications entreprises restent pour le moins insuffisantes au regard des attentes en la matière. Tout en saluant les efforts déployés pour palier les lacunes préexistantes, force est de constater que le texte révisé apparaît comme insuffisant au regard des attentes concernant le sujet. En effet, l'effort de simplification pourrait être approfondi et d'ores et déjà également étendu aux différents textes afférents, notamment les ordonnances sur la communication électronique dans le cadre des procédures pénales et civiles ainsi qu'en matière de poursuites pour dettes et faillite. Il est par ailleurs regrettable que le texte révisé ne contienne pas encore de principes concernant la valeur des	VD

documents signés électroniquement. Si les intentions et travaux en cours sont positifs, il n'en reste pas moins que la dynamique demeure insuffisamment active, voire proactive. Pour conclure, l'ensemble du cadre légal en matière de communication électronique devrait tendre vers plus de cohérence, de simplicité et de flexibilité au regard des pratiques, afin d'apporter plus de confort que d'incertitudes, obstacles à une adhésion unanime à l'électronique comme moyen de communication. En vous remerciant de nous avoir associés à cette consultation, nous vous prions de croire, Madame la Conseillère fédérale, à l'expression de notre haute considération.	
Le Conseil d'Etat du canton du Valais salue l'introduction dans la loi la nouvelle forme de signature électronique qui complète la signature électronique qualifiée et qui peut être utilisée non plus uniquement par les personnes physiques mais également par les personnes morales et les autorités. Selon le Conseil d'Etat du canton du Valais la création d'une base légale régissant non seulement la signature électronique mais aussi l'authentification sûre par le biais des produits de certification est en effet nécessaire.	VS
Nous sommes convaincus de la nécessité de revoir cette loi ici afin de l'adapter aux besoins courants du commerce électronique au sens large du terme, en particulier pour traiter de la représentation des personnes morales. La révision de la loi ci va dans ce sens et offre, par le niveau de signature électronique réglementée, une couverture positive face au développement du gouvernement électronique. Nous restons cependant persuadés que pour la plupart des transactions électroniques entre les usagers et les collectivités publiques, la mise en œuvre d'un portail d'authentification forte des personnes ou des entreprises permet de répondre aux besoins essentiels en la matière à l'image de ce que notre canton a mis en œuvre sur le Guichet sécurisé unique. Nous pensons également qu'il est juste d'assouplir ie ccncept de signature électronique au niveau de la règlementation centrale au profit des lois par secteur qui, en fonction de leurs propres besoins, pourront s'appuyer sur i'une ou l'autre des diffórentes signatures éléctroniques existantes (signature qualifie avec horodatage ou non, signature règlemente). En conclusion, le Conseil d'Etat soutient sans restriction la révision proposée de la loi sur la signature éléctrcnique.	NE
Il n'est pas certain que la refonte complète de la loi du 19 décembre 2003 sur la signature électronique permette d'atteindre tous les buts visés, notamment d'améliorer la compréhension de la législation en la matière. Si notre Conseil soutient le développement de l'administration numérique et l'utilisation de la signature électronique, l'avant-projet de loi fédérale soumis à consultation est encore insuffisant par rapport aux objectifs que vous annoncez. Il mériterait donc d'être encore amélioré pour en faciliter la lecture et, par conséquent, la mise en oeuvre concrète de l'administration électronique. Notre position vis-à-vis du texte soumis à consultation n'est donc pas favorable en l'état, bien que sur le principe, notre Conseil appuie votre démarche.	GE
L'introduction dans la loi d'une forme de signature électronique adaptée aux entreprises et aux autorités est à saluer car elle répond à un réel besoin. Les règles applicables à la signature électronique réglementée, en particulier à l'article 7 de l'avant-projet offrent à la fois une certaine souplesse et des garanties de sécurité a priori adéquates (sous réserve de la remarque figurant au point 4 ci-dessous). L'avant-projet comprend une seconde innovation en tendant son champ d'application aux moyens d'authentification dans leur ensemble. Nous pouvons nous rallier à cette évolution. Il convient toutefois de rappeler que es certificats numériques ont trois usages différents:	JU

la signature électronique, l'authentification et le chiffrement. Or le chiffrement n'est pas abordé expressément dans la loi. Nous vous laissons déterminer s'ii convient de le faire. L'ordonnance qui découlera de la loi devra quant à elle procéder à ces distinctions car des règles spécifiques sont nécessaires à chacun des trois domaines.	
Mit dem Schreiben vom 29. März 2012 wurden wir eingeladen, über die oben genannte Vorlage, Stellung zu nehmen. Für diese Gelegenheit zur Meinungsäusserung danken wir bestens und lassen Ihnen hiermit gerne unsere Antwort zukommen. Die CVP unterstützt nach wie vor der Strategie des Bundesrates zur Informationsgesellschaft Schweiz. In diesem Sinne begrüsst die CVP auch den Grundsatz, die qualifizierte elektronische Signatur auszuweiten und eine geregelte elektronische Signatur juristischen Personen zugänglich zu machen. Damit wird einem Bedürfnis der Wirtschaft, aber auch der Behörden entsprochen. Die CVP äussert hingegen einige Bedenken bezüglich der Umsetzung, der Kontrolle und dem Missbrauch. Die Ausweitung der elektronischen Signatur und der allfällige Missbrauch können weitreichende Konsequenzen haben. Die CVP behält sich deshalb vor, diverse Fragen in den Kommissionsberatungen vertieft abklären zu lassen. Ebenso verhält es sich mit der Variante bezüglich der Einführung eines obligatorischen Zeitstempels bei der qualifizierten elektronischen Signatur.	CVP
Le PEV soutient cette révision de loi, telle qu'explicitée dans le rapport explicatif. Le fait que cet outil est, avec la normailsation de l'utilisation d'internet, de plus en plus utilisé, également par les personnes morales et les autorités, justifie les changements apportés. Ceux-ci paraissent adéquats au vu des mesures en vigueur selon les lois européennes, mais surtout en regard des besoins dans les secteurs administratifs et économiques.	EVP (PEV)
Infolge der Annahme der Motion Baumann (08.3741) wurde dem Bundesamt für Justiz der Auftrag erteilt, vertiefte Abklärungen über die Revisionsbedürftigkeit des Bundesgesetzes über die elektronische Signatur (ZertES) zu treffen. Dabei wurde ein Bedarf nach einer Regelung der elektronischen Signatur für juristische Personen resp. Behörden sowie der Authentifikation festgestellt. FDP.Die Liberalen unterstützt das Ziel der Vorlage, Rechtssicherheit im Umgang mit elektronisch signierten Dokumenten zu beseitigen und die elektronische Signatur für juristische Personen resp. Behörden zu regeln. Damit wird dem Bedürfnis der Wirtschaft nach einer zeitgemässen Regelung Rechnung getragen. Die Ergänzung der bisherigen qualifizierten elektronischen Signatur mit der geregelten elektronischen Signatur, die auch von juristischen Personen benutzt werden kann, erachten wir als sinnvoll. Auch die terminologische Bereinigung sowie die Schaffung einer gesetzlichen Grundlage für die Authentifikation mit Produkten von Zertifizierungsdiensten unterstützen wir. Abschliessend möchten wir festhalten, dass wir die Vorlage unterstützen. Voraussetzung hierfür ist jedoch, dass der oben erwähnte Einwand (OR 59a Abs. 1) berücksichtigt wird. Zudem behalten wir uns vor, in den Kommissionsberatungen weitere Änderungsanträge einzubringen.	FDP
Aus Sicht der SVP ist der vorliegenden Totalrevision des Bundesgesetzes vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES; SR 943.03) grundsätzlich zuzustimmen. Insbesondere die Einführung der „geregelten elektronischen Signatur“ und des „geregelten Zertifikates“ sind zu befürworten, um einer Massentauglichkeit den Weg zu ebnen. Ebenso ist zu befürworten, dass eine Kompatibilität zur europäischen Signaturrichtlinie beachtet wird. Nicht berücksichtigt werden konnten in der vorliegenden Revision die aktuell geplanten europäischen Entwicklungen in diesem Bereich. In diesem Sinne sollte die Vorlage auf ihre Kompatibilität erneut überprüft und allenfalls überarbeitet werden.	SVP

Das Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES; SR 943.03) trat am 1. Januar 2005 in Kraft. Dieses Gesetz regelt die Voraussetzungen, unter den sich Anbieter von Zertifizierungsdiensten im Bereich der elektronischen Signatur anerkennen lassen können und die Rechte und Pflichten der anerkannten Anbieter von Zertifizierungsdiensten. Mit der vorliegenden Revision soll dieser Erlass „massengeschäfts-tauglich“ gemacht werden. Hierzu soll die sogenannt „geregelte elektronische Signatur‘ (und das dazu ver wendete „geregelte Zertifikat“) als dritte Spezialisie-rungs-Stufe eingeführt werden (und erst als vierte Stufe die qualifizierte elektronische Signatur fungieren), welche auch von juristischen Personen und Behörden genutzt werden kann. Der Gesetzgeber, der ein bestimmtes Verfahren zu re-geln hat, hätte für seine Formvorschriften alsdann die Wahl zwischen der bisherigen qualifizierten elektronischen Signatur für spezielle Anforderungen und der neuen geregelten elektronischen Signatur für normale Anforderungen. Weiter soll mit der Revision die gesetz-liche Grundlage geschaffen werden, damit nebst der elektronischen Signatur auch die sichere Authentifikation mit Zertifizierungs-dienste-Produkten geregelt werden kann. Schliesslich führt die Revisionsvorlage eine terminologische Bereinigung bei der Regelung der elektronischen Signatur in den verschiedenen Gesetzen und Verordnungen ein.	
Grundsätzlich begrüsst es der SGV jedoch sehr, dass auf Bundesebene eine einfach anwendbare, praxistaugliche und technisch ein-wandfreie Lösung im Bereich der elektronischen Signaturen gesucht wird. Eine solche Lösung könnte insb. auch auf kommunaler Ebene zu effizienteren Geschäftsprozessen führen und zu einer noch höheren Dienstleistungsqualität für die Einwohnerinnen und Einwohner beitragen. Beim Abklären des Anwendungsbereichs der elektronische Signatur möchte der SGV schliesslich anregen, dass dies eng mit der eGovernment-Strategie Schweiz, respektive dem Katalog der priorisierten eGovernment-Vorhaben koordiniert wird und dabei auch die unterschiedlichen kantonalen und kommunalen Rahmenbedingungen berücksichtigt werden.	SGV
Wir begrüssen die Revision des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur und unterstützen insbesondere die Bestrebungen, die elektronische Signatur für Unternehmen und Behörden zugänglich zu machen, da damit ein aus-gewiesenes Bedürfnis von Wirtschaft und Verwaltung erfüllt wird. Mit dem zusätzlichen Signaturtypus der geregelten elektronischen Signatur und dem geregelten Zertifikat wird eine wichtige Voraussetzung für die Erleichterung von Geschäftsvorgängen zwischen Un-ternehmen sowie für die Förderung eines elektronischen Behördenverkehrsgeschaffen und damit den Bedürfnissen von Zielgruppen der E-Government-Strategie Schweiz entsprochen. Im Rahmen unseres internen Vernehmlassungsverfahrens wurde festgestellt, dass durch die Schaffung einer zusätzlichen Signatur für juristische Personen ein verhältnismässig komplexes Angebot realisiert wurde. Demgegenüber ist es den Städten ein zentrales Anliegen, dass es im Zusammenhang mit der digitalen Signatur eine möglichst einfach zu handhabende Identifi-zierung und Authentifizierung in wenigen Arbeitsschritten geschaffen wird. Bei den weiteren Umsetzungsarbeiten zu den elektroni-schen Signaturen sollte unseres Erachtens ein wichtiges Augenmerk auf Praktikabilität und Wirtschaftlichkeit gerichtet werden. Die geregelte und auch die qualifizierte Signatur müssen unter wirtschaftlichen Gesichtspunkten sinnvoll einsetzbar sein. Auch wurde darauf hingewiesen, dass der Grundfehler, wonach die elektronischen Identitätsausweise (digitale Signaturen) für die Authentifizierung von Personen von mehreren privaten Anbietern und in der Folge mit unterschiedlichen Produkten ausgestellt wer-den, statt wie die herkömmlichen Identitätsausweise durch staatliche Stellen wie Einwohnerkontrollen und Passbüros, durch die Revi-	Städte-verband

sion nicht korrigiert wird. Auch als nach wie vor unbefriedigend beurteilen manche Städte, dass das Ausstellen von Zertifikaten teuer und aufwändig sei (bspw. im Zusammenhang im Verkehr von natürlichen Personen mit den Steuerbehörden) und so der Ausbau und die Weiterentwicklung von E-Government-Dienstleistungen gebremst werde. Nachdem bereits hier die Einführung der SuisselD wenig geändert habe, dürfte auch die vorliegende Gesetzesrevision diesbezüglich keine Auswirkungen haben. Vielmehr würden die Kantone versucht sein, für Behördengeschäfte mit hohen Anforderungen an Authentizität, Persönlichkeitsschutz, lnformationsschutz und Integrität andere Verfahren als die qualifizierte elektronische Unterschrift einzusetzen.	
Die nachfolgenden Äusserungen beschränken sich auf die wichtigsten Kernaussagen aus gesamtwirtschaftlicher Sicht. Für die technischen Einzelfragen verweisen wir auf die beiliegenden Stellungnah man einzelner Mitglieder Die Anpassung des Bundesgesetzes vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur an die heutigen wirtschaftlichen Gegebenheiten wird grundsätzlich begrüsst. Generell ist jedoch zu beachten, dass im täglichen Wirtschaftsverkehr aufgrund der (positiv zu wertenden) Formfreiheit, die grosse Mehrzahl der Verträge per E-Mail ohne Gebrauch einer elektronischen Signatur abgeschlossen wird. Der effektive Anwendungsbereich der elektronischen Signatur wird daher bescheiden bleiben. Falls eine Formvorschrift jedoch besteht, oder von den Parteien gewählt wird, ist der einfache, praxisnahe kostengünstige und sichere Einsatz von elektronischen Signaturen und Zertifikaten erforderlich. Besonders kritisch betrachtet economiesuisse die internationale Abstimmung der Vorlage und die Haftung für Signaturschlüssel in Art. 59a OR. Dem Bundesgesetz über die elektronische Signatur (ZertES) ist schon beim Erlass im Jahr 2003 vorgeworfen worden, die Latte für die Anerkennung elektronischer Signaturen bzw. deren Gleichstellung mit der eigenhändigen Unterschrift zu hoch anzusetzen und daher nicht ‚massengeschäftstauglich“ zu sein. Dies will die Vorlage nun korrigieren. Mit einer Revision des ZertES soll insbesondere die bisherige qualifizierte elektronische Signatur, die nur natürlichen Personen zugänglich ist, mit der geregelten elektronischen Signatur ergänzt werden. Diese soll auch von juristischen Personen und Behörden genutzt werden können. Neben der elektronischen Signatur soll ferner die sichere Authentifikation mit Produkten von Zertifizierungsdiensten gesetzlich geregelt werden. Schliesslich soll, wo immer möglich, die Regelung der elektronischen Signatur in den verschiedenen Gesetzen und Verordnungen terminologisch bereinigt bzw. vereinfacht werden. An den bestehenden Konzepten und Prinzipien der bisherigen Regelung, wie beispielsweise der Freiwilligkeit für die Anbieter und der nicht abschliessenden Regelung von Zertifikatsprodukten, soll nichts geändert werden. Auch soll die schweizerische Gesetzgebung mit der europäischen Richtlinie weiterhin kompatibel bleiben. Gemäss Art. 11 Abs. 1 OR bedürfen Verträge zur ihrer Gültigkeit nur dann einer besonderen Form, wenn das Gesetz eine solche vorschreibt. Das schweizerische Recht geht damit vom Vorrang der Formfreiheit aus. Namentlich ist es grundsätzlich den Parteien überlassen, ob sie einen Vertrag einer bestimmen Form unterstellen wollen. Im täglichen Wirtschaftsverkehr wird daher die grosse Mehrzahl der Verträge per E-Mail und damit ohne Gebrauch einer elektronischen Signatur abgeschlossen. Der effektive Anwendungsbereich der elektronischen Signatur wird daher bescheiden bleiben. Für diejenigen Fälle, bei welchen eine Formvorschrift gesetzlich vorgeschrieben ist oder von den Parteien freiwillig gewählt wird, ist der einfache, praxisnahe kostengünstige und sichere Einsatz von	economiesuisse

elektronischen Signaturen und Zertifikaten zu begrüssen. Dabei muss die elektronische Signatur bzw. Zertifikat insbesondere folgende Anforderungen erfüllen: Identität (Herkunft des Absenders), Authentizität (sichere Zuordnung zum in der Erklärung angegebenen Aussteller), Nichtbestreitbarkeit des Versandes, Integrität (Unversehrtheit des Inhalts der übermittelten Nachricht), Rechtliche Gültigkeit der elektronischen Signatur/Zertifizierung zur Erfüllung der spezifischen formellen Anforderungen in Spezialgesetzen	
Mit der Revision soll die Anwendung der elektronischen Signatur auf für juristische Personen und Behörden vereinfacht und damit die Bedürfnisse der Wirtschaft und der Verwaltung nach einer zeitgemässen Regelung befriedigt werden. Die heutigen gesetzlichen Grundlagen sind nicht massentauglich für den Geschäftsverkehr. Mit dem Vorschlag soll die bisherige qualifizierte elektronische Signatur, die lediglich natürlichen Personen zugänglich ist, mit der geregelten elektronischen Signatur ersetzt werden. Diese soll neu auch von juristischen Personen und Behörden genutzt werden können. Die heute gültige Regelung ist auf die elektronische Unterschrift ausgerichtet, die mit der eigenhändigen Unterschrift gemäss OR 14 Abs. 2 bis vergleichbar ist. Für den elektronischen Geschäftsverkehr reicht diese Regel heute nicht mehr. Neu werden deshalb zwei Zertifikatsklassen geregelt. Wie bisher gilt elektronische Signatur als Äquivalent zur persönlichen Unterschrift als qualifiziertes Zertifikat. Neu wird das geregelte Zertifikat, das für eine breitere Anwendung offen ist, vorgeschlagen. Es kann auch für juristische Personen, einfache Gesellschaften und Personengesellschaften sowie für Behörden ausgestellt werden. Damit wird der Nachweis für Vertretungsbefugnisse vereinfacht. Der Schweizerische Gewerbeverband unterstützt die vorgesehenen Änderungen, da sie einem vereinfachten Geschäftsverkehr dienen. Seitens unserer Mitgliederverbände und Partnerorganisationen sind ebenfalls Stellungnahmen im zustimmenden Sinn eingegangen, zum Teil mit der Forderung, die Anpassungen eng mit der Entwicklung im europäischen Raum zu koordinieren.	sgv
Die Vorlage enthält keine Rechtsschutzbestimmungen. Es gelten daher die üblichen Bestimmungen der Bundesrechtspflege. Dem ist zuzustimmen. Zur materiellen Ausgestaltung der Vorlage äussert sich das Bundesgericht praxisgemäss nicht. Hingegen nimmt es die Gelegenheit gerne wahr, sich zum elektronischen Rechtsverkehr zu äussern, soweit es von der Vorlage selber betroffen ist.	BGer
Mit diesem Schreiben nehmen wir Stellung zur Totalrevision des ZertES. Wir wissen es sehr zu schätzen, dass wir zu einer Stellungnahme eingeladen wurden und begrüssen das Revisionsvorhaben.	keyon AG
Laut Medienmitteilung vom 28.3.20 12 will der Bundesrat mit der Revision des ZertES die Anwendung der elektronischen Signatur auch flXrjuristische Personen und Behörden vereinfachen und damit die Bedürfnisse der Wirtschaft und Verwaltung nach einer zeitgemässen Regelung befriedigen. Der publizierte Revisionseiitwurf kommt diesem Ziel sehr nahe. Hauptziele der Gesetzesrevision: Terminologische Bereinigung bzw. Vereinfachung der Regelung der elektronischen Signatur in den verschiedenen Gesetzen und Verordnungen. Beurteilung: Ziel wurde mit Revision erreicht Keine Änderung von bestehenden Kompetenzen und Prinzipien der bisherigen Regelungen (z.B. Freiwilligkeit für Anbieter und nicht abschliessende Regelung von Zertifikatprodukten. Beurteilung: Ziel mit Revision erreicht. Es muss sichergestellt werden, dass die „geregelten“ digitalen Signaturen auch nach dieser neuen Gesetzesvorlage und einer neu zu erstellenden Ausführungsbestimmung gemäss SR 943.032.1 (TAV), Technische und administrative Vorschrift über Zertifizierungsdienste im Bereich der elektronischen Signatur) bestimmt werden müssen. Dazu kam der Europäische Signatur Standard ETSI TS 102.042 als Vorgabe für die Schweiz definiert werden. Auf der Basis des ETSI 102.042 Standards würde die Schweiz sieh an die Eu-	KPMG AG

ropäische Standardisierung anlehnen. Abschliessende Bemerkung: Im Rahmen des vorliegenden Textentwurfs möchten wir besonders positiv hervorheben, dass die geregelten GF-Signaturen inhaltlich den fortgeschrittenen digitalen Zertifikaten (advanced certificats) entsprechen. Die Schweiz spricht indes leider nach wie vor von <(geregelten Signaturen», während im EU-Raum von «fortgeschrittenen Zertifikaten» bzw. «advance certificats» gesprochen wird.	
QuoVadis hat im Rahmen der ISSS Task Force intensiv mitgearbeitet (und auch versucht entgegenzuwirken, dass allzu viel auf den Kopf gestellt wird – was nicht immer gelungen ist). Dies, weil wir von QuoVadis der Ansicht sind, dass der vorliegende Entwurf mit wenigen Korrekturen sehr praxisnahe geschrieben und so auch umsetzbar ist. Selbstverständlich auch im Bewusstsein, dass dann der „Teufel“ im Detail und in der Verordnung liegen wird. Im Wissen und in Kenntnis, dass nebst ISSS unsere SuisseID-Kollegen Swisscom und SwissSign eine Stellungnahme abgeben werden, verzichten wir von QuoVadis auf eine eigene Stellungnahme. Der Stellungnahme von Swisscom können wir uns inhaltlich 100% anschliessen.	QuoVadis
Der SAV sieht das Bundesgesetz über Zerlifizierungsdienste im Bereich der elektronischen Signatur als Regelwerk für die technischen Voraussetzungen (Instrumente) im elektronischen Behördenverkehr. Der SAV ist wie das EJPD jedoch auch klar der Meinung, dass das ZertES nicht isoliert betrachtet werden darf. Der Regelung der Anwendung dieser im ZertES festgelegten Instrumente, kommt eine ebensolche Bedeutung zu. In diesem Sinne unterstützt der SAV die Bemühungen des EJPD insbe sondere darin, dass auch die Anpassung des entsprechenden geltenden Rechts in Angriff genommen wird. Die Kommentare unter Punkt B sind deshalb auf das im erläuternden Bericht zum Vernehmlassungsentwurf formulierte Ziel Nr. 3 unter Punkt 1.2, welches u.a. eine Vereinfachung bei der Regelung der elektronischen Signatur in den verschiedenen Gesetzen und Verordnungen vorsieht, ausgerichtet. Der SAV glaubt, dass erst wenn die technischen Voraussetzungen für den elektronischen Rechtsverkehr (ERV) und deren Anwendung in Abstimmung zueinander harmonisiert und vereinfacht werden, die Vorteile/Vereinfachung, Beschleunigung und Rationalisierung - ausgeschöpft werden können und dass die Glaubwürdigkeit der Justiz erhöht wird, wenn sie effiziente Verfahrensabläufe garantieren kann. Seit dem seinerzeitigen Startschuss — es ist mittlerweile über 10 Jahre her — zum dazumal noch visionären Pilotversuch JusLink hat sich die Umgebung des elektronischen Rechtsverkehrs wesentlich verändert. Internet bestimmt den Geschäftsalltag. Mit der Einführung der SuisseID und mit den Vorgaben in den neuen Prozessordnungen (StPO, ZPO samt Anpassungen SchKG). und den beiden Übermittlungsverordnungen hat der Bund weitere Grundlagen für die Umsetzung des elektronischen Rechtsverkehrs mit Behörden geschaffen. Generell: Der elektronische Rechtsverkehr findet heute eine ganz andere Basis und ein ganz anderes Verständnis, als dies noch vor 10 Jahren der Fall war. Trotzdem: Der Durchbruch zum elektronischen Rechtsverkehr hat noch nicht stattgefunden, weil die Instrumente und deren Anwendung noch zu uneinheitlich und teilweise zu wenig benutzerfreundlich sind. Über 2500 Anwältinnen und Anwälte haben sich mit der SuisseID ausgerüstet, die sie im Verkehr mit den Behörden noch kaum nutzen können. Hier braucht es nach unserer Einschätzung einerseits gesetzliche Anpassungen, andererseits aber auch massentaugliche Anwendungen, welche vorteilhafterweise elektronisch abgewickelt werden. Umsetzung des elektronischen Behörden- und Rechtsverkehrs: Der SAV wünscht sich, dass im Zuge der Umsetzung des elektroni-	SAV

schen Rechtsverkehrs je nach zu regelnden Abläufen geprüft wird, ob der Einsatz einer qualifizierten elektronischen Signatur überhaupt notwendig ist oder bereits der Einsatz eine geregelten elektronischen Signatur den berechtigten Anliegen an die Identifizierung des Absenders / Berechtigten genügt. Der SAV schlägt deshalb vor, der Einsatz der qualifizierten elektronischen Signatur auf das absolut Notwendige zu beschränken. So ist es beispielsweise nicht notwendig, Beilagen zu einer Eingabe an ein Gericht oder eine Behörde mit einer Signatur zu versehen. Demgegenüber kann es angezeigt sein, eine Eingabe mit einer qualifizierten Signatur zu versehen. Je höher die Anforderungen an die einzusetzende elektronische Signatur sind, desto weniger kann der Inhaber der Signatur Hilfspersonen delegieren, sofern er sich nicht der Haftung nach Art. 59a OR aussetzen will. Im Zuge der Umsetzungsarbeiten wird auch jeweils zu prüfen sein, ob der bisherige „physische Prozess" eins zu eins in elektronischer Form abgebildet werden soll oder ob es sich rechtfertigt, den elektronischen Prozess vollständig neu zu gestalten. Beispielsweise macht es wohl kaum Sinn, eine elektronisch beglaubigte Abbildung der Identitätskarte z.B. als PDF-File einzureichen, wenn die Person mittels qualifiziertem elektronischen Zertifikat eindeutig identifiziert werden kann. Ebenso wenig ist es sinnvoll, einem Rechtsvertreter 1V-Akten bzw. Akten des Ausländer- und Migrationsamtes, welche behördenseits bereits elektronisch archi viert werden als Dateien via Zustellplattform zuzustellen. Vielmehr sollte der Rechtsvertreter Zugriff auf das Dossier erhalten, und die ihm zugänglich gemachten Dokumente direkt von der Behördendatenbank herunterladen können.	
Besten Dankfür die Gelegenheit, zur obengenannten Angelegenheit Stellung nehmen zu können. Wir begrüssen die Zielsetzung der Revision und sind der Meinung, die vorgeschlagenen Änderungen schaffen gute Grundlagen zur Verbesserung der Praxistauglichkeit elektronischer Signaturen. Aus Sicht einer nach ZertES anerkannte Anbieterin von Zertifizierungsdiensten, sollte dem Markt bezüglich Auswahlmöglichkeiten von gesetzlich geregelten digitalen Zertifikaten mehr Flexibilität geboten werden. Unseres Erachtens ist das neu eingeführte geregelte Zertifikat zu stark dem qualifizierten Zertifikat angegliedert. Insbesondere die geforderte persönliche Identifikation der Zertifikatsinhaber schränkt die Verbreitung und damit die Nutzbarkeit der geregelten Zertifikate zu stark ein. Dies speziell auch unter Berücksichtigung der Zielsetzung, dass das geregelte Zertifikat zur sicheren Authentisierung verwendet werden soll. Im Bereich der sicheren Authentisierung steht das geregelte Zertifikat in Konkurrenz zu anderen im Markt etablierten Prozessen/Produkten. Das geregelte Zertifikat soll sich qualitativvon diesen Konkurrenzprodukte abheben, jedoch die Hürde (persönliche Identifikation) nicht zu hoch setzen. So sollte es z.B. möglich sein, dass Unternehmen für ihre eigenen Mitarbeiter ein geregeltes Zertifikat beantragen können, ohne dass sich diese explizit persönlich identifizieren müssen. Ein bestehender Arbeitsvertrag mit überprüfter Verbindung zu Sozialversicherungen (z.B. AHV, SUVA) müssten beispielsweise ausreichend sein.	Swisscom
Die Information Security Society Switzerland (ISSS) http://www.isss.ch ist der führende Fachverband in der Schweiz auf dem Gebiet der ICT-Sicherheit, welchem heute mehr als 1000 Einzel- und Firmenmitglieder aus Wirtschaft, Verwaltung und Wissenschaft angehören. ISSS setzt sich mit den technischen, wirtschaftlichen, regulatorischen und gesellschaftspoli tischen Aspekten von ICT-Sicherheit und lnformationsschutz auseinander. ISSS wurde 1993 als Verein unter dem früheren Namen FGSec gegründet. ISSS ist offizieller Security Fachpartner von SwisslCT. Unsere Stellungnahme beschränkt sich auf diejenigen Punkte des Gesetzesentwurfes, welche im Zusammenhang mit der ICT-Sicherheit und dem lnformationsschutz stehen. Wir hoffen, dass wir mit unserer Stellungnahme einen Beitrag zur Förderung der ICT-Sicherheit und dem Informationsschutz in unserem Lande leisten können und danken Ihnen für die Berücksichtigung unserer Anträge.	ISSS

Die qualifizierte elektronische Signatur gemäss dem ZertES von 2003 hat sich in der Praxis nicht in dem ursprünglich erwarteten Umfang durchgesetzt. Dieser Zustand dürfte im Wesentlichen auf folgende Umstände zurückzuführen sein:
a. Der Grundsatz der Formfreiheit im Privatrechtsverkehr (Art. 11 OR) lässt die Abwicklung der überwiegenden Mehrheit aller Rechtsgeschäfte durch beliebige Erklärungsmittel wie Telefon (Art. 4 Abs. 2 OR), E-Mail, Telefax oder SMS zu.
b. Der nicht unerhebliche Aufwand im Zusammenhang mit der Ausstellung und der Verwendung der qualifizierten elektronischen Signatur nach ZertES und die mit der Verwendung von zertifikatsgestützten kryptografischen Schlüsseln verbundene ver schuldensunabhängige Gefährdungshaftung (Art. 59a OR) dürfte viele Subjekte des Privatrechts vom Erwerb und der Verwendung von elektronischen Signaturen abschrecken.
c. Das Fehlen einer Rechtsgrundlage für das Signieren maschinell lesbarer Dokumente durch juristische Personen und öffentlich-rechtliche Organisationen erwies sich als erhebliche Schranke für die Anwendung der elektronischen Signatur im Verkehr von Un ternehmen und Behörden.
Das ZertES schafft die rechtlichen Rahmenbedingungen für die technischen und organisatorischen Grundlagen im Zusammenhang mit elektronischen Signaturverfahren, welche bestimmte Mindestanforderungen erfüllen, kann als solches jedoch nur einen beschränkten Beitrag zur Durchsetzung derartiger Verfahren in der Praxis leisten.
Die breite Anwendung der elektronischen Unterschrift setzt nach unserer Auffassung eine umfassende Uberprüfung des gesamten Privat- und Verwaltungsrechts (Bund und Kantone) voraus, wobei für jeden Kommunikationsvorgang die Anforderungen an die Identifizierung, Authentifizierung sowie Wahrung der Integrität zu prüfen und flexibel zu regeln sind.
Dabei sind zwei Gesichtspunkte zu berücksichtigen:
a. Erstens ist anzustreben, dass generell der elektronische Geschäftsverkehr nach Möglichkeit gefördert wird. Dies bedeutet auch, dass für den elektronischen Geschäftsverkehr keine unnötig hohen formellen Anforderungen geschaffen werden, wo dies nicht notwendig ist. Zu vermeiden ist z.B., dass im elektronischen Bereich die geregelte oder qualifizierte elektronische Signatur gefordert wird, wenn „auf Papier“ keine entsprechen den Formerfordernisse gelten (zu erinnern ist an das Beispiel des deutschen Steuervereinfachungsgesetzes vom 1.11.2011, wo auf das zwingende Erfordernis der elektronische Signatur für Rechnungen im Rahmen der Mehrwertsteuer verzichtet wurde, da auch auf Papier nicht erforderlich ist, dass Rechnungen unterschrieben sind).
b. Zweitens ist nach Möglichkeit dafür zu sorgen, dass dort, wo für den elektronischen Geschäftsverkehr der Einsatz der im ZertES geregelten Signaturtypen gefordert wird, auch tatsächlich die Möglichkeit von deren Einsatz sichergestellt ist, und nicht daran scheitert, dass der Adressat für den Empfang und die Prüfung von digital signierten Nachrichten
technisch gar nicht vorbereitet ist.
Als Beispiele für jeweils unterschiedliche Anforderungen betreffend Identifizierung, Authentifizierung und Integrität können die Begehren für Auszüge aus dem Grundbuch nach Art. 26ff.
Grundbuchverordnung (GBV — SR 211.432.1) oder aus dem Betreibungsregister nach Art. 8a SchKG einerseits, im Vergleich zum Auszug aus dem Strafregister (Art. 24 VOSTRA Verordnung — SR 331) oder zur Weitergabe von Daten aus einem elektronischen Patientendossier andererseits dienen (in den beiden letztgenannten Fällen geht es um “besonders schützenswerte Daten“ im Sinne von Art. 3 Bst. c DSG, was als Hinweis für qualifizierte Sicherheitsanforderungen dienen kann) sowie der Vergleich zwischen der Einreichung einer allgemeinen Anfrage oder Eingabe an eine Behörde, im Vergleich zur Zustellung einer Rechtsschrift innerhalb einer

rechtsverbindlich zu wahrenden Frist oder der Teilnahme an einer elektronischen Abstimmung. Richtungsweisend für die Zulassung vereinfachter elektronischer Kommunikationsvorgänge könnten Art. 23 Ziff. 2 des Lugano Übereinkommens (SR 0.275.12) sowie Art. 17 Abs. 2 ZPO sein, wo der elektronische Abschluss von Gerichtsstandsvereinbarungen zugelassen wird, wenn sie eine "dauerhafte Aufzeichnung der Vereinbarung in Textform" ermöglichen; eben falls kann in diesem Zusammenhang auf die offene Formulierung von Art. 9 Abs. 1 Bst. b Ziff. 1 GeBüV — SR 221.431) hingewiesen werden. Eine allgemeine Gesetzgebung betreffend den elektronischen Geschäftsverkehr zwischen Privaten und Behörden sollte daher auch Formen der elektronischen Kommunikation zulassen, welche im ZertES nicht geregelt sind, wie Zustellung durch E-Mail oder die Zulassung der fortgeschrittenen elektronischen Signatur. Nur für anspruchsvolle Anwendungen ist die Notwendigkeit der Verwendung der geregelten bzw. der qualifizierten elektronischen Signatur vorzusehen. Als Grundsatz sollte gelten, dass überall dort, wo der elektronische Verkehr mit der Verwaltung möglich und zulässig ist, die Privaten einen Anspruch auf elektronische Übermittlung haben und die Behörden zur Bereitstellung der entsprechenden Infrastruktur verpflichtet sind. Dies gilt insbesondere auch dann, wenn für die elektronische Kommunikation die im ZertES geregelten Signaturverfahren gesetzlich vorausgesetzt sind. Diese Anforderung könnte mit verhältnismässig geringem Aufwand, und unter Einräumung einer angemessenen Übergangsfrist, durch die Pflicht zum Anschluss aller (Bundes-) Behörden an eine elektronische Zustellplattform erfüllt werden. Subjekte des Privatrechts hätten hierauf die Möglichkeit, die gesetzlichen Anforderungen an Form und Frist für die Eingabe an eine Behörde zu erfüllen, wenn sie eine solche in maschinell lesbarer Form, unter Verwendung der digitalen Signatur, an die von der betreffenden Behörde bezeichnete Zustellplattform einreichen. Parallel zu der vorstehend vorgeschlagenen Regelung wäre denkbar, dass bestimmte Rechtssubjekte des Privatrechts, z.B. die sog. "Publikumsgesellschaften" gemäss Art. 727 OR, verpflichtet werden, Möglichkeiten für die elektronische Kommunikation mit Behörden und Privaten zu schaffen. Im Sinne von Beispielen sei nachstehend auf die wichtigsten möglichen Anwendungen elektronischer Signaturverfahren im öffentlichen Bereich hingewiesen, welche die Anwendung elektronischer Kommunikation massgeblich fördern würden: a. Anerkennung elektronisch signierter Dokumente als "Rechtsöffnungstitel" im Sinne von Art. 82 SchKG; b. Ein- und Ausfuhrwesen, inklusive Ursprungsdeklarationen; c. Verkehr mit Gerichten und Vollstreckungsbehörden sowie mit Behörden im Rahmen von Verwaltungsverfahren. Nach Auffassung der ISSS sollte die Totalrevision des ZertES im Interesse des Wirtschaftsstandortes Schweiz a. auf die Bedürfnisse der Anwender in der Praxis, insbesondere für den elektronischen Verkehr mit Behörden und Amtsstellen, ausgerichtet werden; b. als Regelung der Rahmenbedingungen für Signaturverfahren für Kommunikationstatbestände mit hohen Anforderungen an die Identifizierung, Authentifizierung und Integrität in eine umfassende Gesetzgebung über die elektronische Kommunikation im Bereich des privaten und des öffentlichen Rechts eingebettet werden und c. auf die internationale Entwicklung der elektronischen Kommunikation abgestimmt werden, wie sie insbesondere im Vorschlag vom 4.6.2012 für eine Verordnung des Europäischen Parlamentes über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt zum Ausdruck kommt.	

Aufgrund dieser Überlegungen sollte die Totalrevision des ZertES zwar weitergeführt, jedoch erst abgeschlossen werden, wenn die vorstehend umschriebenen wesentlichen Anforderungen erfüllt werden können.	
Bisher ist der Durchbruch der elektronischen Signatur bei den natürlichen Personen nach unserem Dafürhalten ausgeblieben. Dies hat vor allem mit der Formfreiheit im Privatrechtsverkehr und dem Aufwand für die qualifizierte elektronische Signatur nach ZertES zu tun. Durch die Totalrevision des ZertES soll die elektronische Signatur auf juristische Personen ausgedehnt werden. Im Geschäftsbereich dominiert ebenfalls die Formfreiheit. Wir erwarten daher nicht, dass der bisher ausgebliebene Durchbruch der elektronischen Signatur nun im B2B- oder B2C-Bereich stattfinden wird. Verschiedene Rückmeldungen aus unserer Mitgliedschaft bestätigen diese Erwartung. Bereits heute werden problemlos Verträge per E-Mail rechtsverbindlich abgeschlossen; auch ohne elektronische Signatur. Wenn überhaupt, dann rechtfertigt sich die elektronische Signatur am ehesten im Kontakt mit Behörden. Wir möchten aber in aller Form darauf hinweisen, dass die Verwendung von elektronischen Mitteln auf freiwilliger Basis beruhen muss. Falls man sich nicht auf den Kontakt mit Behörden beschränken will, ist es aufgrund der starken Ausrichtung der Schweizer MEM-Industrie auf internationale Märkte wichtig, dass die Gesetzgebung der Schweiz international abstimmt wird. Dabei sind vor allem die neueren Entwicklungen (Vorschlag vom 4. Juni 2012 für eine Verordnung des Europäischen Parlaments über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt) im Auge zu behalten. Wir beantragen das Folgende: 1. Wir erachten eine Ausdehnung der elektronischen Signatur auf Unternehmen als zurzeit verzichtbar. 2. Wenn die elektronische Signatur auf juristische Personen ausgedehnt wird, dann sollte sie auf den Kontakt der Unternehmen mit Behörden beschränkt bleiben. Die Verwendung der elektronischen Mittel für diesen Kontakt muss dabei freiwillig sein. 3. Falls man wie beabsichtigt an einer umfassenden Regelung festhält, sollte sich der Gesetzesvorschlag an den internationalen Entwicklungen orientieren.	SwissMem
a) Das geregelte Zertifikat kann sowohl für Authentisierung als auch für Signatur verwendet werden. Die Signatur entspricht aber nicht einer eigenhändigen Unterschrift gemäss OR 14 durch eine natürliche Person. Dafür ist nach wie vor ein qualifiziertes Zertifikat zu verwenden. Bei der Verwendung eines geregelten Zertifikates für Signierung durch eine natürliche Person besteht bezüglich Haftung gemäss OR 59 a (neu) aber kein Unterschied zu einem qualifizierten Zertifikat. Die in Punkt 5 angesprochene verschiedene Haftung für Authentisierung und Signatur legt deshalb nahe, dass es möglich sein sollte, ein Zertifikat NUR für Authentisierung lösen zu können und für Signierung im Sinne von OR 14 Abs. 2bis ein qualifiziertes Zertifikat zu lösen. Im Abschnitt 1.2 des erläuternden Berichtes „Ziele der Revision“ wird diese Ansicht gestützt durch (Zitat) „In der Praxis wird das Vertrauen zwischen Partnern im elektronischen Verkehr in der Mehrzahl der Fälle nicht durch eine signierte Meldung, sondern durch die Authentisierung an einem Online-Dienst hergestellt.“ b) Die Haftungs-Regelung für geregelte Zertifikate, wonach bei geregelten Zertifikaten nur bei Signatur und nicht bei Authentisierung die implizite Beweislastumkehr von OR 59 a (neu) gilt, ist missverständlich (unklar, schwer zu verstehen). Diese Regelung wird im erläuternden Bericht durch die Aussage zu OR 59a (neu) erörtert, wonach diese Haftung eine essentielle Grundlage für die Akzeptanz von geregelten Zertifikaten bei Dritten sei. Wir bezweifeln diese Aussage aber. Das Problem kann gelöst werden, indem die beste-	CI AG

hende Formulierung von OR 59a beibehalten wird, d.h. dass diese Haftungsregelung nur für qualifizierte Zertifikate gilt. Ohne implizite Beweislastumkehr wird die geregelte elektronische Signatur gemäss Neufassung Art. 2.c zu dem, was eine Unterschrift im normalen Geschäftsverkehr ist. c) Die Referenzierung der UID-Einheit im geregelten Zertifikat gemäss UIDG vom 18.6.2010 ist ein starker „Added Value“ für ein geregeltes Zertifikat. Es ist aber notwendig, dass dies in einer Weise geschieht, welche die Interoperabilität mit bestehenden Identifikator-Systemen zur Identifikation von Zertifikatshaltern gewährleistet. Dies können etwa private Schemen sein, die im automatisierten B2B-Verkehr genutzt werden (z.B. GS1 GLN od. D&B D-U-N-S). Zu beachten ist auch, dass auch Privatpersonen UID-Einheiten sein können und somit eine UID besitzen. Hier muss eine klare Unterscheidung zu Nummerierungs-Systemen für Privatpersonen (z.B. SuisseID-Nr.) möglich sein. Die neue Verordnung und die Technischen Administrativen Vorschriften müssen deshalb verlangen: Die zugehörige Identifikationsnummern (UID) müssen gemäss bestehenden internationalen Normen referenziert werden, sodass sie auch international automatisch ausgelesen und verwendet werden können; in Art. 20 des neuen ZertES sind die gesetzlichen Grundlagen gegeben. Beim Comité Européen de Normalisation (CEN) sind die notwendigen Standards vorhanden. d) Begrüssenswert ist die Möglichkeit, ein geregeltes Zertifikat auf irgendeine UID-Einheit ausstellen zu können. Dadurch kann auch eine einfache Gesellschaft (keine juristische Person), welche mehrwertsteuerpflichtig ist, ein geregeltes Zertifikat erhalten. Damit ist auch ein Problem der Mehrwertsteuer-Verwaltung gelöst und es braucht kein spezielles Zertifikat.	
SwissSign ist eine Tochtergesellschaft der Schweizerischen Post („Post“) und seit 2006 anerkannte Anbieterin für qualifizierte Zertifikate nach ZertES. Als weltweit tätiger Certificate Service Provider („CSP“) stellt SwissSign auch Zertifikate nach anderen Standards (z. B. EV SSL nach CABForum, ETSI TS 101 456, Webtrust, ISO 27001, Time-Stamping etc.) aus. SwissSign ist in diversen Standardisierungsgremien (z. B. Trägerschaft SuisseID) aktiv beteiligt. Zudem ist SwissSign ein führender Anbieter von Sicherheitstechnologien, die u.a. auf Zertifikatstechnologie basieren. SwissSign hat dabei wertvolle Erfahrungen sowohl im Konsumentenmarkt als auch im Firmen- und Behördenumfeld gewinnen können. Die Post setzt konzernweit auf Technologien, die nicht zuletzt auch dank dem Einsatz elektronischer Signaturen und Zertifikate erlauben, ihren privaten und staatlichen Kunden im In- und Ausland attraktive und sichere innovative Dienstleistungen anzubieten. Die Post ist eine führende Anbieterin von E-Government-Lösungen und setzt dabei zentral auch auf die Technologielösungen von SwissSign. Die Revision des ZertES betrifft das Kerngeschäft unserer Tochtergesellschaft SwissSign. Zudem ist die Revision für diverse Innovationsprojekte der Post von Bedeutung. Aus diesen Gründen kommt die Post gerne dem Wunsch von SwissSign nach, sie bei der Vernehmlassung zu unterstützen. Die vorliegende Vernehmlassungsantwort soll in erster Linie den Anliegen von SwissSign, die auch unsere sind, Geltung verschaffen. Das menschliche Kommunikationsverhalten hat sich im letzten Jahrhundert und vor allem in den letzten zwei Jahrzehnten dank neuer Technologien (Telefonie, Funk/Radio, Halbleiter/Digitalisierung, Computernetzwerke/Internet etc.) grundlegend verändert. Kennzeichnend ist die extreme Geschwindigkeit und die zunehmende Automatisierung digitaler Kommunikationsvorgänge. Den Effizienz- und Annehmlichkeitsgewinnen aller Beteiligten stehen Anonymisierung und kaum mehr fassbare Komplexität der eingesetzten Technik gegenüber. Wir haben die Erfahrung gemacht, dass sowohl die Informationstechnologie wie auch deren staatliche Regulierungen (wie z. B. das	Die Post

ZertES) für nicht mit der Materie eingehend vertraute Personen in der Regel nur sehr schwer verständlich sind.

Die Kommunikationsprotokolle, auf denen das Internet basiert, sehen die Identifizierung von Maschinen mittels eindeutiger Adressen, nicht aber von deren Benutzern vor.
Viele Menschen kommunizieren über das Internet anonym oder unter Pseudonym. Die Gründe dafür können z. B. sein, dass den Kommunikationspartnern eine virtuelle Identität genügt oder dass die Kommunikationspartner ihre Identität zwar gegenseitig kennen, aber – wie dies auch in der realen Welt selbst unter unverdächtigen Umständen durchaus üblich ist – keinen Grund zur Offenlegung sehen. So ist es für die meisten Internetbenutzer eine Selbstverständlichkeit, dass das „Ansurfen" von Internetseiten oder die Abfrage von Suchmaschinen nicht erst nach einer erfolgreichen Identifizierung ihrer Person möglich ist. Auf dem Internet ist jeder in erster Linie, wer er zu sein vorgibt, und nicht, wer er tatsächlich ist.
Anderseits haben viele Internetbenutzer in bestimmten Situationen das Bedürfnis, im Internet nicht mit anderen verwechselt zu werden und andere Benutzer zuverlässig unterscheiden zu können. Die verlässliche Unterscheidung von Personen an Hand ihrer wahren Identität und nicht nur einer virtuellen Identität ist überall dort erforderlich, wo Personen, Unternehmen oder Behörden rechtsverbindlich handeln oder wo aus anderen Gründen die Identität der Beteiligten von Bedeutung ist.
Ohne auf die Einzelheiten von Identifizierungs- und Authentifizierungstechnologien eingehen zu wollen, kann festgehalten werden, dass die Akzeptanz neuer Technologien1 weitgehend davon abhängt, ob der Benutzer sie als benutzerfreundlich und nützlich wahrnimmt. Für die Signaturtechnologie ist neben einheitlicher Standards eine breite Akzeptanz von grosser Bedeutung, da deren Nützlichkeit mit der Anzahl Benutzer steigt („Netzwerkeffekt").
Da die Signaturtechnologie mit bewährten, weitverbreiteten und relativ günstigen Papierlösungen konkurrenziert, muss sie gar subjektiv als überlegen wahrgenommen werden.
Die Signaturtechnologie hilft, rechtsverbindliches Handeln im Internet in erweiterter Weise zu ermöglichen und besetzt damit eine zentrale Schnittstelle zwischen Computercode und Rechtsordnung. Die Technologie einerseits und die staatliche Regulierung derselben anderseits bilden ein Ganzes. Die Regulierung wird quasi zum Bestandteil der Technologie und umgekehrt. Vorbehalte gegen einen Einzelteil hemmen die Akzeptanz des Ganzen. Aus einer Endanwenderperspektive beeinflusst die Rechtsordnung vor allem die Nützlichkeit und die Technologie vor allem die Benutzerfreundlichkeit. Eine einfach handhabbare elektronische Signatur, die von der Rechtsordnung nur in unklaren Situationen als rechtsgültig anerkannt wird, findet kaum Akzeptanz. Desgleichen würde eine von der Rechtsordnung global anerkannte elektronische Signatur kaum akzeptiert werden, wenn sie technisch benutzerunfreundlich umgesetzt wäre.
Entscheidungsträger in Unternehmen und Behörden, die sich zwar mit den gesetzlichen Vorgaben auseinandersetzen, diese aber nicht auf den ersten Blick verstehen oder anderen Entscheidungsträgern verständlich machen können, werden tendenziell zurückhaltender sein, den Einsatz der Technologie im eigenen Unternehmen oder in der eigenen Behörde zu akzeptieren oder andere davon zu überzeugen versuchen.

Die SuisseID ist der erste national standardisierte elektronische Identitätsnachweis für natürliche Personen, mit dem sowohl eine rechtsgültige elektronische Signatur wie auch eine sichere Authentifizierung möglich sind. Bei der SuisseID befinden sich die entspre-

chenden elektronischen Zertifikate auf einem ausschliesslich dafür bestimmten Mikrochip (sog. Hard-Token). Das Staatssekretariat für Wirtschaft SECO ist Eigentümerin der Marke „SuisseID“ (fig.) und Gründungsmitglied des Vereins „Trägerschaft SuisseID“, der die SuisseID fördert und weiterentwickelt. Die SuisseID wird seit Mai 2010 von drei Anbietern, zu denen auch wir gehören, verkauft. Mittlerweile sind mehrere Hunderttausend SuisseID bei Behörden, Unternehmen und Privatpersonen im Einsatz.
Mit der SuisseID Initiative hat der Bund unserer Ansicht nach rechtzeitig einen zukunftsweisenden Weg eingeschlagen, der nun gemeinsam mit allem Akteuren weiter zugehen ist.

Unsere langjährige Erfahrung lehrt uns, dass bei jeder Regulierung immer vom Nutzer und dem von diesem verfolgten Zweck (Prozesse, Geschäftsfall, Use Case) auszugehen ist. Der Geschäftsfall bildet das logische Fundament für übergeordnete Überlegungen. Diese Geschäftsfälle können bezüglich Zertifikate auf folgende Grundanwendungen oder deren Kombinationen zurückgeführt werden:

- Willensäusserung des Akteurs Zertifikatsinhaber. Beispiele: Verträge (OR), gerichtliche Eingaben (VeÜ-ZSSchK, VeÜ-VwV);
- Dokumentenauthentizitätsnachweis, d. h. Nachweis, dass ein bestimmtes Dokument vom Akteur Zertifikatsinhaber stammt und nicht verändert wurde. Beispiele: Rechnungen (Bsp. ElDI-V), Kontoauszüge, Registerauszüge, Archivdaten (GeBüV), etc.;
- Identitäts- und Authentizitätsnachweis des Akteurs Zertifikatsinhaber. Beispiele: Identitätsnachweise;
- Gewährleistung der Vertraulichkeit der Kommunikation zwischen zwei Partner Beispiel: Einhalten von Datenschutzanforderungen.

Eine staatliche Regulierung hat von diesen Grundanwendungen, so wie sie in den Amts und Geschäftsverkehr aufgenommen werden sollen, auszugehen. Die Regulierung der Anerkennung der Verwendung der Technologie im Geschäftsverkehr und die Regulierung der Qualitätsanforderungen an die dabei verwendete Technologie, sind wegen der inhärenten Wechselwirkungen gegeneinander abzustimmen bzw. als Einheit zu betrachten.

Die Anwendungsbereiche der elektronischen Signatur sind im ZertES selber nicht geregelt. Insbesondere fehlt eine für die ganze Rechtsordnung zentrale Norm für die Anerkennung elektronischer Signaturen. Zwischen der Regelung der Qualität von elektronischen Signaturen und der Regelung von Anwendungsbereichen der elektronischen Signatur bestehen viele Wechselwirkungen.
In unzähligen Einzelerlassen auf Gesetzes- und Verordnungsstufe sind für einzelne Anwendungsfälle in einzelnen Rechtsgebieten die Voraussetzungen an die elektronische Signatur und weitere formelle

Anforderungen für deren Verwendung (z. B. zwingende Zustellplattform) geregelt. In vielen Fällen wird die qualifizierte elektronische Signatur nach ZertES als Referenz und als genügend anerkannt. Im wichtigen Anwendungsfall der Erzeugung mehrwertsteuerkonformer Rechnungen genügen fortgeschrittene Signaturen; qualifizierte Signaturen werden dort zwar im Grundsatz, aber nicht ausnahmslos akzeptiert.
Vor diesem Hintergrund gilt zusätzlich zu beachten, dass gemäss den Erläuterungen der Bundesrat das EJPD am 28. März 2012 damit beauftragt hat, den Umfang einer umfassenden Gesetzgebung im Anwendungsbereich der elektronischen Signatur abzuklären und dem Bundesrat bis Ende 2012 einen Vorschlag zum weiteren Vorgehen zu unterbreiten.
Der erläuternde Bericht, S. 2, erwähnt z. B. dass die Möglichkeit ausgelotet werden soll, die Anforderungen an die qualifizierte elekt-

ronische Unterschrift als Äquivalent zur eigenhändigen Unterschrift zu senken.
Bedeutende regulatorische Veränderungen auf nationaler Ebene mit unmittelbaren Wechselwirkungen zur Regelungsmaterie der vorliegenden Totalrevision sind zu erwarten.

Regulierung schafft Vertrauen und Stabilität. Nach Regulierungsänderungen müssen sich Vertrauen und Stabilität erst wieder einstellen bzw. erarbeitet werden. Trotz der vorliegenden Totalrevision erscheinen kurz- bis mittelfristig weitere tiefgreifende Totalrevisionen des ZertES unausweichlich, um eine national und international abgestimmte Regulierung zu gewährleisten.
Produkte und Systeme, die qualifizierte Signaturen und Zertifikate einsetzen, sind bei jeder Gesetzesänderung zumindest daraufhin zu prüfen, ob sie an die neuen Vorschriften angepasst werden müssen. In vielen Fällen sind Anpassungen unausweichlich, um neue gesetzliche Qualitätsvorgaben erfüllen zu können. Bereits ausgelieferte Produkte lassen sich, wenn überhaupt, nicht ohne Weiteres aktualisieren. Oft müssen sie ersetzt werden, was für den Benutzer unerwünschte Umtriebe mit sich bringt und Zweifel an der Investitionssicherheit, Beständigkeit und Zuverlässigkeit der Technologie entstehen lassen.
Eine Abfolge grösserer Regulierungsänderungen gefährdet die Akzeptanz der Signatur-Technologie und ist für deren Verbreitung schädlich. Die durchaus vorhandenen Verbesserungen der vorliegenden Totalrevision können diesen schwerwiegenden Nachteil nicht aufwiegen.

Wir begrüssen alle regulatorischen Anstrengungen, die den Einsatz von Zertifikaten und Signaturen sowohl vereinfachen, als auch die grösstmögliche Klarheit, Sicherheit und Verlässlichkeit schaffen.
Beim ursprünglichen ZertES vom 19. Dezember 2003 (Stand am 1. August 2008) stand die Grundanwendung „Willensäusserung des Akteurs Zertifikatsinhabers“ im Fokus und wurde entsprechend umfassend abgedeckt, indem auch Pflichten und Rechte aller relevanten Akteure beschrieben wurden. Die nun in der Vernehmlassung stehende Änderung hat diesen Fokus verloren. So ist es für den Leser unklar, welcher Typ von Signatur/Zertifikat für welcher Grundanwendung zu verwenden ist. Dies wird durch das Ausschliessen der Rechtswirkung bei der Verwendung von Zertifikaten (s. Art. 1 Abs. 2 VE ZertES) explizit gemacht.
Wie das geltende ZertES beschränkt sich die vorliegende Totalrevision auf die Regelung der Qualität einiger ausgewählter Zertifikats-Produkte. Die rechtliche Anerkennung der elektronischen Signatur ist nach wie vor punktuell in Einzelgesetzen für die jeweiligen Bereiche geregelt. Die lediglich punktuelle Anerkennung elektronischer Signaturen und teilweise abweichenden qualitativen Anforderungen an deren Qualität behindern die Verbreitung der Signaturtechnologie.
Eine grundsätzliche rechtliche Anerkennung der qualifizierten elektronischen Signatur durch Gleichsetzung mit der eigenhändigen Unterschrift für die gesamte Rechtsordnung in einer zentrale Anerkennungsnorm, wie sie z. B. Österreich (§ 4 (1) Signaturgesetz) kennt, halten wir für einen enorm wichtigen und lange überfälligen Schritt, um der elektronischen Signatur zu der gewünschten, breiten Verwendung zu verhelfen. Wir wünschen dies nicht als Selbstzweck, sondern weil wir von den vielfältigen Vorteilen und dem gesamtgesellschaftlichen Nutzen eines elektronischen Wirtschaftsraumes überzeugt sind.
Möglichst breit abgestützte, verlässliche Qualitätsstandards für elektronische Signaturen sind Voraussetzung für die Anerkennung von elektronischen Signaturen in Geschäfts- und Behördenprozessen und für deren Akzeptanz in der Bevölkerung.
Für eine breite Akzeptanz der Signaturtechnologie bei den Bürgerinnen und Bürgern sowie in Verwaltung und Wirtschaft ist ein

sprachlich verständliches Gesetz unabdingbar. Das ZertES in seiner aktuellen Version wie auch der Vorwurf sprechen eine Sprache, die nur für mit der Zertifizierungstechnik Vertraute zugänglich ist. Die Verständlichkeit des Textes kann unseres Erachtens bereits durch wenige kleine sprachliche Anpassungen (siehe z. B. unten: 3.3, 3.4, 3.7, 3.12, 3.17, 3.21, 3.22, 3.23, 3.26, 3.27) stark verbessert werden. Anderseits haben wir durchaus Verständnis dafür, dass die Regulierung einer komplizierten Technologie ein gewisses Technologieverständnis voraussetzt. Allerdings sollte bei der Regulierung im Auge behalten werden, dass sie für ein breiteres Publikum verständlich sein soll und nicht nur für Experten. Dies darum, weil die Akzeptanz der Technologie von der subjektiven Wahrnehmung jedes einzelnen potentiellen Benutzers abhängt und die Qualität der Regulierung diese mit beeinflusst. Das Ziel der Gesetzesrevision, einer terminologische Bereinigung bzw. Vereinfachung bei der Regelung der elektronischen Signatur in den verschiedenen Gesetzen und Verordnungen herbeizuführen, wird nur teilweise erreicht. Insbesondere fehlt der ganze Bereich des Verwaltungsrechtes. Es bleibt z. B. weiterhin unklar, ob man Steuererklärungen elektronisch unterzeichnen darf oder nicht. Die ElDI-V - einer der Auslöser dieser Revision – wird nicht angepasst. Eine umfassende Einordung dieser Gesetzesrevision ist daher nicht möglich und führt zu folgenden Thematiken: Es ist nicht ersichtlich, für welche Anwendung welcher Zertifikatstyp zu nutzen ist und was dessen Sicherheits-/Vertrauensniveau sein soll; der Bundesrat wird das dann entscheiden. Im Anwendungsfall „Identitäts- und Authentizitätsnachweis des Akteurs Zertifikatsinhaber“ gibt es internationale Trends, wie beispielsweise das CABForum, indem Entwickler von Anwendungssoftwaren und CSP zusammenarbeiten um eine hohe Güte im Bereich Zertifikate zu erhalten. Mit dieser Revision besteht die Gefahr, dass Zertifikatsanforderungen diesen internationalen Tendenzen entgegenlaufen. So erhält der Bundesrat durch die starke Verallgemeinerung die Kompetenz das Zertifikatsgeschäft in der Schweiz sehr weitgehend zu regeln. So könnte er sowohl SSL Zertifikate als auch Personenzertifikate regeln, was zu Inkompatibilitäten mit internationalen Industriestandards führen könnte. Die Anforderung, sichere Signaturerstellungseinheiten für qualifizierte Signaturen zu nutzen, entfällt auf Gesetzesstufe. Durch die Konzentration auf ein Gesetz für die Regelung der CSPs entfällt die Darstellung aller Akteure sowie eine Beschreibung derer Rechten und Pflichten: Zertifikatsinhaber; Partei, die sich auf die Angaben im Zertifikat verlässt; Zertifizierungsdienstanbieter (CSP), als unabhängiger Dritte, der die Angaben im Zertifikat bescheinigt; Prüfgesellschaft, die den CSP überwacht und deren korrektes Arbeiten bestätigt. Obwohl der Bundesrat die Kompetenz erhält Zertifikate für Identifizierungs- und Authentifizierungszwecke zu definieren, ist deren Einsatz beispielsweise im Bereich Identifizierung im GwG-Umfeld nicht klar. Für sehr wichtig halten wir, dass die Auswirkungen der Einführung einer juristischen Person zugänglichen geregelten Signatur sorgfältig geprüft werden. Insbesondere stellt sich die Frage, wie diese Signatur im Vertretungs-, Handelsregister- und Gesellschaftsrecht positioniert werden soll. Entsprechend sind dann die Qualitätsanforderungen zu definieren. Wir sind der Ansicht, dass die vorliegende Revision mit dem internationalen Umfeld abgestimmt sein muss und dies im Rahmen der	

von uns vorgeschlagenen „grossen Totalrevision“, jedenfalls aber im Rahmen der vorliegenden Totalrevision zu erfolgen hat. 2.4 Zwischenergebnis Wie oben dargelegt, geht die Totalrevision nicht weit genug und berücksichtigt neue regulatorische Entwicklungen auf der nationalen und europäischen Ebene nicht. Daher empfehlen wir, die vom Bundesrat in Auftrag gegeben Abklärung bezüglich Umfang einer umfassenden Gesetzgebung im Anwendungsbereich der elektronischen Signatur abzuwarten und dann auf deren Basis zu klären, welche Änderungen an der aktuellen ZertES notwendig sind, damit Zertifikate die Förderung von e-Goverment, e-Commerce und e-Health optimal unterstützen. Sinnvollerweise werden die beiden bisher künstlich getrennten Regelungsmaterien im Rahmen einer „grossen Totalrevision“ in einem neuen „Bundesgesetz über die elektronische Signatur“ konsolidiert. Dabei soll auch das internationale Umfeld bezüglich dessen Konzepte berücksichtigt werden. Kern der Revision ist die Einführung der sog. geregelten Signatur für juristische Personen und Behörden. Dieses begrüssenswerte Anliegen lässt sich auch mit einer Teilrevision umsetzen. Für eine Totalrevision ist der aktuelle Zeitpunkt, wie dargelegt, ungünstig. Die kurzfristige Einführung des „geregelten Zertifikates“ und der „geregelten Signatur“ im Rahmen einer darauf reduzierten Teilrevision oder auf Verordnungsebene sehen wir hingegen als gangbaren Weg, um die Einführung eines solchen neuen Produktes nicht zu verzögern. Die „geregelten“ Produkte wären parallel zu und unabhängig von den „qualifizierten“ zu regeln. Die Qualitätsanforderungen sind mit den zu erwartenden Anwendungen abzustimmen. Vorzugsweise ist die vorgelegte Totalrevision demzufolge bis auf Weiteres zurückzustellen. Wir halten den Zeitpunkt für eine Totalrevision des ZertES für verfrüht. Im Rahmen einer „grossen Totalrevision“ sollen Anwendungsbereich und Qualität der elektronischen Signatur stimmig geregelt werden. Dabei müssen regulatorische Entwicklungen der EU zwingend berücksichtigt werden, damit die internationale Anerkennung der nach ZertES erstellten Zertifikate und Signaturen gewährleistet ist. Gegen eine kurzfristige Einführung des „geregelten Zertifikates“ und der „geregelten Signatur“ im Rahmen einer Teilrevision haben wir nichts einzuwenden. Sollte die vorgelegte Totalrevision weiterverfolgt werden, muss auf jeden Fall die Verständlichkeit des Gesetzestextes durch sprachliche Massnahmen verbessert werden. Wir hoffen, mit diesen Ausführungen dazu beizutragen, dass ein Kernanliegen des Vorentwurfes, die Begünstigung der Verwendung digitaler Zertifikate und elektronischer Signaturen, erreicht werden kann.	

Der SWICO: Als Verband der Anbieter von Informations-, Kommunikations- und Drganisationstechnik bündelt der SWICO die Interessen der ICT- und CE-Branche und vertritt diese gegenüber Öffentlichkeit, Politik und Verwaltung. Seinen über 400 Mitgliedern bietet der SWICO zudem eine breite Palette von Dienstleistungen, Informationen und Vernetzungsmöglichkeiten. Die elektronische Signatur gemäss dem ZertES von 2003 hat sich in der Praxis nicht durchsetzen können. Ein Grund hierfür kann — neben der weitgehenden Formfreiheit im Privatrecht — im grossen Aufwand für die qualifizierte elektronische Signatur nach ZertES und in der mit der Verwendung von zertifikatsgestützten kryptografischen Schlüsseln verbundenen Gefährdungshaftung (Art. 59a OR) gesehen werden. Diese dürfte viele Subjekte des Privatrechts vom Erwerb und der Anwendung von elektronischen Signaturen abschrecken. In der Folge hat dies dazu geführt, dass die Teilnehmer am elektronischen Markt (für Geschäfte im B2B und B2C) eigene Regeln für die elektronische Abwicklung geschäftlicher Transaktionen entwickelten, welche sich in der Praxis bewährt haben (wie etwa die EDI Mustervereinbarung des SWICO), so dass heute im Privatrechtsverkehr nur wenige elektronische Transaktionen mit Hilfe qualifizierter Signaturen einer anerkannten Anbieterin von Zertifizierungsdiensten abgewickelt werden. Die ZertES mit ihrem in der Natur der Sache liegenden technischen Approach ist eigentlich nur ein Baustein zur Regelung des elektronischen Marktes und sollte sich auf Transaktionen beziehen, welche eine sehr hohe technische Sicherheit voraussetzen. Für das Massengeschäft braucht es unseres Erachtens indes einfachere und umfassendere Ansätze. Vor wenigen Tagen, am 4. Juni 2012, hat die Europäische Kommission neue Vor schriften vorgeschlagen, um grenzüberschreitende und sichere elektronische Transaktionen in Europa zu ermöglichen. Als Grundsatz sollte gelten, dass überall dort, wo der elektronische Verkehr mit der Verwaltung möglich und zulässig ist, die Privaten einen Anspruch auf elektronische Übermittlung haben und die Behörden sowie Amtsstellen zur Bereitstellung der entsprechenden Infrastruktur (innert angemessener Übergangsfrist) verpflichtet sind. Wir erachten also die Schaffung einer umfassenden Rechtsgrundlage für die effiziente und breite Anwendung digitaler Signaturverfahren im privaten und öffentlichen Bereich, wie sie der Bundesrat zu prüfen angeregt hat, als einen wichtigen Beitrag für die Förderung des Wirtschaftsstandorts Schweiz. In dieser umfassenden Regelung sollte die elektronische Signatur nach dem revidierten ZertES ihren Platz für Anwendungen erhalten, bei denen besonders hohe Anforderungen an die Sicherheit der elektronischen Kommunikation zu stellen sind.	SWICO
La révision proposée par le Conseil fédéral favorise et simplifie nettement les procédures d'échanges nécessitant une signature électronique, en particulier pour es entreprises. Nous ne pouvons qu'approuver 1. L'introduction d'une signature électronique pour les personnes morales et autorités, et non plus seulement pour les personnes physiques, comme actuellement. 2. La création d'une base légale qui régit l'authentification via des produits de certification (ex. SWISSD) aujourd'hui seule la signature électronique est réglementée. 3. La simplification de la législation et de la terminologie juridique en la matière.	FER

Zufällig haben wir erfahren, dass das EJPD die Vernehmlassung zur Revision des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur eröffnet hat. Gerne nehmen wir die Gelegenheit wahr, zu dieser Vorlage Stellung zu nehmen. H+ Die Spitäler der Schweiz ist der nationale Verband aller öffentlichen und privaten schweizerischen Spitäler, Kliniken und einiger Pflegeinstitutionen. Uns sind 355 Spitäler, Kliniken und Pflegeinstitutionen als Aktivmitglieder sowie über 200 Verbände, Behörden, Institutionen, Firmen und Einzelpersonen als Partnerschaftsmitglieder angeschlossen. Bitte berücksichtigen Sie uns in Zukunft bei spitalrelevanten Vernehmlassungen und Anhörungen. Unsere nachfolgende Vernehmlassungsantwort beruht auf einer Umfrage bei unseren Mitgliedern. Wir begrüssen es grundsätzlich sehr, dass es künftig auch juristischen Personen und Behörden möglich sein soll, eine bestimmte Form der elektronischen Signatur zu nutzen. Aus unserer Sicht sind die vorgesehenen Änderungen praktikabel.	Spitäler
Herr Holenstein hat im Mail vom 6. April 2012 den Auftrag erwähnt, „den Umfang einer umfassenden Gesetzgebung im Anwendungsbereich der elektronischen Signatur abzuklären“ und in Magglingen geäussert, dass es nicht klar sei, welche Themen – sofern überhaupt – bereits in der ZertES Revision behandelt werden können. Gerne nehmen wir auch aufgrund der Verflechtung der Themenkreise daher die Gelegenheit wahr, die aktuelle Situation im elektronischen Rechtsverkehr aus unserer Sicht kurz zu beleuchten und die nach unserer Auffassung vordringlichsten legislatorischen Handlungsbedarfe aufzuzeigen. Ein Vertreter unsererseits hat bei der Vernehmlassung der „Information Security Society Switzerland (ISSS)“ mitgearbeitet und auch die vergleichsweise komplementäre Vernehmlassungsantwort des Anwaltsverbandes SAV ist uns bekannt. Die in diesen beiden Antworten vorgebrachten Anliegen unterstützt PrivaSphere voll und ganz, mit Ausnahme von wenigen Details, auf die wir unten noch zurückkommen werden. Generell begrüsst PrivaSphere die vorliegende Revision des ZertES. Die Schweiz hat den Bereich des elektronischen Rechtsverkehrs auf eine aus ordnungspolitischer Sicht zukunftsfähige Grundlage gestellt und sowohl bei der Zertifikatsherausgabe wie auch den Zustellplattform eine Mehrzahl von Anbietern vorgesehen. Diese Idee – wenn auch das Prinzip der „gleichlangen Spiesse“ noch erhebliche Mängel aufweist – hat sich realisiert und es hat sich bereits jetzt erfreulicher, für die Endbenutzer qualitätssteigernder Wettbewerb eingestellt. Leider hat sich insbesondere nach der Inkraftsetzung von ZPO etc. der Enthusiasmus der behördenseitigen Umsetzung in engen Grenzen gehalten und das Desinteresse grenzt mancherorts an vorsätzliche Obstruktion. Wie es die Referate an der Tagung im Dezember 2011 im Berner Rathaus gezeigt haben, hat dies zur Folge, dass das Verkehrsaufkommen im elektronischen Rechtsverkehr der Schweiz im Jahr 2011 wohl nicht mal 1 Tausendstel des Aufkommens in Österreich im selben Jahr erreicht hat. Wir empfehlen daher folgende Korrektureingriffe in untenstehender Prioritätsreihenfolge baldmöglichst vorzunehmen: 1) Klärung der Fragen rund um die Fristeinhaltung 2) Vereinheitlichung und Vereinfachung der Signaturanforderungen: Die Formulierung von ZPO Art. 130 Abs. 2 sollte auch für StPO, BGG, VwVG, etc. verwendet werden. 3) Vom allgemeinen Zwang zum elektronischen Rechtsverkehr wie im Nachbarland ist abzusehen, aber ein Bürger/Anwalt soll, wenn er ein Geschäft elektronisch beginnt, auch das Recht haben, es komplett elektronisch weiterzuführen. Vermutlich ist es mittelfristig sinnvoll, jederzeit von jeder Behörde die gesamte Kommunikation ausschliesslich elektronisch verlangen zu können, unabhängig davon ob man selber auch elektronisch an die Behörde übermittelt.	Priva-Sphere

4) Konsequente Umsetzung der Mehrplattformenstrategie: Das Ziel ist ja, dass ein Bürger/Anwalt sich nur auf einer anerkannten Plattform zu registrieren hat, um am elektronische Behördenverehr teilzunehmen. Dies unabhängig davon, ob er fristgebundene Eingaben macht oder sonstige, vertrauliche bzw. datenschutzrelevante Behördenkommunikation vornimmt. Zurzeit wird dieses Ansinnen z.B. vom Zürcher Handelsregisteramt und IncaMail bewusst unterlaufen. Entweder sind die Plattformen zu zwingen, Interoperabilität auf allen Versandarten anzubieten oder Behörden sind zu zwingen, sich auf allen den Bürgern offen stehenden Plattformen zu registrieren, so sie Ihre eigene Plattform nicht zu zielkonformen Diensteangebot motivieren können. 5) Grössere Firmen und Institutionen sind zu verpflichten, elektronische Unterschriften gem. OR Art. 14 entgegenzunehmen. Anknüpfungskriterium könnte sein, dass sie aufgrund der Mitarbeiterzahl bzw. des Umsatzes der ordentlichen Revisionspflicht unterstehen. Als Beispiel unter Vielen ist z.B. die ZKB auch im Juni 2012 nicht in der Lage online angebotene PDF Formulare für Nebensächlichkeiten auch korrekt mittels SuisseID digital signiert elektronisch wieder entgegenzunehmen. Wir empfehlen dringendst, diese Punkte im ZertES oder dem sonst nächsten relevanten, beschlussreifen Geschäft umzusetzen. Verschiedentlich wurde in den letzten Semestern diagnostiziert, dass die Schweiz in Bezug auf Fortschrittlichkeit im elektronischen Bereich im internationalen Vergleich signifikant am Zurückfallen ist. Wir sind zuversichtlich, dass aufgrund der langfristig soliden, vorbildlichen Grundlagen mit obigen Massnahmen innert weniger Jahre ein Auf- oder Überholen möglich sein wird. Der Begründung sowohl des SAV wie der ISSS stimmen wir zu. Beide vorgeschlagenen Formulierungen lassen nach unserer Auffassung aber noch zu viel Interpretationsspielraum. Aufgrund leidiger Erfahrungen in den letzten Monaten empfehlen wir dringend, dass explizit vermerkt wird, dass eine Bestätigung der anerkannten Zustellplattform des Absenders und nicht erst der empfangenden Behörde ausreichend ist, um eine dem heutigen Briefverkehr analoge Risikoverteilung zu erlangen. Gerne möchten wir Ihre Aufmerksamkeit auf weitere Punkte im Alltag des elektronischen Behördenverkehrs lenken. Ob hierzu auf Gesetzes- oder Verordnungsstufe oder noch anderen Verwaltungsmassnahmen Lösungen gefunden werden müssen, überlassen wir gerne Ihrem fachkundigen Urteil. Unnötige Hürden beim interoperablen Versand. Ohne gesetzliche Grundlage lehnt mind. eine Plattform korrekt signierte, elektronische Meldungen ab, wenn sie nicht von einer identifizierten Person stammen. Im Papierverkehr besteht für die die Sendung überbringende Person bei der Post auch keine Ausweispflicht. Die Zulassungskriterien sind so anzupassen, dass hier keine unnötigen Hürden für den Einsatz von Hilfspersonen errichtet werden. Minimalstandards der Diensterbringung. Z.B. das Bundespatentgericht kann nicht mit Meldungen von 8 MB Nutzdaten (und mehr) erreicht werden. Wenn „die ganze Sendung“ zusätzlich noch signiert werden muss, so reduziert sich die maximale Nutzungsmenge nochmals um 33% und gem. Anwälten ist der elektronische Rechtsverkehr so nicht mehr vernünftig nutzbar. Die Behörden sind daher anzuweisen, eine Mindestgrösse von 15 MB Nutzdaten pro Eingabe verarbeiten zu können. „Right to be left alone“ auch bei Teilnahme am elektronischen Rechtsverkehr. Aus Datenschutzüberlegungen sollte es jedem Teilnehmer am elektronische Rechtsverkehr auf mindestens einer Universal-Plattformen möglich sein, seine eMail-Adresse und allenfalls weitere persönliche Angaben von der öffentlichen Suche	

durch andere Behördenverkehrsteilnehmer auszunehmen[1]. Die Auffindbarkeit aller Adressen und Daten mittels Wild-Card Suche muss ein Privileg der unter Amtsgeheimnis stehenden Behörden sein. Interoperable Plattformen dürfen die Datenschutzleistungen der Vertragsplattform eines Nutzers nicht unterlaufen.	
SwissHoldings ist ein branchenübergreifender Wirtschaftsverband. Sie vertritt die Interessen der grossen, in der Schweiz ansässigen Industrie- und Dienstleistungskonzerne und engagiert sich für gute Rahmenbedingungen und ein liberales Wirtschaftsumfeld auf nationaler und internationaler Ebene. SwissHoldings setzt sich für Effizienzverbesserungen und Innovationen im Bereich der digitalen Wirtschaft, namentlich der Rahmenbedingungen zur Nutzung der digitalen Infrastruktur ein, um die Wettbewerbsfähigkeit der Unternehmen langfristig sicherzustellen. SwissHoldings begrüsst die vorgeschlagene Revision als einen wichtigen Schritt zur volkswirtschaftlich notwendigen Förderung der Verbreitung von digitalen Signaturen. Die Wirtschaft hat ein breites Interesse an einem breit abgestützten und erfolgreichen Einsatz der digitalen Signatur. Um dies zu erreichen, ist eine Zertifikatsvergabe auch an juristische Personen notwendig. Ferner soll der internationalen Rechtsentwicklung bestmöglich Rechnung getragen werden. Diese Anliegen sind in der vorliegenden Revision berücksichtigt. Jedoch ist insbesondere die Haftungslage der Zertifikationsinhaber zu verbessern und die internationale Anerkennung auf eine breitere Basis zu stellen. Die elektronische Signatur gemäss dem ZertES von 2003 hat sich in der Praxis nicht durchsetzen können. Ein Grund hierfür kann – neben der weitgehenden Formfreiheit im Privatrecht – im grossen Aufwand für die qualifizierte elektronische Signatur nach ZertES und in der mit der Verwendung von zertifikatsgestützten kryptografischen Schlüsseln verbundenen Gefährdungshaftung (Art. 59a OR) gesehen werden. Diese dürfte viele Subjekte des Privatrechts vom Erwerb und der Anwendung von elektronischen Signaturen abschrecken. In der Folge hat dies dazu geführt, dass die Teilnehmer am elektronischen Markt (für Geschäfte im B2B und B2C) eigene Regeln für die elektronische Abwicklung geschäftlicher Transaktionen entwickelten, welche sich in der Praxis bewährt haben, so dass heute im Privatrechtsverkehr nur wenige elektronische Transaktionen mit Hilfe qualifizierter Signaturen einer anerkannten Anbieterin von Zertifizierungsdiensten abgewickelt werden. Die ZertES mit ihrem in der Natur der Sache liegenden technischen Ansatz ist eigentlich nur ein Baustein zur Regelung des elektronischen Marktes und sollte sich auf Transaktionen beziehen, welche eine sehr hohe technische Sicherheit voraussetzen. Für das Massengeschäft braucht es unseres Erachtens indes einfachere und umfassendere Ansätze. Vor wenigen Tagen, am 4. Juni 2012, hat die Europäische Kommission neue Vorschriften vorgeschlagen, um grenzüberschreitende und sichere elektronische Transaktionen in Europa zu ermöglichen. Die vorgeschlagene Verordnung soll dafür sorgen, dass Personen und Unternehmen mit ihren eigenen nationalen elektronischen Identifizierungssystemen (eID-Systeme) öffentliche Dienste in anderen EU-Ländern benutzen können, sofern dort eine elektronische Identifizierung verwendet wird. Ausserdem soll sie einen Binnenmarkt für die grenzüberschreitende Verwendung elektronischer Signaturen (e-Signaturen) und einschlägiger Vertrauensdienste schaffen, indem sie dafür sorgt, dass diese Dienste grenzübergreifend funktionieren und den gleichen Rechtsstatus haben werden wie herkömmliche papiergestützte Verfahren. Nach Auffassung der Kommission wird erst dadurch das grosse Potenzial der elektronischen Auftragsvergabe („eBe-schaffung“) voll zum Tragen kommen. Die breite Anwendung der elektronischen Unterschrift setzt unserer Auffassung ebenfalls eine umfassende Überprüfung des gesam-	SwissH

ten Privat- und Verwaltungsrechts (Bund und Kantone) voraus, wobei die Anforderungen an die Identifizierung, Authentifizierung sowie Wahrung der Integrität zu prüfen und unter Beachtung des Gebots zu maximaler Effizienz und unter Gewährung grösstmöglicher Freiheit für die rechtsunterworfenen Unternehmen, ihre Geschäftsprozesse adäquat zu gestalten, zu regeln sind. Eine allgemeine Gesetzgebung betreffend den elektronischen Geschäftsverkehr zwischen Privaten und Behörden ("B2G") kann dabei auch Formen der elektronischen Kommunikation zulassen, welche im ZertES nicht geregelt sind, wie Zustellung durch E-Mail, Zulassung digitaler Signaturverfahren bzw. der fortgeschrittenen elektronischen Signaturen, sowie für anspruchsvolle Anwendungen die Notwendigkeit der Verwendung der geregelten bzw. der qualifizierten elektronischen Signatur. Als Grundsatz sollte gelten, dass überall dort, wo der elektronische Verkehr mit der Verwaltung möglich und zulässig ist, die Privaten einen Anspruch auf elektronische Übermittlung haben und die Behörden sowie Amtsstellen zur Bereitstellung der entsprechenden Infrastruktur (innert angemessener Übergangsfrist) verpflichtet sind. Wir erachten deshalb die Schaffung einer umfassenden Rechtsgrundlage für die effiziente und breite Anwendung digitaler Signaturverfahren im privaten und öffentlichen Bereich, wie sie der Bundesrat zu prüfen angeregt hat, als einen wichtigen Beitrag für die Förderung des Wirtschaftsstandorts Schweiz. In dieser umfassenden Regelung sollte die elektronische Signatur nach dem revidierten ZertES ihren Platz für Anwendungen erhalten, bei denen besonders hohe Anforderungen an die Sicherheit der elektronischen Kommunikation zu stellen sind.	
La législation actuelle sur la signature électronique a été critiquée dès son adoption en 2003. Les exigences fixées dans la SCSE pour qu'une signature électronique soit juridiquement équivalente à une signature manuscrite sont trop élevées pour qu'on puisse l'utiliser pour un important volume de documents. La base du problème vient du fait que les signatures électroniques sont uniquement attribuables à des personnes physiques, les personnes morales et les administrations publiques ne pouvant pas étre dotées d'un paraphe électronique juridiquement fondé. La révision proposée corrige ce problème en créant de nouvelles catégories de signatures électroniques. En tant que telle, la signature électronique qualifiée restera réservée aux personnes physiques. Toutefois, la SCSE révisée prévoit une signature électronique dite "réglementée", répondant des exigences moins strictes. Cette dernière sera ouverte aux entreprises et aux autorités. La loi prévoit encore que les produits de certification devraient à l'avenir étre utilissés pour authentifier des personnes et pas seulement pour créer des signatures électroniques. La reconnaissance des foumisseurs de services de certification restera facultative. Quant à la réglementation des produits de certification, elle restera non exhaustive et la législation suisse sera toujours conforme à la directive européenne sur les signatures. La Chambre vaudoise du commerce et de l'industrie (CVCI) salue cette extension de la loi sur la signature électronique aux entreprises et aux autorités. Les changements favoriseront le développement du commerce éiectronique, qui fonctionne actuellement sur la base d'authentifications via des certificats qui n'ont pas un caractère juridique aussi précis que la SCSE révisée leur accordera. La sécurit des échanges, et la confiance de la clientèle envers les foumisseurs de produits ou de services, en sera accrue puisque la ici validera formeliement la signature des entreprises et des autorits (sans toutefois que le degré de sécurité soit aussi élevé que paur la signature qualifiée). La cyberadministration, encore largement balbutiante à l'heure actuelle, sera également facilitée	CVCI

Die Aargauische Industrie- und Handelskammer (AIHK) unterstützt die Vereinfachung der elektronischen Signatur für juristische Personen und Behörden. Eine elektronische Signatur kann für juristische Personen eine Vereinfachung im täglichen Rechtsverkehr darstellen und für administrative Entlastung sorgen. Im Mittelpunkt sollten dabei stets folgende Punkte stehen: • Die Unterschriftenregelung soll einfach handhabbar sein; • Die Datensicherheit muss jederzeit gewährleistet werden; • Die Signatur soll für die Unternehmen kostengünstig sein; • Es sollen einheitliche Zertifikate von entsprechender Qualität ausgestellt werden. Mit diesen Grundgedanken beurteilen wir die Vorlage dem Grundsatz nach als zweckmässig, soweit wir dies in technischer Hinsicht zu beurteilen vermögen. Damit die elektronische Unterschrift aber «massengeschäftstauglich» wird, reicht eine Gesetzesänderung nach unserem Empfinden nicht aus. Vielmehr sind auch entsprechende Sensibilisierungsbestrebungen bei den Unternehmen erforderlich, die an unserem Wirtschaftsleben teilnehmen.	AIHK

Bemerkungen zu den einzelnen Bestimmungen	**Wer?**
Titel	
Der vorgeschlagene Titel ist inhaltlich durchaus treffend. Dass er einer Denksportaufgabe gleich entschlüsselt werden muss, macht ihn für einen Gesetzestitel ungeeignet. Hinzu kommt, dass der Kurztitel, der unverändert bleiben soll, einen Fokus setzt, der ausserhalb des beschränkten Regelungsgegenstandes des Gesetzes zu liegen kommt. Bereits der erläuternde Bericht, Ziff. 2.1.2., S. 9, weist sinngemäss darauf hin, dass fälschlicherweise angenommen wird, das ZertES regle die elektronische Signatur und deren Wirkung. Der Kurztitel leistet derartigen Überinterpretationen sowohl nach geltendem Recht wie auch unter dem vorgeschlagenen neuen Recht Vorschub. Dies stiftet Verwirrung und schadet der Akzeptanz des Gesetzes. Der Kurztitel lässt sich einzig im Falle einer „grossen Totalrevision“ vertreten. Bis dann sollte auf den Kurztitel verzichtet werden, auch wenn er sich eingebürgert hat. In diesem Sinne schlagen wir als erstes vor, dem Gesetz den Namen „Bundesgesetz über die Rahmenbedingungen für digitale Zertifikate staatlich anerkannter Zertifizierungsdienste“ zu geben. Als Kurztitel schlagen wir „Bundesgesetz über digitale Zertifizierungsdienste“ und als Abkürzung „DZertS“ vor.	Die Post
Artikel 1: Gegenstand und Zweck	
Der erste Artikel sollte sich auf die "Zweckumschreibung" beschränken. Der Geltungs- und Regelungsbereich sind in unmittelbar nachfolgende Artikel auszulagern. Die "geregelte Signatur" als zweiter bundesgesetzlicher Qualitätsstandard für elektronische Signaturen entspricht einem Bedürfnis von Behörden und Unternehmen, eigenständig Inhaber elektronischer Signaturen sein zu können.	Die Post
Art. 1 Abs. 1	
Bst. a: Anforderungen an Zertifikate können sinnvollerweise nur unter der Berücksichtigung des Anwendungsfalles adäquat definiert werden. Daher sollen die Anwendungen explizit aufgeführt werden. Des Weiteren ist sprachlich unklar, ob durch dieses Gesetz auch Qualitätsanforderungen an die Zertifikatsanwendungen gemacht werden sollten. Wobei diese in diesem Gesetz dann gänzlich fehlen würden. Eine mögliche alternative Formulierung könnte wie folgt lauten: a. die Anforderungen an bestimmte digitale Zertifikate in Abhängigkeit von deren Anwendung. Zu unterstützende Anwendungen sind die qualifizierte elektronische Signatur, der geregelte Dokumentenauthentizitätsnachweis und der geregelte Identitätsnachweis;	Die Post
Bst. b: Durch die Ergänzung erfährt der Begriff „Zertifizierungsdienst“ mehrere Bedeutungen, einmal im Sinne von Certificate Service Provider und einmal als Anwendung digitaler Zertifikate. Wir empfehlen, den Klammerinhalt ersatzlos zu streichen. Eventuell könnte folgende Formulierung mehr Klarheit schaffen: b. die Voraussetzungen, unter denen sich Anbieterinnen von Zertifizierungsdiensten im Bereich gesetzlich geregelter Zertifikatsanwendungen anerkennen lassen können;	Die Post

Art. 1 Abs. 2	
L'article 1 al. 2 ne définit pas les effets juridiques de la signature électronique, ce qui pourrait étre délicat.	FR
La loi ne règle pas les effets juridiques ; il serait pourtant à ce propos judicieux d'indiquer, parmi les indications figurant dans le certificat, par exemple en cas de mauvais usage d'un certificat réglementé dont une personne morale est titulaire, qui doit être contacté ou est répondant pour clarifier la situation.	GE
Die relativ geringe praktische Verbreitung der mit dem ZertES geregelten Signatur- bzw. Zertifikatstypen wird sich durch die vorgeschlagene Totalrevision des ZertES (RevE ZertES') aus folgenden Gründen aus unserer Optik vorerst kaum wesentlich ändern: Ebenfalls wird begrüsst, dass der Gesetzgeber die Verwendung elektronischer Signatu ren fördern und begünstigen will (Art. 1 Abs. 2 Bst. b RevE ZertES). Das revidierte ZertES enthält allerdings keine Bestimmungen, welche wirksam der praktischen Umsetzung dieses Ziels dienen.	ISSS
Durch diesen Absatz wird das Förderungsversprechen von Art. 1 Abs. 3 nicht eingelöst. Um e-Goverment, e-Commerce und e-Health zu fördern, schlagen wir daher vor, diesen Absatz ersatzlos zu streichen.	Die Post
Art. 1 Abs. 3	
Begrüssenswert ist, dass neu auch die sichere Authentifikation mit Produkten von Zertifizierungsdiensten gesetzlich geregelt werden soll. Aus heutiger Sicht der Informatik sind in der Umsetzung keine Hindernisse zu erwarten. Durch die Erweiterung der akzeptierten Zertifikate erhöht sich deren Zahl auf sieben. In diesem Zusammenhang ist darauf zu achten, dass die Anzahl von Zertifikaten bzw. Kategorien auch in Zukunft überschaubar und einfach handhabbar bleibt.	SZ
Artikel 2: Begriffe	
Ist es tatsächlich notwendig, vier Abstufungen bei den elektronischen Signaturen und drei Differenzierungen beiden Zertifikaten vorzusehen? Wir bitten Sie zu prüfen, ob nicht eine einfachere Regelung mit weniger Abstufungen möglich wäre, die den Zweck der Vorlage auch erfüllen würde. Ausserdem ersuchen wir Sie, ein besonderes Augenmerk auf die Koordination des Gesetzgebungsprojekts mit anderen Anstrengungen des Bundes auf dem Gebiet des elektronischen Geschäftsverkehrs zu richten. Aus dem begleitenden Bericht geht z.B. nicht hervor, welche Beziehungen und allenfalls Verschränkungen zwischen der unterbreiteten Revisionsvorlage und dem Projekt zur Umsetzung des bundesrechtlichen Notariatsregisters bestehen.	BE
Gemäss Art. 13 mit der Marginalie «Qualifizierte Zeitstempel» müssen anerkannte Anbieterinnen von Zertifizierungsdiensten auf entsprechendes Begehren hin eine mit ihrer geregelten elektronischen Signatur versehene Bescheinigung abgeben, wonach bestimmte digitale Daten zu einer bestimmten Zeit vorliegen. Der Begriff «qualifizierter Zeitstempel» sollte deshalb im Gesetz vorgängig unter Art. 2 definiert werden. Antrag: Art. 2 sei mit einem neuen Buchstaben k zu ergänzen, in welchem der Begriff des qualifizierten Zeitstempels definiert wird.	ZG
L'article 2 «Définitions » devrait étre revu car certains termes sont trop techniques pour le législateur et partiellement inexacts pour les spécialistes. il convient de rappeler que les certificats numériques ont trois usages différents : la signature électronique, l'authentification et le chiffrement. Or le chiffrement n'est pas abordé expressément dans la loi. L'ordonnance qui découlera de la loi devra quant à elle procéder à ces distinctions car des règles spécifiques sont nécessaires à chacun des trois domaines.	FR

En effet, la définition des différents types de signatures électroniques (article 2, lettres a, b, c et d) reste compliquée à comprendre. L'exposé des motifs n'est malheureusement pas très utile. En outre, les conséquences des types de signatures en fonction des bénéficiaires (personnes physiques, personnes morales, autorités) ne sont pas claires.	GE
Es fehlen Definitionen wie beispielsweise: Akteur „Zertifikatsinhaber“; Akteur „Partei, die sich auf die Angaben im Zertifikat verlässt“; Begriff „Authentifizierung“; Begriff „Identifizierung“. Diese Definitionen sollten sich so eng wie möglich an den Definitionen der Richtline 1999/93/EG bzw. an künftigen Definitionen auf europäischer Ebene orientieren.	Die Post
Art. 2 Bst. b	
Beurteilung: Ziel mit Revision erreicht. Kommentar: Die zukünftige Regelung auf Gesetzesebene gibt den rechtlichen Rahmen für die Produktanforderungen von "fortgeschrittenen digitalen Signaturen" angemessen vor. Für die Umsetzung und Klarheit auf Kontrollziel-Ebene müssen die funktionellen und technischen Anforderungen in einer Ausführungsbestimmung definiert werden.	KPMG
Art. 2 Bst. c	
De même, l'ajout d'une nouvelle forme de signature dite « réglementée » à l'usage des personnes morales et des autorités est tout autant positive dans la mesure où celle-ci répond aux différents besoins exprimés dont l'envoi de documents de masse.	VD
1. Es ist unklar, worauf sich die Formulierung „…zum Zeitpunkt der Erzeugung…“ bezieht. Aus unserer Sicht wäre die folgende Formulierung passender: „…zum Zeitpunkt der Erzeugung der geregelten elektronischen Signatur…“. 2) Unabhängig von der Formulierung impliziert Art. 2 Bst. c die Prüfung der elektronischen Signatur nach dem Gültigkeitsmodell „Kettenmodell“[1]. Es wäre wünschenswert, wenn im ZertES oder im VZertES diesbezüglich näher auf das Gültigkeitsmodell eingegangen würde. Aus unserer Sicht ist das Kettenmodell zu bevorzugen. Es stellt sicher, dass die Gültigkeit einer einmal gültigen Signatur unberührt bleibt, falls zu einem späteren Zeitpunkt das Benutzer-oder CA- Zertifikat revoziert würde.	keyon AG
Beurteilung: Ziel mit Revision wurde erreicht. Die geregelten digitalen Signaturen wurden auf Gesetzesebene mit den nötigen gesetzlichen Anforderungen geregelt. Mit den geregelten digitalen Signaturen kann neu die Authentifikation für IT-Zielsysteme und Webbasierenden Applikationen eine digitale Sicherheit innerhalb der Schweiz zur Verfügung gestellt werden.	KPMG AG
Der SAV begrüsst die vorgeschlagene Einführung der geregelten elektronischen Signatur, da dies für Behörden, Unternehmen und natürliche Personen ein Schritt in die richtige Richtung bedeutet. Dies namentlich deshalb, weil die geregelte Signatur den betriebsinternen Bewirtschaftungsaufwand der Signaturen im Vergleich zu qualifizierten Signaturen massiv vereinfacht und zudem die Beschaffungskosten (ein Unternehmenszertifikat anstelle von vielen personenbezogenen Zertifikaten) senkt. Zudem hat sich im gelebten Geschäftsalltag der Austausch von Willenserklärungen mittels (noch) unsignierten Mails durchgesetzt. Mit der Einführung der geregelten Signatur kann die Rechtssicherheit beim Austausch von elektronischen Willenserklärungen erheblich erhöht werden. Nach Ansicht des SAV muss es möglich sein, eine geregelte Signatur auch unter Verwendung eines Signaturdienstes (bspw. werden alle aus gehenden Mails des Mailservers mit der geregelten Signatur versehen) einzusetzen.	SAV

Diese Formulierung lässt Soft-Token zu, d. h. die Speicherung von Zertifikaten auf einem nicht ausschliesslich dafür bestimmten Gerät (z. B. Personal Computer, Server, Notebook, Smartphone, Mobiltelefon). Soft-Token sind für die Anwendung von SSL-Zertifikate gerechtfertigt. Ob dies auch bei Willensäusserungen und Authentizitätsnachweisen von Dokumenten sinnvoll ist, erscheint uns fraglich. Die Vertrauenswürdigkeit und Sicherheit von auf Hard-Token basierenden Lösungen (z. B. SuisseID) erscheint als wesentlich höher.	Die Post
Der SWICO begrüsst die vorgeschlagene Revision als einen ersten Schritt zur Förderung der Verbreitung von digitalen Signaturen (vgl dazu nachstehend Ziff. 3). Nachdem wir bereits im März 2001 darauf aufmerksam gemacht haben, dass aus dem Interesse der Wirtschaft an einem breit abgestützten und erfolgreichen Einsatz der digitalen Signatur, aber auch aus Gründen der internationalen Rechtsentwicklung, eine Zertifikatsvergabe auch an juristische Personen möglich sein sollte, wird nun dieses Anliegen in der vorliegenden Revision berücksichtigt. Dass sich die elektronische Signatur nicht weiter ausgebreitet hat, ist nicht zuletzt darauf zurückzuführen, dass eben keine “Killer-Applikation“ vorgelegen hat, wie es etwa die Massenverarbeitung von Rechnungen mit mehrwertsteuerrelevanten Angaben darstellen würde. Wenn dies mit der vorliegenden Revision sichergestellt werden kann, wird ein altes Anliegen des SWICO erfüllt. Eine solche Umsetzung würde aber (mindestens) seitens des EFD eine Anpassung der EIDI-V voraussetzen. Wie in den nachstehenden Bemerkungen zum Thema „Weiterführende Revision“ ausgeführt, kann unser Grundanliegen wohl nur mit einer weiter greifenden Revision schlagkräftig umgesetzt werden.	SWICO
Nachdem die Wirtschaft bereits früher darauf aufmerksam gemacht hatte, dass aus dem Interesse der Wirtschaft an einem breit abgestützten und erfolgreichen Einsatz der digitalen Signatur, aber auch aus Gründen der internationalen Rechtsentwicklung (namentlich derjenigen in der EU), eine Zertifikatsvergabe auch an juristische Personen möglich sein sollte, wird nun dieses Anliegen in der vorliegenden Revision berücksichtigt. Dass sich die elektronische Signatur nicht weiter ausgebreitet hat, ist nicht zuletzt darauf zurückzuführen, dass sich unter dem aktuellen Gesetzesrahmen eben kaum konkret nutzbringende Anwendungsfälle eröffnet haben, wie es etwa die flächendeckende Massenverarbeitung von elektronischen Rechnungen, mit oder ohne mehrwertsteuerrelevanten Angaben, darstellen könnte. Eine solche Umsetzung wird die formelle und zum Teil auch materielle Anpassung einer grösseren Zahl von weiteren Erlassen, wie etwa eine Anpassung der ElDI-V durch das EFD, voraussetzen. Wie in den nachstehenden Bemerkungen zum Thema „Weiterführende Revision“ ausgeführt, kann unser Grundanliegen wohl nur mit einer weiter greifenden Revision schlagkräftig umgesetzt werden.	SwissH
Art. 2 Bst. d	
Siehe Anmerkungen bei Art. 2 Bst.c	keyon AG
Durch den expliziten Wegfall der sicheren Signatureinheit können auch Soft-Token für qualifizierte elektronische Unterschriften verwendet werden. Dies ist eine klare Schwächung bezüglich Sicherheit der qualifizierten elektronischen Unterschrift zur heutigen Situation. Folgende mögliche Formulierung könnte dem abhelfen: d. qualifizierte elektronische Signatur: eine geregelte elektronische Signatur, die auf einer sicheren Signaturerstellungseinheit nach Artikel 6 und auf einem qualifizierten und zum Zeitpunkt der Erzeugung gültigen Zertifikat beruht;	Die Post
Zur Löschung des alten Art. 2 lit. d Diese Vereinfachung ist nachvollziehbar.	Die Post

Art. 2 Bst. e (alt)	
Zur Löschung des alten Art. 2 lit. e Diese Vereinfachung ist nachvollziehbar.	Die Post
Art. 2 Bst. f	
Anbieter von Zertifizierungsdienste verlieren die Wahlfreiheit bezüglich Anerkennung. Aktuell gibt es nur eine Anerkennungsstelle. Um die Qualität zu gewährleisten wäre es sinnvoll, mehrere zu haben, respektive die Wahlfreiheit zu behalten. So wird im Bereich Revisionen/Buchprüfung die Forderung diskutiert, alle zehn Jahre die Revisionsstelle zu wechseln.	Die Post
Art. 2 Bst. g	
Définition du certificat qualifié. Pour une meilleure compréhension par les administrés du texte légal, il conviendrait d'ajouter à la définition proposée : « La notion de certificat réglementé inclut par défaut celle de certificat qualifié. » En effet, pour ne prendre qu'un exemple, il n'est pas évident de comprendre que l'article 11 SCSE, qui se rapporte à l'annulation des certificats réglementés, concerne aussi par définition celle des certificats qualifiés.	GE
Siehe Bemerkung zum geregelten Zertifikat Art. 2 lit. f.	Die Post
Art. 2 Bst. i	
Um die bestehende qualifizierte elektronische Signatur von der neu zu schaffenden, leicht vereinfachten Signatur zu unterscheiden, wird für Letztere der Begriff «geregelte elektronische Signatur» verwendet. Wir erachten den Begriff «geregelt» in diesem Zusammenhang als wenig geglückt, denn «geregelt» können auch Signaturen sein, die nicht vom ZertES erfasst werden. Das Gleiche gilt für die Begriffe «geregeltes Zertifikat» und «digitales Zertifikat». Sinnvoller erscheinen uns etwa folgende Bezeichnungen: «ZertES-Signatur» bzw. «qualifizierte ZertESSignatur» und «ZertES-Zertifikat» bzw. «qualifiziertes ZertES-Zertifikat». Dies vereinfacht die Begriffe und grenzt die ZertES-Signaturen und -Zertifikate eindeutig von Signaturen und Zertifikaten ab, die gesetzlich nicht geregelt sind. Die Begriffe «kryptografischer Schlüssel» und «qualifizierter Zeitstempel» sind in Art. 2 nicht definiert. Wir schlagen vor, beide Begriffe in Art. 2 aufzunehmen.	ZH
Die Prüfung der obligatorischen Integration eines Zeitstempels in eine qualifizierte elektronischen Signatur begrüssen wir. Ihr Vorschlag, dieses Anliegen auf dem Wege einer Revision des DR zu verwirklichen, erscheint uns denn auch zielführend. Wenn die Anpassung des OR aber nicht realisiert werden kann, sollte im ZertES festgelegt werden, dass zu einer qualifizierten elektronischen Signatur per Definitionem zwingend der Zeitstempel einer anerkannten Anbieterin von Zertifizierungsdiensten gehört.	BE
Artikel 3: Anerkennung der Anbieterinnen von Zertifizierungsdiensten	
Wir regen aber an bei den Anerkennungsvoraussetzungen für Anbieterinnen von Zertifizierungsdiensten in Artikel 3 als zusätzliches Kriterium die Prüfung der Integrität des Personals aufzunehmen. Der Missbrauch von sensiblen persönlichen Daten ist zu verhindern. Durch eine Integritätsprüfung soll die Vertrauenswürdig keit der Anbieterin selbst wie auch ihres Personals zusätzlich geprüft und dadurch gestärkt werden.	GL

Reconnaissance des fournisseurs. Le point 2.1.3 du rapport explicatif nous apprend qu'il n'est retenu qu'un seul type de reconnaissance s'appliquant aux deux types de certificats. Il ne précise toutefois pas dans quelle mesure l'introduction du certificat réglementé impliquera une reconnaissance complémentaire portant sur les informations nouvellement introduites dans le certificat réglementé, alors que : 1) au niveau procédural, cette introduction de nouvelles informations contenues dans le nouveau certificat (telles que le numéro unique d'identification des entreprises - IDE) induit nécessairement une amplification de la liste des éléments à contrôler, et donc de la capacité du fournisseur à vérifier ces conditions applicables; 2) au niveau technique, il faut introduire ces nouveaux éléments dans le certificat, et donc vérifier la capacité technique du fournisseur à le faire.	GE
Art. 3 Abs. 3	
Grundsätzlich begrüssen wir die in Art. 3 Abs. 3 des Gesetzesentwurfes klar formulierte Absicht, ein breites Angebot an sicheren Zertifizierungsdiensten zu fördern und die Verwendung digitaler Zertifikate und von elektronischen Signaturen zu vereinfachen, um sie einem breiteren Kreis von Anwendern zugänglich zu machen.	NW
3. Abschnitt: Generierung, Speicherung und Anwendung kryptografischer Schlüssel	
Begründung: Im Titel des Gesetzes sowie in Art. 1 Abs. 1 lit. a und b ist von „Anwendungen“ elektronischer Zertifikate die Rede, wobei jeweils klar ist, dass es sich bei elektronischen Signaturen um eine dieser möglichen Anwendungen handelt. Ein andere ist der Einsatz von elektronischen Zertifikaten für die Authentifizierung, wie sich insbesondere aus dem Begleitberichtergibt. Der Begriff „Anwendung“ kann jedoch zu Missverständnissen führen, die insbesondere im Zusammenhang mit Art. 6 vermieden werden sollte. Hier ist nämlich nicht die Rede von Anwendungen digitaler Zertifikate, sondern von der Anwendung kryptographischer Schlüssel. Das ZertES soll auch nach der vorgeschlagenen Totalrevision auf die Regelung der Zertifizierungsdienste für die Erzeugung kryptografischer Schlüssel und die Ausgabe von Zertifikaten durch die Anbieter von Zertifizierungsdiensten (“ZDA“) sowie die damit verbundenen Rechte und Pflichten der ZDA beschränkt bleiben. Die im ZertES aufgestellten Anforderungen an die Erstellung und Ausgabe digitaler Zertifikate schaffen zwar die Grundlage für die sichere elektronische Kommunikation und Information. Darüber hinaus werden jedoch auch auf Seiten der Betreiber von Anwendungen, in deren Zusammenhang digitale Zertifikate zum Einsatz gelangen (z.B. e-Banking-Lösungen, Zustellplattformen, Lösungen für die elektronische Abstimmung etc.), Massnahmen zur Schaffung einer sicheren Infrastruktur vorausgesetzt. Diese anwendungsseitig zu treffenden Massnahmen sind auch nach dessen Totalrevision nicht Gegenstand des ZertES. Es wird daher empfohlen, im Zusammenhang mit Art. 6 zur Vermeidung von möglichen Missverständnissen nicht von der Anwendung, sondern von der “Verwendung“ von kryptographischen Schlüsseln zu sprechen.	ISSS

Artikel 6	
Art. 6 Abs. 1	
Der Bundesrat soll nur die Schlüsselgenerierung der „geregelten Zertifikate“ regeln. Diese Formulierung impliziert, dass die Schlüsselgenerierung für qualifizierte Zertifikate analog erfolgen soll wie für geregelte Zertifikate. Dieser Sachverhalt entspräche auch der neuen Kaskade gem. Kapitel 1.3.1 der Erläuterungen. Wir erachten diese Formulierung als problematisch, da sie dem Bundesrat nicht die Kompetenz gibt, die Schlüsselgenerierung spezifisch für qualifizierte Zertifikate zu regeln. Wir gehen davon aus, dass in den künftigen VZertES und TAV ZertES die Anforderungen an die Schlüsselgenerierung sowie an die SSCD für geregelte Zertifikate analog formuliert sein wird wie bisher für qualifizierte Zertifikate. Dies impliziert eine entsprechend CC, FIPS oder IT-SEC zertifizierte SSCD. Wir gehen weiter davon aus, dass künftig beispielsweise die SuisseID nicht nur ein qualifiziertes Zertifikat, sondern auch ein geregeltes Zertifikat anbieten soll. Wir möchten darauf hinweisen, dass auf den aktuell verfügbaren SSCDs der SuisseID die Anforderung von Art. 6 Abs. 1 nicht erfüllt werden könnte, da der Bereich, in welchem die Schlüsselpaare der geregelten Zertifikate generiert und gespeichert würden, nicht CC, FIPS oder IT-SEC zertifiziert sind[2]. Mit einer Formulierung „Der Bundesrat regelt die Generierung kryptografischer Schlüssel, für die geregelte oder qualifizierte Zertifikate im Sinne…“ wäre klar, dass diesbezüglich unterschieden werden könnte. Hinweis: Wir sind der Meinung, dass die Anforderungen an die SSCD's für geregelte Zertifikate analog sein sollten wir für qualifizierte Zertifikate. Allfällige Diskussionen im Zusammenhang mit den künftigen Eigenschaften der SuisseID sowie den entsprechenden Möglichkeiten sollten allerdings berücksichtigt werden.	keyon
Art. 6 Abs. 2	
L‘article 6 al. 2 lettre a) est totalement inapproprié. “Garantir {...] que les clefs ne puissent se rencontrer qu‘une seule fois“ ne précise pas s‘ii s‘agit de clefs privées (uniques) ou de clefs publiques (diffusés largement, donc en contradiction avec le texte de loi). “Garantir que leur confidentiaité soit suffisamment garantie“ est pour le moins hypothétique et encore une fois il n‘est pas précis s‘il s‘agit de clefs privées ou publiques.	FR
L‘article 6, alina 2, lettre a, de l'avant-projet, relatif aux clefs cryptographiques, mérite selon nous d‘étre revu. Il prévoit qu‘il doit étre garanti que “les clefs ne puissent, pratiquement, se rencontrer qu‘une seule fois et que leur confidentialité soit suffisamment garantie“. Le mot “pratiquement“ ne parait pas utile. En outre, le contenu de cette disposition n‘est pas applicable aux clefs dites “publiques“, qui sont diffusées largement et par essence dupliquées. Quant aux clefs privées, Il est effectivement souhaitable qu‘elles ne puissent se rencontrer qu‘une seule fois s‘agissant de la signature électronique, mais ii sagit d‘une exigence qui n‘est pas applicable, par exemple, dans le cadre de la sécurisation de sites Internet dans la mesure ou de nombreux systèmes informatiques procèdent actuellement à la duplication des clefs privées également. La disposition devrait par conséquent étre rédigée différemment.	JU

Die Formulierung „praktisch nur einmal auftreten“ sollte präzisiert werden. Im aktuellen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt[4], Anhang II, ist eine Sicherung des Schlüsselmaterials vorgesehen. 4. Qualifizierte Vertrauensdienstanbieter, die elektronische Signaturerstellungsdaten im Namen des Unterzeichners verwalten, können die elektronischen Signaturerstellungsdaten zu Sicherungszwecken kopierenm sofern folgende Anforderungen erfüllt sind, a) die kopierten Datensätze müssen das gleiche Sicherheitsniveau wie die Original-Datensätze aufweisen; b) es dürfen nicht mehr kopierte Datensätze vorhanden sein als zur Gewährleistung der Dienstleistungskontinuität unbedingt nötig Die Sicherung des Schlüsselmaterials ist vor allem bei Unternehmenssignaturen oder bei qualifizierten Signaturen, die auf zentralen Signaturservern ausgeführt werden, von essentieller Bedeutung. Wir würden es begrüssen, wenn die Formulierung in Art. 6 Abs. 2 Bst. a eine aktuelle oder künftige Sicherung des Schlüsselmaterials nicht verhindern würde.	keyon AG
Infolge der Begriffsdefinition können Zertifikate auch Soft-Token sein, d. h. der Einsatz von sicheren Signaturerstellungseinheiten für QC sind nicht mehr zwingend.	Die Post
Art. 6 Abs. 3	
1 Der Bundesrat regelt (unverändert) 2 Bei Systemen zur Generierung, Speicherung und ~~Anwendung~~ Verwendung geheimer kryptografischer Schlüssel, insbesondere bei Signaturerstellungseinheiten, zumindest gewährleistet ist, dass die erzeugten Schlüssel: a. (unverändert) b. mit hinreichender Sicherheit nicht abgeleitet werden können und ihre ~~Anwendung~~Verwendung bei ~~Verwendung~~Einsatz der jeweils verfügbaren Technologie vor Fälschungen geschützt ist; c. von der rechtmässigen Inhaberin oder vom rechtmässigen Inhaber, soweit es die jeweils verfügbare Technologie erlaubt, vor der missbräuchlichen Verwendung durch andere verlässlich geschützt werden können. Begründung Absatz 2 und Unterabsatz b: Es kann auf das oben zum Titel des 3. Abschnitts verwiesen werden. Unterabsatz c: Der Anwendungsbereich kryptografischer Schlüssel und digitaler Zertifikate ist bekanntlich weit offen. Die Anbieter von Zertifizierungsdiensten sind daher nur insoweit zu Massnahmen für die Sicherung kryptografischer Schlüssel und digitaler Zertifikate gegen missbräuchliche Verwendung durch Dritte zu verpflichten, als es die jeweils verfügbare Technologie erlaubt.	ISSS
Obwohl die entsprechenden Bemerkungen in den Erläuterungen nachvollziehbar erscheinen, erachten wir das Argument der Nichtdurchsetzbarkeit als nicht stichhaltig. So erscheint es uns als wichtig, • dass die Rechte und Pflichten aller Akteure geregelt werden, um entsprechende Transparenz und Rechtssicherheit zu schaffen, und • dass Regelungen bezüglich Zertifikatsformate mit der Praxis der auf dem Weltmarkt üblichen Anbieter verträglich sind. So waren in den Anfangszeiten des ZertES die Vorgaben im Wiederspruch zu diesen Anforderungen. Zusätzlich gab es Anbieter, deren Zertifikate in PDF Viewern als nicht vertrauenswürdig gekennzeichnet wurden.	Die Post

4. Abschnitt: Geregelte Zertifikate	
Remplacer « Certificats réglementés » par « Certificats réglementés et certificats qualifiés »	GE
2. Dieser Fokus ist zu eng und wird den vielfältigen Anwendungen von digitalen Zertifikaten wie z.B. Massensignatur von elektronischen Dokumenten, Code Signatur und Authentisierung eines Partners im elektronischen Geschäftsverkehr nicht gerecht. Zu Recht geht deshalb die Neufassung des ZertES davon aus, dass in der Praxis den jeweiligen Anwendungen entsprechend verschiedene Zertifikatsklassen eingesetzt werden. Im neuen Gesetz werden deshalb zwei Zertifikatsklassen gesetzlich geregelt, nämlich: a) Das qualifizierte Zertifikat wie bisher für die qualifizierte Signatur äquivalent zur persönlichen eigenhändigen Unterschrift gemäss OR 14; b) Das geregelte Zertifikat, offen für vielfältige heutige und künftige Anwendungen im automatischen oder Personengebundenen elektronischen Verkehr, sowohl für elektronische Signatur als auch für Authentisierung von Geschäftspartnern. Mit den entsprechenden Regelungen der Haftung wird die nötige Rechtssicherheit bei der Ausstellung und Verwendung dieser beiden Zertifikate geschaffen. 3. Damit folgt der Gesetzgeber nunmehr dem Standard „eCH-0048 PKI-Zertifikatsklassen“ (2006; rev. 2012) des Vereins eCH für eGovernment Standards. Zweck des Standards ist (Zitat): Wesentliche Grundlage zur Realisierung verbindlicher und vertrauenswürdiger eGovernment Geschäftsprozesse ist die verlässliche Identifikation der beteiligten Partner. Als internationaler Standard hat sich in diesem Kontext der Einsatz von elektronischen Signaturen mittels X.509 Zertifikaten etabliert. Diesem technischen Standard ist zusätzlich ein organisatorisches und juristisches Regelwerk an die Seite zu stellen, damit die eindeutige Zuordnung von Dokumenten, Willenserklärungen, etc. zu ihren Urhebern in Form digitaler Signaturen sichergestellt werden kann und mit den von allen Beteiligten gewünschten Rechtsfolgen verbunden ist. Das Einsatzgebiet von X.509 Zertifikaten ist nicht nur auf die Signatur von elektronischen Dokumenten beschränkt. Es umfasst weiterhin die Authentifizierung, Code-Signaturen, Verschlüsselung und weitere. Der vorliegende eCH-Standard adressiert sämtliche Einsatzbereiche. Das notwendige Know-How für die Neufassung der Verordnung und der Technischen und Administrativen Vorschriften ist bei eCH vorhanden und kann in Anspruch genommen werden.	CI AG
Artikel 7: Anforderungen an alle geregelte Zertifikate	
Als Ergänzung zur bisherigen qualifizierten elektronischen Signatur, die nur natürlichen Personen zugänglich ist, soll eine weitere Form der elektronischen Signatur definiert werden, die zusätzlich auch von juristischen Personen und Behörden genutzt werden kann. Aus Informatiksicht ist diese Erweiterung der Zertifizierung auf juristische Personen und Unternehmen zu begrüssen, vor allem weil damit auch der Einsatz einer elektronischen Signatur im Massengeschäft möglich wird.	SZ
Der Regierungsrat des Kantons Aargau begrüsst die Zielsetzung der vorliegenden Gesetzesrevision, die Anforderungen für die Anerkennung elektronischer Signaturen im Hinblick auf deren Verbreitung und im Vergleich zur eigenhändigen Unterschrift alltagstauglicher zu machen. Die Einführung der geregelten elektronischen Signatur für juristische Personen und Behörden unter Verwendung des Unternehmens- und Behördenzertifikats deckt weitere Anforderungen ab und eröffnet weitere Nutzungsmöglichkeiten, die mit der bisherigen Regelung nicht oder nur in kombiniertem Einsatz vorliegen. So ist beispielsweise im Zusammenhang	AG

mit der rechtsverbindlichen elektronischen Veröffentlichung amtlicher Publikationen die Erfahrung gemacht worden, dass die Behörden die heute geltende, grundsätzlich nur ad personamnutzbare elektronische Signatur lediglich mit Umgehungslösungen nutzen können. Die neue Regelung führt diesbezüglich zu einer wesentlichen Erleichterung. Ebenfalls kann die Einsatzmöglichkeit des elektronischen Rechtverkehrs durch eine elektronische Unternehmens- und Behördenunterschrift erweitert werden. Hinsichtlich des Zeitstempels ist zu bemerken, dass aus unserer Sicht ein Obligatorium weder in technischer noch in anderweitiger Hinsicht gegenüber der fakultativen Anwendung Erschwernisse beinhaltet.	
Art. 7 ZertES bezieht sich auf die Definition der UID-Einheiten gemäss Art. 3 Abs. 1 Bst. c des Bundesgesetzes über die Unternehmens-Identifikationsnummer (UIDG; SR 431 .02). Die Definition der UID-Stellen ist jedoch noch nicht abschliessend geregelt. So gibt im Bereich der juristischen Personen vor allem die Tatsache, dass Betriebsstätten keine UID erhalten sollen, Anlass zu Diskussion. Erhalten Betriebsstätten keine UID, ist die UID-Nummer für diverse staatliche Stellen wie z.B. die Steuerverwaltung unattraktiv. Andererseits werden UID-Nummern an Personenkreise vergeben, für welche der Einsatz der neuen, dreizehnste(ligen AHV-Nummer genügen würde, so etwa im Bereich Landwirtschaft (A-Control).	TG
Voraussehbare Auswirkungen der vorgeschlagenen ZertES-Totalrevision: Die relativ geringe praktische Verbreitung der mit dem ZertES geregelten Signatur- bzw. Zertifikatstypen wird sich durch die vorgeschlagene Totalrevision des ZertES (RevE ZertES‘) aus folgenden Gründen aus unserer Optik vorerst kaum wesentlich ändern: a. Zwar wird das Konzept der Schaffung einer “geregelten elektronischen Signatur“ für UID-Einheiten ausdrücklich begrüsst. Der Erwerb geregelter Signaturen bzw. Zertifikate ist allerdings faktisch - unabhängig von der konkreten Anwendung - weitestgehend an die gleichen Voraussetzungen geknüpft, wie sie bisher für qualifizierte elektronische Signaturen Geltung haben.	ISSS
Hervorzuheben ist im Entwurf der Neufassung (Art. 7 und Art. 13): a) Das geregelte Zertifikat kann auf natürliche Personen UND auf UID-Einheiten (juristische Personen, Personengesellschaften, einfache Gesellschaften, etc. gem. UIDG vom 18.6.2010, welche mit einer Unternehmens-Identifikationsnummer UID identifiziert sind) ausgestellt werden. b) Das geregelte Zertifikat kann zudem enthalten: „spezifische Attribute der Inhaberin oder des Inhabers des zugehörigen geheimen kryptografischen Schlüssels, beispielsweise berufliche Qualifikationen;“ sowie bei natürlichen Personen den Hinweis, „dass sie zur Vertretung einer bestimmten Person oder UID-Einheit berechtigt ist;“	CI AG
Art. 7 Abs. 1	
Es wird begrüsst, dass sich neu auch UID-Einheiten zertifizieren können. Im Zusammenhang mit der Zertifizierung von UID-Einheiten ist aber auf Folgendes hinzuweisen: Auch Privatpersonen können UID-Einheiten sein. Deshalb ist darauf zu achten, dass klare Unterscheidungen zwischen UID und anderen Nummerierungssystemen für Privatpersonen (z. B. SuisseID-Nr.) möglich sind. Ferner gibt es gemäss eCH-Standard UID auch einen provisorischen Status einer UID. Hier stellt sich die Frage, ob auch bereits bei provisorischer UID ein geregeltes Zertifikat ausgestellt werden kann oder erst bei der definitiven. Zudem ist es notwendig, dass die Interoperabilität mit bestehenden Identifikatorsystemen zur Identifikation von Zertifikatshaltern gewährleistet wird.	ZH

Wie in den Erläuterungen korrekt dargelegt, werden Vereine und Stiftungen ohne Mehrwertsteuerpflicht, Handelsregistereintrag und AHV-Beitragspflicht, nicht erfasst. Es besteht die Gefahr, dass beim zukünftigen Gesetz über die Anwendung von Zertifikate, diese Gruppe zum Einsatz von geregelten Zertifikaten gedrängt wird, ohne dass Sie diese beziehen darf. Es erscheint uns aus gesellschaftlicher Sicht unschön, wenn legale juristische Personen, wie Dorfvereine etc. nur aus Gründen der Einfachheit ausgeschlossen werden. Unsere Erfahrung zeigt, dass diese öfters nach entsprechenden qualitativ hochstehenden Zertifikaten nachfragen. Sollte der Bundesrat seine neue Kompetenz wahrnehmen und EV SSL Zertifikate als geregelte bezeichnen, dürfen diese nicht mehr an diese Gruppe ausgestellt werden.	Die Post
Bst. g: Es ist nicht ersichtlich, warum diese Anforderung wegfällt, insbesondere weil durch diesen Wegfall für den Signaturprüfer nicht mehr ersichtlich ist, wer die Anerkennung durchgeführt hat.	Die Post
Art. 7 Abs. 2	
Art. 7 Abs. 2 Bst. a des geltenden ZertES beschränkt die Hinweise in Zertifikaten auf die Vertretung von juristischen Personen. Diese Einschränkung scheint nun (ohne nähere Begründung) weggefallen zu sein («zur Vertretung einer bestimmten Person oder UID-Einheit berechtigt»). Bei juristischen Personen ist die Vertretungsmacht durch das Handelsregister und den Zweck begrenzt. Bei natürlichen Personen fehlt diese Beschränkung. Die Möglichkeit, auf einer ZertES-Signatur die Vertretung für eine natürliche Person zu verewigen, geht deshalb zu weit. Die (korrekte) Einschränkung auf juristische Personen sollte im geltenden ZertES beibehalten werden.	ZH
Mit dem zusätzlichen Signaturtypus der geregelten elektronischen Signatur und dem gere gelten Zertifikat wird eine wichtige Voraussetzung für die Erleichterung von Geschäftsvorgängen zwischen Unternehmen sowie für die Förderung eines elektronischen Behörden verkehrs geschaffen. Dass die mit dem ZertES 2003 eingeführten Verfahren aus Gründen der Rechtssicherheit nicht gestrichen, sondern ergänzt werden sollen, ist nachvollziehbar. Dadurch wurde aber ein verhältnismässig komplexes Angebot realisiert, das einer terminologischen Vereinfachung teilweise entgegensteht. Auch der Grundfehler, dass die elektronischen Identitätsausweise (digitale Signaturen) für die Authentisierung von Personen von mehreren privaten Anbietern und in der Folge mit unterschiedlichen Produkten ausgestellt werden, statt wie die herkömmlichen Identitätsausweise durch staatliche Stellen wie Einwohnerkontrollen und Passbüros, wird nicht korrigiert.	BS
Contenu du certificat : remplacer « le nom » par « le nom ou la raison sociale », vu qu'une personne morale peut devenir à présent directement titulaire d'une clef. « lorsqu'il existe un risque de confusion » : il existe toujours un risque de confusion, par exemple de type homonymie entre titulaires. Par conséquent, l'ajout d'un élément distinctif invariant de type date de naissance doit être systématique.	GE

Art. 7 Abs. 3	
Valeur limite des transactions pour lesquelles le certificat est prévu : cette valeur doit être associée à une monnaie donnée et reste fluctuante, en fonction du cours de la monnaie de référence. Plafond délicat à manier.	GE
L'article 7, alinéa 3, lettre c, de l'avant-projet, relatif au certificat réglementé, prévoit que l'indication du domaine d'utilisation du certificat est facultative. A notre sens, cette indication devrait être obligatoire au vu de son importance pratique, et figurer dans l'alinéa 2.	JU
Die Formulierung „den Wert der Transaktionen…" sollte präzisiert werden. Es ist unklar, worauf sich der „Wert der Transaktionen" bezieht. 1) Bezug des Werts auf jede einzelne Transaktion 2) Bezug des Werts auf alle Transaktionen, die innerhalb der Gültigkeit des Zertifikats abgewickelt werden	keyon AG
Artikel 8: Anforderungen an qualifizierte Zertifikate	
Das qualifizierte ZertES-Zertifikat unterscheidet sich vom geregelten ZertES-Zertifikat einzig durch: (1) die Beschränkung auf natürliche Personen; (2) die Verwendung nur für die elektronische Signatur. Die Erklärung zur zweiten Einschränkung im erläuternden Bericht ist dürftig. Sie lautet «Nichttechnische Kreise haben sich immer daran gestört, dass eine so wichtige Einschränkung, die sich offenbar aus technischen Gründen aufdrängt und daher vorerst nur einmal Technikern plausibel erscheint, nicht ausdrücklich im Gesetz aufgeführt ist.» Interessant wäre es zu erfahren, warum sich diese Einschränkung aus technischen Gründen aufdrängt. Sinn und Zweck der beiden Stufen sind so jedenfalls nicht klar voneinander abgegrenzt. Es ist demnach entweder eingehend und verständlich zu begründen, weshalb die Unterscheidung vorzunehmen ist, oder aber es ist auf sie ganz zu verzichten.	ZH
Bisher wurden qualifizierte Personenzertifikate qualifiziert signiert von Anbieterinnen der Zertifizierungsdienste (siehe Art. 4 Abs. 2 VZertES). Neu werden qualifizierte Personenzertifikate geregelt signiert von Anbieterinnen der Zertifizierungsdienste. Dies wäre grundsätzlich konsistent bez. der Ausstellung von qualifizierten Zertifikaten an juristische Personen[5], könnte aber problematisch sein bez. der internationalen Nutzung von qualifizierten Zertifikaten nach ZertES, da international die „geregelten Zertifikate" unseres Wissens nach nicht bekannt sind.	keyon AG
Eine Änderung des Titels auf „Zusätzliche Anforderungen an qualifizierte Zertifikate" würde die Lesbarkeit und Verständlichkeit erhöhen.	Die Post
Gemäss dem erläuternden Bericht enthält Art. 7 (geregelte Zertifikat) die bisherigen Anforderungen an das qualifizierte Zertifikat. Der neue Art. 8 enthält für das qualifizierte Zertifikat zusätzliche Anforderungen. So wie ich den Bericht verstehe, müsste das qualifizierte Zertifikat grundsätzlich die gleichen Anforderungen erfüllen wie das geregelte Zertifikat. Falls dies der Fall ist, müsste Art. 8 zum besseren Verständnis einen Hinweis dahingehend enthalten, dass die Anforderungen des Art. 7 soweit dies Sinn macht auch für das qualifizierte Zertifikat gelten sollen. Abs. 2: Die Klarstellung, dass ein qualifiziertes Zertifikat nur für die elektronische Signatur verwendet werden darf, ist zu begrüssen.	VSUD

Art. 8 Abs. 2	
Die neue Angabe in Art. 8 Abs. 2, wonach das qualifizierte Zertifikat nur für die elektronische Signatur verwendet werden darf, erhöht nach unserem Dafürhalten die Sicherheit dieses Zertifikats und ist eine wichtige Ergänzung. Wir schlagen daher vor, diese Anforderung auch obligatorisch in der Erweiterung „Key Usage“ unterzubringen. Ferner machen wir Sie darauf aufmerksam, dass der unterbreitete Gesetzesentwurf in Art. 8 Abs. 3 versehentlich auf Art. 7 Abs. 1 Bst. b statt auf Art. 7 Abs. 2 Bst. b verweist.	BE
Art. 8 Abs. 3	
Dieser Absatz enthält eine falsche Verweisung auf Art. 7 Abs. 1 lit. b. Korrekt ist die Verweisung auf Art. 7 Abs. 2 lit. b.	ZH
Abschliessend gestatten wir uns noch, auf ein redaktionelles Versehen in Artikel 8 Absatz 3 des Revisionsentwurfs hinzuweisen. Dort muss es richtigerweise "gemäss Artikel 7 Absatz 2? Buchstabe b" heissen.	BL
Nous formulons pour le surplus deux remarques de forme: - à l‘article 8, alinéa 3, de l'avant-projet, ii convient de renvoyer l‘article 7, aiinéa 2, lettre b;	JU
Artikel 9: Ausstellung geregelter Zertifikate	
1 Die anerkannten Anbieterinnen (unverändert) a. (unverändert) b. (unverändert) c. Der Antrag für UID-Einheiten, welche im Handelsregister eingetragen sind, kann schriftlich durch den oder die eingetragenen Zeichnungsberechtigten gestellt werden. (Absätze 2 — 6 unverändert) Begründung: Mit dem Handelsregister verfügen wir über ein Instrument zur Legitimation der Vertretungs macht für juristische Personen, welche die persönliche Überbringung des Antrages durch eine natürliche Person (in der Praxis wäre dies eine Hilfsperson aus dem Sekretariat) über flüssig machen. Der Vorschlag dient der Vereinfachung des Erwerbs geregelter Zertifikate durch die im Handelsregister unter Eingabe der Vertretungsberechtigung eingetragenen UID-Einheiten und damit der Förderung der Verwendung digitaler Zertifikate und elektronischer Signaturen gemäss der Zielsetzung von Art. 1 Abs. 3 Bst. b RevE ZertES.	ISSS
Art. 9 Abs. 1	
Der Aufwand für das persönliche Erscheinen steht nicht im Einklang mit der Abschwächung der Anforderungen an die Schlüsselverwaltung (Soft-Token anstelle von Hard-Token). Sofern wieder die höheren Sicherheitsanforderungen aufgenommen werden, erscheint uns diese Anforderung als gerechtfertigt.	Die Post
Art. 9 Abs. 1 Bst. b	
Der Aufwand für das persönliche Erscheinen steht nicht im Einklang mit der Abschwächung der Anforderungen an die Schlüsselverwaltung (Soft-Token anstelle von Hard-Token). Die Forderung nach persönlichem Erscheinen macht nur Sinn, wenn der entsprechende Anwendungskontext berücksichtigt wird.	Die Post
Aufgrund der vorgängig dargelegten Ausdehnung der geregelten Zertifikate auf weitere Identifikationsmerkmale, empfehlen wir die Streichung der Formulierung „persönlich erscheinen“. a. bei natürlichen Personen: dass sie (persönlich erscheinen und) den Nachweis ihrer Identität erbringen; Das persönliche Erscheinen von Firmenvertretern sollte sowohl für die Erstabgabe wie auch für die Verlängerung von Zertifikaten nicht nötig sein. Ein mit geregelter Signatur von im HR eingetragenen Vertretern unterschriebener Zertifikatsantrag ist ausreichend.	Swisscom

b. bei UID-Einheiten, die nicht natürliche Personen sind: dass [...] oder derAntrag gemäss Vertretungsbefugnis des Unternehmens qualfiziert elektronisch unterschrieben ist Die zulässigen Attribute für berufsbezogene oder sonstige Angaben zur Person müssen definiert und die zuständigen Stellen, die diese Angaben bestätigen können, müssen klar festgelegt werden, damit eine verlässliche, gleichbleibende Qualität der Angaben zwischen den nach ZertES anerkannte Anbieterin von Zertifizierungsdiensten gewährleistet bleibt. Die Akkreditierungsstelle (Variante: Der Bundesrat) erstellt eine Liste möglichen Attribute bezeichnet die zur Angaben berechtigten Stellen. Wie oben dargelegt, sollte für geregelte Zertifikate kein persönliches Erscheinen notwendig sei. Er kann vorsehen, dass unter bestimmten Voraussetzungen auch für qualfizierte Zertfikate auf das persönliche Erscheinen [...] verzichtet wird. Zudem wäre es wünschenswert, wenn die Voraussetzungen, bei welchen auf persönliches Erscheinen auch beim qualifizierten Zertifikat verzichtet werden kann, zeitnah bestimmt werden.	
Gemäss dem erläuternden Bericht soll Buchstabe a) des Absatzes 1 sowohl natürliche Personen als auch UID-Einheiten, die natürliche Personen sind, umfassen. Zum besseren Verständnis würde ich daher vorschlagen, dies unter Buchstabe a) einzufügen, so dass es heisst,, bei natürlichen Personen und bei natürlichen Personen, die gleichzeitig UID-Einheiten sind . Art. 9 Abs. 1 verweist nur auf natürliche Personen und auf UID-Einheiten, die nicht natürliche Personen sind (Buchstabe b)).	VSUD
Artikel 10: Informations- und Dokumentationspflicht	
Im Rahmen der Dokumentationspflicht wäre es nach meiner Ansicht ratsam zu regeln, dass der Anbieter die ausgestellten Zertifikate so zu dokumentieren hat, dass die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind. Die Dokumentation sollte so erfolgen, dass sich nachträglich nicht unbemerkt verändert werden kann. Dies könnte hier das Risiko einer nachträglichen Verfälschung minimieren.	VSUD
Artikel 11: Ungültigkeitserklärung geregelter Zertifikate	
Annulation des certificats réglementés : concernant les cas d'annulation lorsque les renseignements concernant le titulaire du certificat (personne physique ou morale) changent et ne sont plus exacts, il convient de préciser de quel délai le titulaire dispose pour avertir le fournisseur ; l'immédiateté imposée ne s'applique en effet qu'au fournisseur, qui n'a pas une connaissance directe du changement, contrairement au titulaire (exemple : changement de nom).	GE
Die Formulierung sollte so erweitert werden, dass eine im Zertifikat genannte Organisation ebenfalls die Möglichkeit oder gar die Pflicht hat, ein Zertifikat zu wiederrufen, falls sich etwas in der Beziehung zwischen der Inhaberin oder dem Inhaber und der im Zertifikat genannten Organisation geändert hat. Bei Bst. b. ist nicht klar, wer ein solcher Antrag stellen darf (die Personen gem. Art. 11 Abs. 1 Bst. a. oder explizit auch im Zertifikat genannte Organisationen).	keyon AG
Diese Regelung ist für geregelte Zertifikate zu einschränkend und sollte nur auf qualifizierte Zertifikate anwendbar sein. Sie informieren die Inhaberinnen und Inhaber (geregelter) qualfizierter Zertifikate unverzüglich über die erfolgte Ungültigkeitserklärung.	Swisscom

1 (unverändert) 2 (unverändert) [3]Bei Ungültigerklärung nach Absatz 1 lit. b, weil Attribute im Sinne von Art. 7 Abs. 3 Bst. a nicht oder nicht mehr richtig sind, können sich die anerkannten Anbieterinnen auf Mitteilungen der für die Bestätigung von Angaben zu derartigen Attributen zuständigen Stelle gemäss Art. 9 Abs. 2 verlassen. [4]...(bisheriger Absatz 3 unverändert) Begründung: Die ZDA müssen die Möglichkeit erhalten, gestützt auf die Mitteilung einer Berufs- oder Standesorganisation, Zertifikate ohne weitere Abklärungen ungültig zu erklären, weil die Angaben nach Art. 7 Abs. 3 RevE ZertES nicht mehr richtig sind. Die Frage, ob die betreffende Mitteilung und die sich daraus ergebende Ungültigerklärung zu Recht vorgenommen wurden, ist dagegen Sache der Auseinandersetzung zwischen dem Inhaber des kryptografischen Schlüssels und der betreffenden Berufs- oder Standesorganisation.	ISSS
Hier würde ich die Regelung vorschlagen, dass die Anbieter von Zertifizierungsdiensten die Möglichkeit haben sollen, weitere Ungültigkeitsgründe vertraglich zu vereinbaren.	VSUD
Artikel 12: Verzeichnisdienste für geregelte Zertifikate	
Dem Sicherheitsaspekt wird die nötige Aufmerksamkeit geschenkt. So muss unter anderem die Gültigkeit der Zertifikate zuverlässig überprüft werden können (Art. 11 ZertES bzw. Art. 12 Entwurf).	LU
Art. 12 Abs. 3	
Die Abfragen sollten nicht nur für die öffentliche Hand, sondern grundsätzlich unentgeltlich sein. Die Zertifikate dürften nur dann breite Verwendung finden, wenn jeder jederzeit unentgeltlich überprüfen kann, ob ein Zertifikat gültig ist. Soll die Regelung beibehalten werden, wäre auszuführen, weshalb das notwendig ist und weshalb die Verbreitung der Verwendung der Zertifikate darunter nicht leidet. Hinweise für die eine oder andere Lösung könnte eine Übersicht über die heutige Praxis geben.	ZH
Artikel 13: Qualifizierte Zeitstempel	
L'article 13 concernant l'horodatage est à revoir en globalité car ce dernier est obligatoire et primordial dès que l'on veut obtenir une signature électronique légale, faute de quoi il serait notamment possible de falsifier ou meme d'antidater certains éléments, ou d'utiliser également des certificats numériques expirés.	FR
Bei der Frage, ob neu ein Zeitstempel obligatorischer Bestandteil einer qualifizierten elektronischen Signatur sein sollte, befürworten wir die im Entwurf vorgeschlagene Variante, bei der sich das ZertES selbst zu dieser Frage nicht äussert und dieses Erfordernis bei Bedarf in der jeweiligen (Spezial-) Gesetzgebung vorgesehen wird.	SO
Inclure la notion d'horodatage à cette révision de la loi apparaît pertinent dans la mesure où la nécessité d'un tel système s'est très tôt présentée pour certains cas. Si l'idée d'une disposition globale et étendue pourrait se justifier, à contrario l'adoption de dispositions spécifiques en la matière semble une solution intermédiaire admissible dans la mesure où les besoins sont propres à certains contextes particuliers.	VD

Enfin, concernant l'horodatage et les options soumises à notre considération, à savoir l'une dans laquelle la signature ne doit pas forcément être horodatée pour être assimilée à la signature manuscrite, l'autre dans laquelle elle doit l'être, le Conseil d'Etat du canton du Valais est de l'avis l'obligation d'horodater peut être fixée selon les nécessités des domaines. Ainsi, le CO requérant ce système pour assimiler la signature électronique qualifiée à la signature manuscrite est approprié au sens du Conseil d'Etat du canton du Valais.	VS
Concernant l'horodatage, notre Conseil est d'avis que la variante avec prise en compte de l'horodatage nous semble la seule envisageable. En effet, cette dernière sera certainement utilisée dans le cadre de procédures impliquant le respect de délais stricts telles que les procédures de recours. Dès lors, l'horodatage paraît être un élément indissociable de la signature électronique, non seulement qualifiée, mais également réglementée.	GE
Siehe Anmerkungen zu Art. 8.	keyon AG
Nach Ansicht des SAV rechtfertigt sich die Einführung des Zeitstempels. Zu einem späteren Zeitpunkt soll ja überprüft werden können, wann die Signatur angebracht worden ist. Dies gilt für die fortgeschrittene, die geregelte und die qualifizierte Signatur.	SAV
Damit kann die heute notwendige Infrastruktur zum Gebrauch dieser Zertifikate wie Nachweis von Berufsausweisen und Vertretungsbefugnissen stark vereinfacht werden. Ein qualifizierter Zeitstempel gem. c) kann insbesondere die Beweiskraft der qualifizierten Signatur im Verkehr mit Behörden und Gerichten erhöhen.	CI AG
Die Erklärungen in der Erläuterung sind nachvollziehbar. Hingegen wäre es sinnvoll, wenn entweder im Art. 21 („Änderung bisherigen Rechts“) die bereits heute im Gesetzeswerk referenzierte Zeitstempel entsprechend angepasst würden (Bsp. GeBüV) oder zumindest in den Erläuterungen eine Erklärung dazu gegeben würde.	Die Post
Artikel 14: Einstellung der Geschäftstätigkeit	
Auch die Förderung eines breiten Angebots an Zertifizierungsdiensten ist sinnvoll. Voraussetzung dafür ist jedoch, dass diese Anbieter auch längerfristig existieren können und die Weiterführung der Dienstleistung im Falle einer Einstellung der Geschäftstätigkeit genau geregelt ist. Dieses Bedürfnis wird im geltenden Recht wie auch im Entwurf abgedeckt (Art. 13 ZertES bzw. Art. 14 Entwurf).	LU
Artikel 15: Datenschutz	
Art. 15 Abs. 1	
Zu Artikel 15 "Datenschutz", Absatz 1 des Revisionsentwurfs, der unverändert den heute geltenden Artikel 14 Absatz 1 übernimmt, erlauben wir uns, zwei redaktionelle Vorschläge anzubringen: - Der erste Satz dieser Revisionsbestimmung gibt einen Anwendungsfall des Verhältnismässigkeitsprinzips wieder, das im Bereich des Datenschutzes von grosser Bedeutung ist. Da die Rechtslehre[1] im Zusammenhang mit dem Verhältnismässigkeitsprinzip regelmässig das Adjektiv "erforderlich" - und nicht das Adjektiv "notwendig" - verwendet, schlagen wir im Sinne einer Begriffsharmonisierung folgende Änderung des ersten Satzes vor: "Die anerkannten Anbieterinnen von Zertifizierungsdiensten und die von ihnen beauftragten Registrierungsstellen dürfen nur diejenigen Personendaten bearbeiten, die zur Erfüllung ihrer Aufgaben erforderlich sind. (...)" - Der zweite Satz hat von seinem Sinngehalt her einen engen Bezug zum datenschutzrechtlichen Zweckbindungsgebot. Dieses besagt, dass Personendaten grundsätzlich nur für den Zweck bearbeitet werden dürfen, zu dem sie erhoben worden sind. Allerdings wird in Satz 2 des Revisionsentwurfs nur der Datenhandel erwähnt. Da es keinen Grund gibt, das Zweckbindungsgebot auf ein Verbot des gewinnorientierten Datenverkaufs einzuschränken, schlagen wir für den zweiten Satz folgenden Wortlaut vor: (...) Sie dürfen diese Daten nur zur Erfüllung ihrer Aufgaben verwenden und insbesondere keinen Handel mit ihnen treiben.	BL

Art. 15 Abs. 2	
Die Bestimmung zum Datenschutz (Art. 15 ZertES) bleibt im Rahmen der vorliegenden Revision unverändert. Es wäre jedoch zu begrüssen, wenn in der Botschaft zu Art. 15 Abs. 2 ZertES ausgeführt würde, dass soweit kantonale oder kommunale öffentliche Organe betroffen sind, das jeweilige kantonale Datenschutzgesetz anwendbar ist und nicht etwa das Datenschutzgesetz des Bundes. Im Gesetz selbst wird lediglich darauf hingewiesen, dass „im Übrigen die Datenschutzgesetzgebung“ gilt.	OW
Grundsätzlich hat die Vernehmlassungsvorlage keine erheblichen Auswirkungen auf die Vollzugsorganisation des Kantons im Bereich Datenschutz. Art. 15 Abs. 2 des Gesetzesentwurfes verweist im Zusammenhang mit der Bearbeitung von Personendaten auf die „Datenschutzgesetzgebung“. Gemäss Art 3 Abs. 3 des Gesetzesentwurfes dürfen auch Verwaltungseinheiten von Bund, Kantonen und Gemeinden als Anbieterinnen von Zertifizierungsdienstleistungen anerkannt werden. Soweit kantonale oder Kommunale öffentliche Organe betroffen sind kann deshalb mit dem erwähnten Verweis nur die kantonale Datenschutzgesetzgebung gemeint sein. Das Bundesgesetz über den Datenschutz gilt definitionsgemäss ausschliesslich für die Bundesbehörden und den Verkehr der Privaten untereinander. Um Missverständnisse oder Unsicherheiten über die massgebende Datenschutzgesetzgebung vorzubeugen, regen wir an, in der Botschaft zum ZertES bei den Erläuterungen zu Art. 15 Abs. 2 deutlich festzuhalten, dass für die Verwaltungseinheiten der Kantone und Ge meinden das jeweilige kantonale Datenschutzgesetz anwendbar ist.	NW
Artikel 17: Haftung der Anbieterin von Zertifizierungsdiensten	
In den Erläuterungen wird auf Seite 15 darauf hingewiesen, dass die Haftung auf Signatur-Anwendungen beschränkt sei und nicht für Authentisierung oder weitere Anwendungen gelten soll. Wir unterstützen die Aussage, dass die CSP nicht für den Authentisierungsprozess haftbar gemacht werden können und schlagen vor im 7. Abschnitt „Haftung“ Art 17 „Haftung von Anbieterin von Zertifizierungsdiensten“ wie folgt zu ergänzen. Die Haftung ist auf Signatur-Anwendungen beschränkt und gilt nicht für die Authentisierung oder weitere Anwendungen.	Swisscom
Artikel 19: Verjährung	
Es ist nicht sinnvoll, Verjährungsbestimmungen in Spezialgesetze aufzunehmen, insbesondere dann, wenn sie mit den Verjährungsbestimmungen des Obligationenrechts identisch sind. Wir regen daher an, Art. 19 ZertES durch eine Verweisung auf Art. 60 OR zu ersetzen.	ZH

Artikel 20	
Dans ce sens, les travaux en cours devraient s'associer aux réflexions de l'Union européenne concernant la dimension transnationale de l'usage des signatures électroniques.	VD
Ebenso ist zu befürworten, dass eine Kompatibilität zur europäischen Signaturrichtlinie beachtet wird. Nicht berücksichtigt werden konnten in der vorliegenden Revision die aktuell geplanten europäischen Entwicklungen in diesem Bereich. In diesem Sinne sollte die Vorlage auf ihre Kompatibilität erneut überprüft und allenfalls überarbeitet werden. Die Revision achtet zu Recht die Kompatibilität zur europäischen Signaturrichtlinie (RL 1999/93/EG über die gemeinschaftlichen Rahmenbedingungen für elektronische Signaturen), konnte jedoch die aktuellen Erweiterungsschritte nicht einbeziehen. Anfangs Juni 2012 hat die Europäische Kommission neue Vorschriftenvorgeschlagen, um grenzüberschreitende und sichere elektronische Transaktionen in Europa zu ermöglichen. Die vorgeschlagene Verordnung soll dazu führen, dass Personen und Unternehmen mit ihren eigenen nationalen elektronischen Identifizierungssystemen (eID-Systeme) öffentliche Dienste in anderen Ländern benutzen können, sofern dort eine elektronische Identifizierung verwendet wird. Ausserdem schafft sie für den EU-Binnenmarkt eine grenzüberschreitende Verwendung elektronischer Signaturen (e-Signatur) und einschlägiger Vertrauensdienste, indem sie dafür sorgt, dass diese Dienste grenzüberschreitend funktio nieren und den gleichen Rechtsstatus haben werden, wie herkömmliche papiergestützte Verfahren. Die beiden Bestandteile der neuen Verordnung (eID und eSignatur) sollen verlässliche rechtliche Rahmenbedingungen schaffen, um sichere und nahtlose elektronische Transaktionen zwischen Unternehmen, Bürgern und öffentlichen Verwaltungen zu ermöglichen. Dadurch soll die Effektivität öffentlicher und privater Online-Dienstleistungen, des elektronischen Geschäftsverkehrs und des elektronischen Handels erhöht werden. Aufgrund der engen wirtschaftlichen Verflechtungen mit der EU sollte mit der Revision der Vorlage deshalb vorerst zugewartet werden.	SVP
Das Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur muss international abgestimmt sein, Dabei sind insbesondere die neueren Entwicklungen innerhalb der EU (Vorschlag einer Verordnung des Europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt vom 4. Juni 2012) im Auge zu behalten. Zudem muss die Anerkennung ausländischer Anbieter von Zertifizierungsdiensten weiterhin gewährleistet sein.	economie-suisse
Beurteilung: Ziel der Revision nur teilweise erreicht. Die technischen und administrativen Ausführungsbestimmungen müssen als nächsten Richtlinie Schritt von Seite des BAKOM‘s (Bundesaint für Kommunikation) neu erstellt werden. Eine Fachgruppe hat bereits mit dem BAKOM einen Vorschlag für die neue TAV ausgearbeitet. Nur mit einer neu erstellten TAV-Regulation hat die offizielle akkreditierte Zertiftzierungsstelle die Möglichkeit, diese neu definierten geregelten (fortgeschrittenen) digitalen Signaturen zu auditieren bzw. zu zertifizieren.	KPMG AG

ISSS erachtet die Schaffung einer Rechtsgrundlage für die effiziente und breite Anwendung digitaler Signaturverfahren im privaten und öffentlichen Bereich als einen wichtigen Beitragfür die Förderung des Wirtschaftsstandorts Schweiz. Aufgrund der internationalen Ausrichtung der schweizerischen Wirtschaft ist es vordringlich, dass die Gesetzgebung unseres Landes über digitale Zertifikate und den elektronischen Geschäfts- und Behördenverkehr auf das harmonisierte internationale Recht (Europäische Signaturrichtlinie 1999/93/EG vom 13. Dezember 1999 und deren Umsetzung in den Signaturgesetzen unserer Nachbarländer: Deutschland - Gesetz über Rahmenbedingungen für elektronische Signaturen vom 16.05.2011 (GE-SigG); Österreich - Bundesgesetz über elektronische Signaturen vom 19.08.1999 (A-SigG); Fürstentum Liechtenstein - Gesetz über elektronische Signaturen vom 18.09.2003 (FL-SiG)) und dessen laufende Weiterentwicklung (Vorschlag vom 04.06.2012 für eine Verordnung des Europäischen Parlamentes über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt) sowie die vorhandenen technischen Standards abgestimmt wird.	ISSS
Auf europäischer Ebene wurden erhebliche Harmonisierungsdefizite im Bereich elektronische Identifizierung, Authentifizierung und Signaturen sowie bei einschlägigen Vertrauensdiensten (eIAS) erkannt und als Hindernis für die grenzüberschreitende Nutzung identifiziert. Am 4. Juni 2012 hat die Europäische Kommission deshalb neue Vorschriften2 vorgeschlagen, um grenzüberschreitende und sichere elektronische Transaktionen in Europa zu ermöglichen. Dies soll mit den beiden Bestandteilen elektronische Identifizierung (eID) und e-Signatur erreicht werden, so dass verlässliche rechtliche Rahmenbedingungen geschaffen werden, die dank einschlägiger Vertrauensdienste sichere und nahtlose elektronische Transaktionen zwischen Unternehmen, Bürgern und öffentlichen Verwaltungen ermöglichen. „Vertrauensdienste“ (z. B. Zustellplattformen) sollen zu diesem Zweck EU-weit reguliert werden. 2 Vorschlag Wir haben die Vorschläge der vorgeschlagenen europäischen Regulierungen noch nicht im Detail analysieren können. Ein erster Blick zeigt, dass die Richtlinie 1999/93/EG in zahlreichen und wesentlichen Punkten präzisiert und erweitert werden soll. Inhaltlich steht in Bezug auf elektronische Signaturen eine Pflicht der Mitgliedstaaten, die Rechtswirkung qualifizierter elektronischer Signaturen derjenigen handschriftlicher Unterschriften gleichzustellen sowie qualifizierte elektronische Signaturen grenzübergreifend zu akzeptieren, im Vordergrund. Die Anforderungen an qualifizierte Signaturzertifikate sollen präzisiert und gewisse impraktikable Bestimmungen entfernt werden. So sollen einerseits diverse neuartige Elemente (z. B. Ort der Gültigkeitsprüfung) aufgenommen und anderseits z. B. die Begrenzung des Transaktionswertes weggelassen werden. Auf europäischer Ebene ist im Bereich eIAS mit tiefgreifenden regulatorischen Änderungen zu rechnen, die im Rahmen des „autonomen Nachvollzuges“ Anpassungen des nationalen Rechts erfordern, um mit dem elektronischen Binnenmarkt interoperabel zu sein.	Die Post
Vor wenigen Tagen, am 4. Juni 2012, hat die Europäische Kommission neue Vorschriften vorgeschlagen, um grenzüberschreitende und sichere elektronische Transaktionen in Europa zu ermöglichen. Die vorgeschlagene Verordnung soll dafür sorgen, dass Personen und Unternehmen mit ihren eigenen nationalen elektronischen Identifizierungssystemen (eID-Systeme) öffentliche Dienste in anderen EU-Ländern benutzen können, sofern dort eine elektronische Identifizierung verwendet wird. Ausserdem soll sie einen Binnenmarkt für die grenzüberschreitende Verwendung elektronischer Signaturen (e-Signaturen) und einschlägiger Vertrauensdienste schaffen, indem sie dafür sorgt, dass diese Dienste grenzübergreifend funktionieren und den gleichen Rechtsstatus haben werden wie herkömmliche papiergestützte Verfahren. Nach Auffassung der Kommission wird erst dadurch das grosse Potenzial der elektronischen Auftragsver-	SWICO

gabe (,,eBeschaffung“) voll zum Tragen kommen. Die breite Anwendung der elektronischen Unterschrift setzt unserer Auffassung ebenfalls eine umfassende Überprüfung des gesamten Privat- und Verwaltungsrechts (Bund und Kantone) voraus, wobei für jeden Kommunikationsvorgang die Anforderungen an die Identifizierung, Authentifizierung sowie Wahrung der Integrität zu prüfen und flexibel zu regeln sind. Eine allgemeine Gesetzgebung betreffend den elektronischen Geschäftsverkehr zwischen Privaten und Behörden (“B2G“) kann dabei auch Formen der elektronischen Kommunikation zulassen, welche im ZertES nicht geregelt sind, wie Zustellung durch E-Mail, Zulassung digitaler Signaturverfahren bzw. der fortgeschrittenen elektronischen Signaturen, sowie für anspruchsvolle Anwendungen die Notwendigkeit der Verwendung der geregelten bzw. der qualifizierten elektronischen Signatur.	
Die vom bisherigen ZertES übernommene Regelung, dass ausländische Zertifikate nach Einzelanerkennung durch die schweizerische Anerkennungsstelle anerkannt werden können (Art. 3 Abs. 2 revZertES), hat sich in der Praxis als zu hohe Hürde erwiesen. International tätige Firmen kommen in der Regel nicht darum herum, ihre Infrastruktur mit schweizerischen Sonderlösungen bzw. aufwändigem „Swiss finish“ zu belasten. Wir schlagen deshalb vor, entweder die Anerkennungsvoraussetzungen zu entschlacken oder dann im Sinne von Art. 20 revZertES den Abschloss internationaler Anerkennungsabkommen, namentlich mit der EU, zu forcieren. Ferner ist in Anbetracht der am 4. Juni 2012 vorgestellten Entwürfe der Europäischen Kommission zur Regelung der digitalen Schriftlichkeit eine möglichst weitgehende Harmonisierung sowohl inhaltlich, wie auch betreffend Terminologie herbeizuführen.	SwissH
Artikel 21: Vollzug	
1 Der Bund fördert in seiner gesamten Gesetzgebung die Anwendung digitaler Zertifikate und elektronischer Signaturen. 2 Die zugelassenen digitalen Signaturverfahren sind auf die Anforderungen an dieIdentifizierung und Authentifizierung der am betreffenden Kommunikationsvorgang Beteiligten sowie die Wahrung der Integrität des Inhaltes abzustimmen. [3]Privatpersonen haben das Recht, mit Behörden und Amtsstellen unter Nutzung der gesetzlich vorgeschriebenen Kommunikationsverfahren zu verkehren. Das ZertES als solches kann zwar keine Regeln über die Anwendung der verschiedenen elektronischen Signaturverfahren im Privat- und Verwaltungsrecht aufstellen. Mit dem vorgeschlagenen 9. Abschnitt soll jedoch der in Art. 1 Abs. 3 RevE ZertES um schriebenen Zielsetzung Rechnung getragen werden, dass der Bund die Verwendung digitaler Zertifikate und elektronischer Signaturen begünstigen will. Die Umsetzung dieser Zielsetzung soll in der gesamten Bundesgesetzgebung zum Tragen kommen	ISSS

Abs. 3	
Grundsätzlich begrüssen wir die in Art. 3 Abs. 3 des Gesetzesentwurfes klar formulierte Absicht, ein breites Angebot an sicheren Zertifizierungsdiensten zu fördern und die Verwendung digitaler Zertifikate und elektronischen Signaturen zu vereinfachen, um sie einem breiteren Kreis von Anwendern zugänglich zu machen. Eines der Mittel, das diesem Zweck dienen soll, halten wir aber für ordnungspolitisch heikel: Art. 21 Abs. 3 des Gesetzesentwurfes sieht ausdrücklich vor, dass der Bundesrat eine Verwaltungseinheit des Bundes – gemeint ist wohl das Bundesamt für Informatik und Telekommunikation (BIT) – beauftragen kann, auch für den Privatrechtsverkehr geregelte Zertifikate auszustellen. Eine derartige Bestimmung liesse sich – wenn überhaupt – nur dann rechtfertigen, wenn es am Markt überhaupt keine privaten Zertifikatsanbieter gäbe. Dann dürfte der Bund koordinierend eingreifen, um die angestrebten Ziele erreichen zu können. Möglicherweise war dies im Jahr 2003 noch der Fall, weshalb die Aufnahme einer solchen Bestimmung damals vielleicht noch gerechtfertigt war (vgl. die gleich lautende Bestimmung im geltenden Art. 20 Abs. 3 ZertES). Heute ist die Situation jedoch eine andere, denn inzwischen sind verschiedene private Anbieter am Markt, die geregelte Zertifikate für den Privatrechtsverkehr ausstellen. Würde der Bundesrat gestützt auf Art. 21 Abs. 3 des Gesetzesentwurfes z.B. das BIT beauftragen, auch für den Privatrechtsverkehr geregelte Zertifikate auszustellen, träte ein öffentliches Organ des Bundes in direkte Konkurrenz zu den privaten Zertifikatsanbietern. Dies ist aus ordnungspolitischen Gründen als sehr heikel zu betrachten. Steuergelder dürfen grundsätzlich nicht dazu verwendet werden, Private am Markt zu konkurrenzieren. Das wäre ein unzulässiger Eingriff in die Wirtschaftsfreiheit. Der Staat darf nur subsidiär eingreifen. Dies ist hier aber nicht (mehr) notwendig, denn der Gesetzeszweck bzw. die angestrebten Ziele – Förderung eines breiten Angebotes an sicheren Zertifizierungsdiensten und Begünstigung der Verwendung digitaler Zertifikate und elektronischer Signaturen – können auch ohne den Eingriff des Bundes in den Wettbewerb erreicht werden. Es genügt, wenn der Bund die gesetzlichen Rahmenbedingungen für die sichere und rechtsgültige Abwicklung von elektronischen Transaktionen zwischen Privaten schafft und sich im Übrigen darauf beschränkt, Zertifikate für den elektronischen Geschäftsverkehr unter Bundesbehörden oder zwischen den kantonalen und den Bundesbehörden auszustellen. Hinzu kommt, dass unter anderem auch DIE POST und Swisscom wichtige Anbieter von elektronischen Zertifikaten für den Privatrechtsverkehr sind. Beide Unternehmen gehören – ganz oder mehrheitlich – dem Bund. Würde das BIT gestützt auf Art. 21 Abs. 3 des Gesetzesentwurfes beauftragt, eine gleiche oder ähnliche Dienstleistung anzubieten wie DIE POST oder Swisscom, dann würde der Bund mit einem Bundesamt die eigenen Unternehmen konkurrenzieren. Das Angebot geregelter Zertifikate für den Privatrechtsverkehr durch eine Verwaltungseinheit des Bundes ist ferner auch aus finanzpolitischen Gründen skeptisch zu beurteilen. Entwicklung und Vermarktung der entsprechenden Produkte und Dienstleistungen würden beim betreffenden Bundesamt zu offensichtlich zu Mehrausgaben führen (Infrastrukturen, Personal, Organisation, Entwicklungskosten). Die Teilnahme am wirtschaftlichen Wettbewerb mit Produkten und Dienstleistungen, die auch von Privaten angeboten werden, würde einer objektiven und ergebnisoffenen Aufgabenüberprüfung des Bundes kaum standhalten. Schliesslich ist anzufügen, dass es heute auch einige grosse kantonale Informatikleistungserbringer gibt, die (theoretisch) in der Lage wären, geregelte Zertifikate für den Privatrechtsverkehr auszustellen. Gemäss Art. 21 Abs. 3 des Gesetzesentwurfes kann der Bundesrat aber ausdrücklich nur eine Verwaltungseinheit des Bundes damit beauftragen. Wenn man den ordnungs- und finanzpolitischen Sündenfall schon zulassen will, dann sollten Bund und Kantone wenigstens gleich lange Spiesse erhalten. Das heisst, auch die	SZ

kantonalen Informatikleistungserbringer sollten unter den gleichen Bedingungen, wie sie für die Verwaltungseinheiten des Bundes gelten, mit der Ausstellung von geregelten Zertifikaten für den Privatrechtsverkehr beauftragt werden können. Vorschlag Art. 21 Abs. 3 Art. 21 Abs. 3 des Gesetzesentwurfes sei wie folgt zu ändern: „Um den Gesetzeszweck zu erfüllen, kann er sich an einer privaten Anbieterin von Zertifizierungsdiensten beteiligen." – Alternativ dazu seien zumindest die Voraussetzungen für die Anwendung dieser Bestimmung sozu formulieren, dass ein unzulässiger Eingriff in den Wettbewerb ausgeschlossen ist (z.B. Angebot durch eine Verwaltungseinheit nur als „Starthilfe", das heisst nur so lange, wie keine privaten Anbieter am Markt tätig sind; Beschränkung des Angebotes auf das Notwendige; usw.). – Soll die Möglichkeit des Angebotes geregelter Zertifikate für den Privatrechtsverkehr durch den Staat trotz der geäusserten ordnungs- und finanzpolitischen Bedenken offen gehalten werden, sollen auch kantonale Verwaltungseinheiten damit beauftragt werden können.	
Um den Gesetzeszweck zu erfüllen kann der Bundesrat gemäss Art. 21 Abs. 3 ZertES weiterhin eine Verwaltungseinheit des Bundes beauftragen, geregelte Zertifikate auch für den Privatrechtsverkehr auszustellen. Die Bestimmung wird im Rahmen der vorliegenden Revision lediglich dahingehend geändert, dass der Begriff „qualifizierte Zertifikate" durch „geregelte Zertifikate" ersetzt wird. Es stellt sich unseres Erachtens jedoch die Frage, ob diese Bestimmung überhaupt noch notwendig ist. Die Bestimmung wurde ursprünglich ins Gesetz aufgenommen, um der Möglichkeit Rechnung zu tragen, dass sich allenfalls kein privater Zertifizierungsdiensteanbieter um eine Anerkennung bemüht (Botschaft zum ZertES, BBI 2001, 5703). Die Situation hat sich seither geandert und es besteht für den Bund keine Notwendigkeit mehr, hier selber aktiv zu werden und damit allenfalls den Markt zu konkurrenzieren.	OW
Eines der Mittel, das diesem Zweck dienen soll, halten wir aber für ordnungspolitisch unzulässig. Art. 21 Abs. 3 des Gesetzesentwurfes sieht ausdrücklich vor, dass der Bundesrat eine Verwaltungseinheit des Bundes — gemeint ist wohl das Bundesamt für Informatik und Telekommunikation (BIT) — beauftragen kann, auch für den Privatrechtsverkehr geregelte Zertifikate auszustellen. Eine derartige Bestimmung liesse sich — wenn überhaupt — nur dann rechtfertigen, wenn es am Markt überhaupt keine privaten Zertifikatsanbieter gäbe. Dann dürfte der Bund koordinierend eingreifen, um die angestrebten Ziele erreichen zu können. Möglicherweise war dies im Jahr 2003 noch der Fall, weshalb die Aufnahme einer solchen Bestimmung damals noch gerechtfertigt war (vgl. die gleich lautende Bestimmung im geltenden Art. 20 Abs. 3 ZertES). Heute ist die Situation jedoch eine andere, denn inzwischen sind verschiedene private Anbieter am Markt, die geregelte Zertifikate für den Privatrechtsverkehr ausstellen. Würde der Bundesrat gestützt auf Art. 21 Abs. 3 des Gesetzesentwurfes z.B. das BIT beauftragen, auch für den Privatrechtsverkehr geregelte Zertifikate auszustellen, träte ein öffentliches Organ des Bundes in direkte Konkurrenz zu den privaten Zertifikatsanbietern. Dies ist aus ordnungspolitischen Gründen abzulehnen. Der Staat darf nur subsidiär eingreifen. Dies ist hier nicht mehr notwendig, denn der Gesetzeszweck bzw. die angestrebten Ziele — Förderung eines breiten Angebotes an sicheren Zertifizierungsdiensten und Begünstigung der Verwendung digitaler Zertifikate und elektronischer Signaturen — können auch ohne den Eingriff des Bundes in den Wettbewerb erreicht werden. Es genügt, wenn der Bund die gesetzlichen Rahmenbedingungen für die sichere und rechtsgültige Abwicklung von elektronischen Transaktionen zwischen Privaten schafft und sich im Übrigen darauf beschränkt, Zertifikate für den elekt-	NW

ronischen Geschäftsverkehr unter Bundesbehörden oder zwischen den kantonalen und den Bundesbehörden auszustellen. Hinzu kommt, dass u.a. auch DIE POST und Swisscom wichtige Anbieter von elektronischen Zertifikaten für den Privatrechtsverkehr sind. Beide Unternehmen gehören — ganz oder mehrheitlich — dem Bund. Würde das BIT gestützt auf Art. 21 Abs. 3 des Gesetzesentwurfes beauftragt, eine gleiche oder ähnliche Dienstleistung anzubieten wie DIE POST oder Swisscom, dann würde der Bund mit einem Bundesamt die eigenen Unternehmen konkurrenzieren. Das Angebot geregelter Zertifikate für den Privatrechtsverkehr durch eine Verwaltungseinheit des Bundes ist ferner auch aus finanzpolitischen Gründen abzulehnen. Entwicklung und Vermarktung der entsprechenden Produkte und Dienstleistungen würden beim betreffenden Bundesamt zu erheblichen Mehrausgaben führen (Infrastrukturen, Personal, Organisation, Entwicklungskosten). Dies ist schlecht mit den laufenden Sparbemühungen des Bundes vereinbar. Die Teilnahme am wirtschaftlichen Wettbewerb mit Produkten und Dienstleistungen, die auch von Privaten angeboten werden, würde einer objektiven und ergebnisoffenen Aufgabenprüfung des Bundes kaum standhalten. Schliesslich ist anzufügen, dass es heute auch einige grosse kantonale Informatikleistungserbringer gibt, die theoretisch in der Lage wären, geregelte Zertifikate für den Privatrechtsverkehr auszustellen. Gemäss Art. 21 Abs. 3 des Gesetzesentwurfes kann der Bundesrat aber ausdrücklich nur eine Verwaltungseinheit des Bundes damit beauftragen. Wenn man den ordnungs- und finanzpolitischen Sündenfall schon zulassen will, was an sich klar abzulehnen ist, dann sollten Bund und Kantone wenigstens gleich lange Spiesse erhalten. D.h. auch die kantonalen Informatikleistungserbringer sollten unter den gleichen Bedingungen, wie sie für die Verwaltungseinheiten des Bundes gelten, mit der Ausstellung von geregelten Zertifikaten für den Privatrechtsverkehr beauftragt werden können Gestützt auf vorstehenden Ausführungen schlagen wir vor, Art. 21 Abs. 3 des Gesetzesentwurfes wie folgt zu ändern: „Um den Gesetzeszweck zu erfüllen, kann er sich an privaten Anbietern von Zertifizierungsdiensten beteiligen“. Alternativ dazu seien zumindest die Voraussetzungen für die Anwendung dieser Bestimmung so zu formulieren, dass ein unzulässiger Eingriff in den Wettbewerb ausgeschlossen ist. Ein Angebot durch eine Verwaltungseinheit soll nur als „Starthilfe“, d.h. nur so lange, wie keine privaten Anbieter am Markt tätig sind. Dieses ist auf das Notwendige zu beschränken. Soll die Möglichkeit des Angebotes geregelter Zertifikate für den Privatrechtsverkehr durch den Staat trotz der geäusserten ordnungs- und finanzpolitischen Bedenken offen gehalten werden, sollen auch kantonale Verwaltungseinheiten damit beauftragt werden können.	
Artikel 22: Aufhebung und Änderung bisherigen Rechts	
La révision traite sous article 22 de l'abrogation et des modifications du droit en vigueur. Or l'ancien article 22 de la version initiale de la SCSE traitait des mesures transitoires, qui ont été avec raison abrogées depuis, mais qui seraient de nouveau d'actualité à l'occasion de l'introduction de cette nouvelle version de la SCSE, en particulier concernant l'introduction de la signature électronique réglementée. Or l'avant-projet ne contient pas de disposition relative au droit transitoire.	GE

Bemerkungen zu den Erläuterungen	Wer?
Obschon die Erläuterungen zu einem Gesetzesentwurf derartige Angaben zur geplanten Umsetzung und ihren finanziellen und personellen Auswirkungen auf die Kantone haben müssten (vgl. Art. 8 VIV i.V.m. Art. 141 Abs. 2 lit. d und f ParlG), schweigt sich der unterbreitete Bericht dazu aus. Wir ersuchen Sie, diesen Mangel bei der Erarbeitung der Botschaft zu beheben und die Konsequenzen der Vorlage in möglichst allen Dimensionen (z.B. finanzielle, rechtliche und technische Aspekte) aufzuzeigen.	BE
Le rapport explicatif (point 1.1 Contexte) fait état d'une «grande insécurité juridique», entendant par là que l'avant-projet actuel la règle ; or on ne sait ni de quelle nature est cette insécurité ni comment le présent avant-projet entend y remédier. Ad autres lois et ordonnances concernées On peut regretter que les conséquences sur l'OSCSE ne soient pas encore explicitées ou connues dans le cadre de cet avant-projet, alors que les deux révisions sont indéniablement liées. Les conséquences sur les prescriptions techniques et administratives devraient aussi être explicitées.	GE
Seite 2: Gemäss den Ausführungen auf Seite 2 des erläuternden Berichts ist ein erklärtes Ziel der vorliegenden Totalrevision die terminologische Vereinfachung bei der Regelung der elektronischen Signatur. Vor diesem Hintergrund ist es u.E. nicht einsichtig, weshalb man an den unterschiedlichen Bezeichnungen elektronische Signatur und digitales Zertifikat festhält. Wäre es nicht sinnvoll, im Zuge dieser Totalrevision auch bei den Signaturen von digitalen Signaturen zu sprechen? Sollte es allerdings eine technische Begründung für diese Differenzierung geben, so würden wir es begrüssen, wenn in den Materialien zu dieser Gesetzesrevision erläutert würde, aus welchen Gründen man in diesem Punkt auf die terminologische Vereinfachung verzichtet.	Städteverband
Da die Normen zum elektronischen Behörden- und Gerichtsverkehr historisch gewachsen sind, sind die heutigen gesetzlichen Bestimmungen uneinheitlich und nicht aufeinander abgestimmt. Diese Normen sollten vereinheitlicht werden. Zudem wird zu prüfen sein, wie der elektronische Behördenverkehr schweizweit einheitlich umgesetzt werden kann (Einsatz Personenidenfikator [UID / AHV-Nummer], strukturierte Daten im XML-Format, etc.). Es handelt sich hierbei um folgende Bestimmungen: — Anpassung der Kann-Vorschriften gemäss Art. 26 Abs. ibis und 34 Abs. 2 VwVG, Art. 60 Abs. 3 BGG, 139 Abs. 1 ZPO; 34 Abs. 2 SchKG und 86 StPO auf eine obligatorische Zustellung, wenn dies die den ERV benützende Person verlangt; — Streichung der Kann-Vorschriften (Nachreichung in Papierform), die das Gesetz gemäss Art. 130 Abs. 3 ZPO; 33a Abs. 3 SchKG und Art. 110 Abs. 2 StPO vorsieht; — Harmonisierung der historisch gewachsenen gesetzlichen Bestimmungen zum ERV mit den Regeln in den neuen Prozessordnungen: insbesondere die Art. 20 Abs. 2bis VwVG, 44 Abs. 2 BGG und 38 Abs. 2bis ATSG. Damit Stammdaten quer durch alle Instanzen und Kantone nur einmal eingegeben werden müssen, womit Fehler vermieden, Zeit gespart und Kosten gesenkt werden können, sollten verbindliche Vorschriften für eine strukturierte Datenübermitt lung erlassen, wofür in Artikel 6 Absatz 2 der Verordnung vom 18. Juni 2010 über die elektronische Ubermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren bereits eine Grundlage besteht. Mit der weiteren Anpassung einzelner Artikel, die ohnehin geändert werden müssen, soll nach Meinung des SAV nicht zugewartet werden. Damit ist gewährleistet, dass die fehlende Koordination einzelner Bestimmungen und damit auch alle Unsicherhei ten in der Auslegung rasch beseitigt werden.	SAV

3. Abschnitt	
Der Titel des 3. Abschnitts des ZertES ändert von „Generierung und Verwendung von Signaturund Signaturprüfschlüsseln“ zu „Generierung, Speicherung und Anwendung kryptografischer Schlüssel. Im erläuternden Bericht wird dazu nur auf die Änderung zum allgemeinen Ausdruck des „kryptografischen Schlüssels“ Bezug genommen. Uns würden zusätzliche Erläuterungen, weshalb neu auch die Speicherung der Schlüssel relevant ist, sinnvoll erscheinen.	Städteverband
Art. 6 Abs. 3 (bisher)	
Die Ausführungen zu der Streichung des bisherigen Artikels 6 Absatz 3 vermögen uns nicht zu überzeugen. Aus den Erläuterungen geht nicht hervor, wie der Empfänger einer elektronischen Signatur überprüfen können soll, ob u.a. die Identität der Inhaberin oder des Inhabers des Signaturschlüssels korrekt angezeigt wird, die Verwendung eines Pseudonyms eindeutig angegeben wird oder die sicherheitsrelevanten Veränderungen erkannt werden können. Nach unserer Ansicht müsste man diese Bestimmung, anstatt sie zu streichen, so formulieren, dass der Normadressat — die Anbieterin von Zertifizierungsdiensten — verpflichtet wird, technisch sicher zu stellen, dass der Empfänger einer elektronischen Signatur diese in geeigneter Weise überprüfen kann, respektive ihm taugliche Werkzeuge für die Überprüfung zur Verfügung stehen (z.B. durch Zusammenarbeit mit den entsprechenden Anbietern).	Städteverband
Artikel 13: Qualifizierte Zeitstempel	
S‘agissant de l‘horodatage, le rapport relève au point 1 .3.4 qu‘il s‘agit parfois du seul moyen d‘éviter des attaques informatiques ou des fraudes, que ce service est répandu et figure souvent en tant que paramètre par défaut, et qu‘il ne pose quasiment plus de problème dès qu‘une connexion est possible à internet. Dans ces circonstances, nous saisissons mal pourquoi la solution consistant à rendre l‘horodatage de la signature électronique qualifiée obligatoire par le biais de la SCSE na pas été retenue. Le motif selon lequel cette solution est “trop restrictive“ n‘emporte pas la conviction, dès lars que le rapport laisse entendre qu‘il n‘y a pas de difficulté technique. Quant au fait que le droit européen ne prévoit pas l‘horodatage, il ne doit pas nous conduire baisser le niveau de sécurité dont Ion peut bénéficier en fonction de l‘état actuel de la technique. Si nécessaire, le Conseil fédéral pourra reconnaitre des signatures européennes non horodatées par le biais de conventions, sur la base de l‘article 20 de l‘avant-projet. En outre, obligation d‘horodater devrait pouvoir étre étendue la signature électronique réglementée.	JU
Artikel 15: Datenschutz	
Art. 15 Abs. 2	
Grundsätzlich hat die Vernehmlassungsvorlage keine erheblichen Auswirkungen auf die Vollzugsorganisation des Kantons im Bereich Datenschutz. Art. 15 Abs. 2 des Gesetzesentwurfes verweist im Zusammenhang mit der Bearbeitung von Personendaten auf die „Datenschutzgesetzgebung“. Gemäss Art. 3 Abs. 3 des Gesetzesentwurfes dürfen auch Verwaltungseinheiten von Bund, Kantonen und Gemeinden als Anbieterinnen von Zertifizierungsdienstleistungen anerkannt werden. Soweit kantonale oder kommunale öffentliche Organe betroffen sind kann deshalb mit dem erwähnten Verweis nur die kantonale Datenschutzgesetzgebung gemeint sein. Das Bundesgesetz über den Datenschutz gilt definitionsgemäss ausschliesslich für die Bundesbehörden und den Verkehr der Privaten untereinander. Vorschlag Erläuterungen Art. 15 Abs. 2: Um Missverständnissen oder Unsicherheiten über die massgebende Datenschutzgesetzgebung vorzubeugen, regen wir an, in der Botschaft zum ZertES bei den Erläuterungen zu Art. 15 Abs. 2 deutlich festzuhalten, dass für die Verwaltungseinheiten der Kantone und Gemeinden das jeweilige kantonale Datenschutzgesetz anwendbar ist.	SZ

Il est parfois délicat de saisir la portée pratique du nouveau format de signature électronique réglementée, car le rapport se refuse expressément à définir ses effets juridiques, renvoyant, au sujet de ceux-ci, aux accords entre parties, à la législation spéciale et à la doctrine (cf. p. ex. point 1 .3.2 i. f.). Sans vouloir remettre en cause la pertinence de l'article 1, alinéa 2, de l'avant-projet, l'approche du rapport ne nous paraît cependant pas totalement satisfaisante car l'intéresse le législateur de connaitre les incidences pratiques de l'outil qu'il crée. A titre d'exemple, ii est douteux qu'un contrat passé au moyen de la signature électronique réglementée puisse donner lieu une mainlevée provisoire de lopposition en cas de poursuites fondées sur la LP. A nos yeux, il s'agit d'une question qui devrait étre clarifiée en amont pour convaincre des utilisateurs de recourir à ce moyen de signature.	JU

Aufhebung und Änderung bisherigen Rechts	
Bundesgerichtsgesetz	
Bei elektronischer Zustellung muss das Dokument, das die Rechtsschrift und die Beilagen enthält, von der Partei oder ihrem Vertreter beziehungsweise ihrer Vertreterin mit einer geregelten elektronischen Signatur versehen werden. Das Bundesgericht bestimmt in einem Reglement das Format der Übermittlung und die zu verwendende Signatur. An die Stelle der „anerkannten elektronischen Signatur“ gemäss heutigem Wortlaut von Art. 42 Abs. 4 BGG soll also die „geregelte elektronische Signatur“ treten. Die „geregelte elektronische Signatur“ ist eine neue Form der fortgeschrittenen elektro nischen Signatur. Sie wird in Art. 2 lit. c E—ZertES definiert. Gemäss den Erläuterungen zum Vorentwurf kann die geregelte elektronische Signatur für natürliche und juristische Behörden bzw. Behörden ausgestellt werden. Sie reiht sich zwischen die fortgeschrittene elektronische Signatur und die qualifizierte elektronische Signatur ein und eignet sich daher auch für den Einsatz in Gerichtsbehörden. Namentlich erleichtert sie die Zustellung von elektronischen Sendungen durch das Bundesgericht immer dann, wenn die Zustellung durch die Gerichtskanzlei genügt und es nicht auf die Person des Absenders ankommt. Die geregelte Signatur gemäss Art. 2 lit. c E—ZertES als solche wird vom Bundesgericht daher durchaus begrüsst. Hingegen kann die Verwendung dieses Begriffes in Art. 42 Abs. 4 E—BGG zu Fehlinterpretationen verleiten. Es kann jedenfalls nicht angehen, dass beliebige Angestellte von Anwaltskanzleien, die sich als juristische Person konstituiert haben, beim Bundesgericht fristwahrende Eingaben machen können. Dieses Recht steht nur den im Anwaltsregister eingetragenen Rechtsanwälten und Rechtsanwältinnen zu. Für solche Eingaben muss das Bundesgericht weiterhin eine qualifizierte elektronische Unterschrift verlangen können. Die erwähnte Unklarheit ergibt sich aus dem Umstand, dass die „geregelte elektronische Signatur“ einerseits in Art. 2 lit. c E—ZertES im oben umschriebenen Sinne als eigenständige elektronische Signatur definiert wird, andererseits aber auch im Zusammenhang mit der qualifizierten elektronischen Signatur gemäss Art. 2 lit. d E—ZertES verwendet wird, die gemäss der gesetzlichen Definition eine „qualifizierte“ geregelte elektronische Signatur darstellt. Die Unschärfe kann behoben werden, indem in Art. 42 Abs. 4 E—BGG das Wort „geregelt“ gestrichen wird. Mit dieser Streichung werden allfällige Schwierigkeiten bei der Auslegung des Begriffes „geregelte elektronische Signatur“ im Sinne von Art. 42 Abs. 4 E—BGG vermieden. Im Übrigen wird dem Bundesgericht ja zu Recht die Kompetenz zugestanden, in einem Reglement „das Format der Übermittlung und die zu verwendende Signatur“ zu bestimmen. Das Bundesgericht wird die zu verwendende Signatur je nach Typ der Eingabe sachgerecht regeln. Es sollte dabei keinen falschen Beschränkungen unterliegen.	BGer
Art. 42 BGG: Änderung Abs. 4 Satz 1 ~~Bei elektronischer Zustellung muss das Dokument, das die Rechtsschrift und die Beilagen enthält, von der Partei oder ihrem Vertreter beziehungsweise ihrer Vertreterin mit einer geregelten elektronischen Signatur versehen~~. Bei elektronischer Ubermittlung muss die Eingabe mit einer geregelten elektronischen Signatur der Partei oder ihres Vertreters beziehungsweise ihrer Vertreterin versehen sein. Begründung: Die Begründung für diese Änderung ist die gleiche wie für die Änderung von Art. 21a Abs. 2 VwVG. Mit dem Zusatz “beziehungsweise ihrer Vertreterin“ wird der Terminologie der BGG Rechnung getragen. Art. 44 BGG: Änderung Abs. 2 (im Vernehmlassungsentwurf nicht vorgesehen) 2 Eine Mitteilung, die nur gegen Unterschrift des Adressaten oder der Adressatin oder einer anderen berechtigten Person bezie-	SAV

hungsweise gegen eine gleichwertige elektronische Empfangsbestätigung überbracht wird, gilt spätestens am siebenten Tag nach dem ersten erfolglosen Zustellungsversuch als erfolgt. Begründung: Es kann vollumfänglich auf die Begründung zur Änderung von Art. 20 Abs. 2bis VwVG verwiesen werden. Gegenüber jener Bestimmung werden hier wie bisher Adressat und Adressatin genannt. Art. 48 BGG: Änderung Abs. 2 (im Vernehmiassungsentwurf nicht enthalten) 2 Im Falle der elektronischen Zustellung ist die Frist gewahrt, wenn ~~der Empfang bei der Zustelladressen des Bundesgerichts vor Ablauf der Frist durch das betreffende Informatiksystem bestätigt worden ist~~, das anerkannte Informatiksystem, über welches die elektronische Zustelladresse des Bundesgerichts erreichbar ist, vor Ablauf der Frist den Empfang bestätigt hat. Begründung: Auch diese Begründung entspricht jener für die Änderung von Abs. 3 von Art. 21a VwVG. Art. 60 BGG: Änderung Abs. 3 Satz 1 ~~Mit dem Einverständnis~~ Auf Verlangen der Partei kann muss für diese die Eröffnung auf dem elektronischen Weg erfolgen. Begründung: Die beantragte Änderung von Art. 60 BGG entspricht wörtlich jener von Art. 34 Abs.ibis VwVG. Auf die Begründung dazu wird verwiesen. Der Formulierungsvorschlag nimmt darauf Bedacht, dass es auch künftig Parteien geben wird, denen nicht elekt ronisch zugestellt werden kann. Der Mehraufwand einer elektronischen und postalischen Zustellung im gleichen Fall ist bescheiden und wird vom Bundesgericht schon heute in Kauf genommen.	
Zu Art. 42 Abs. 4 Bundesgerichtsgesetz (BGG) : Es ist nicht einsichtig, warum nicht eine qualifizierte Signatur gefordert wird. Folgende Formulierung könnte die Verständlichkeit, wann welcher Zertifikatstyp einzusetzen ist, erhöhen: Bei elektronischer Zustellung muss das Dokument, das die Rechtsschrift und die Beilagen enthält, von der Partei oder ihrem Vertreter beziehungsweise ihrer Vertreterin mit einer qualifizierten elektronischen Signatur versehen werden. Das Bundesgericht bestimmt in einem Reglement das Format der Übermittlung.	Die Post

Verwaltungsverfahrensgesetz	
Art. 20 VwVG : Änderung Abs. 2bis (im Vernehmlassungsentwurf nicht vorgesehen) 2bis Eine Mitteilung, die nur gegen Unterschrift des Adressaten oder einer anderen berechtigten Person beziehungsweise gegen eine gleichwertige elektronische Empfangsbestätigung überbracht wird, gilt spätestens am siebenten Tag nach dem ersten erfolglosen Zustellungsversuch als erfolgt. Begründung Im Rahmen der terminologischen Vereinheitlichung der Bestimmungen über die elektronische Signatur sollen nach Meinung des SAV auch Widersprüche zwischen älteren und neueren Vorschriften ausgemerzt werden, die sich bei der elektronischen Zustellung ergeben. Es betrifft dies neben Abs. 2bis von Art. 20 VwVG die Art. 44 Abs. 2 BGG und 38 Abs. 2bis ATSG, wo im Gesetzestext (je seit 2007 geltend) noch unterstellt wird, dass eine (postalische) Zustellung gegen Unterschrift erfolgt und keine anderen Empfangsbestätigungen möglich sind. Tatsächlich erwähnen die neuesten AGB "Postdienstleistungen" der Schweizerischen Post vom April 2012 die Unterschrift des Empfängers nur noch beiläufig (in Ziff. 2.3.2) und bestimmen (in Ziff.2.3.1) die "elektronisch erfassten Zustellereignisse" als Nachweis für die erfolgte Zustellung. Auch die anerkannten Zustellplattformen für den elektronischen Rechtsverkehr liefern sog. eGov-Einschreiben nicht gegen Unterschrift, sondern nach einer Authentifizierung als Inhaber des entsprechenden elektronischen Postfachs aus. Dem wurde in den neuen Prozessordnungen Rechnung getragen, indem die Art. 138 Abs. 3 lit. a ZPO und Art. 85 Abs. 4 lit. a StPO einfach auf die eingeschriebene Zustellung abstellen, die bei der physischen und elektronischen Post grundsätzlich gleich abgewickelt wird. Im Sinne eines minimalen Eingriffs in den Wortlaut von Art. 20 Abs. 2bis VwVG soll dort der Begriff der eingeschriebenen Post nicht eingeführt, sondern nur die Möglichkeit einer alternativen elektronischen Empfangsbestätigung erwähnt werden.	SAV
Art. 21a VwVG: Änderung Randtitel 2. Bei elektronischer ~~Zustellung~~Übermittlung Änderung Abs. 2 Satz 1 sowie dessen 2. Halbsatz 2 ~~Die ganze Sendung ist von der Partei oder ihrem Vertreter mit einer geregelten elektronischen Signatur zu versehen~~Bei elektronischer Ubermittlung muss die Eingabe mit einer geregelten elektronischen Signatur der Partei oder ihres Vertreters versehen sein. Wo das Bundesrecht es verlangt, sind zudem einzelne Dokumente auf die gleiche Art zu unterzeichnen. Änderung Abs. 3 (im Vernehmlassungsentwurf nicht enthalten) Die Frist gilt als gewahrt, wenn das anerkannte lnformatiksystem, über ~~welchem~~welches die elektronische Zustelladresse der Behörde ~~angehört~~terreichbar ist, vor ihrem Ablauf den Empfang bestätigt hat. Begründung Die Bestimmungen des VwVG zum ERV, welche Anfang 2007 in Kraft traten, sind (wie jene des BGG) nicht mit jenen der neuen nationalen Prozessordnungen koordiniert und basieren auf überholten technischen Annahmen. Inzwischen ist ein interoperabler Verkehr über mehrere Plattformen etabliert, was nicht ausschliesst, dass einzelne Behörden direkte elektronische Briefkästen betreiben, wenn diese 24 Stunden in Betrieb sind. Klargestellt ist bereits mit einem Entscheid des Bundesgerichts, dass — jedenfalls im Bereich der ZPO — Zustellungen auf gewöhnlichem E-Mail-Weg nicht zulässig sind. Bei diesen detailliert geregelten Zugangskanälen besteht keine Notwendigkeit mehr, die Authentizität einer Sendung als Ganzes zu bescheinigen, was Motiv war, das Signieren der ganzen Sendung vorzugeben. Letzteres widerspricht auch den Gepflogenheiten im physischen	SAV

Postverkehr. Die ohnehin notwendige Revision von Abs. 2 von Art. 21a VwVG soll gleich auch die störenden Unterschiede zwischen den älteren und neueren Bestimmungen beseitigen. Die Formulierung lehnt sich an jene von Art. 130 ZPO an, wo die Beschränkung auf die Eingabe bereits vorgesehen ist, spricht aber wie bisher von Partei und Vertreters, was unseres Erachtens allerdings auch durch “der Absenderin oder des Absenders“ ersetzt werden könnte. Wie in Art. 130 Abs. 2 ZPO wird der Ausdruck “elektronische Uber mittlung“ verwendet, da “Elektronische Zustellung“ von Art. 139 ZPO für die Behördenzustellung verwendet wird. Bei einer Anpassung von Abs. 2 von Art. 21a VwVG macht auch Sinn, die gesetzlichen Festlegungen über die Fristwahrung zu koordinieren. Entsprechend wird zusätzlich eine Anpassung von Abs. 3 dieser Bestimmung vorgeschlagen. Die vorgeschlagene Formulierung ist offen und lässt auch möglichen künftigen technischen Entwicklungen Raum.	
Art. 26 VwVG: Änderung Abs. 1 bis (im Vernehmiassungsentwurf nicht vorgesehen) lbs Die Behörde ~~kann~~muss die Aktenstücke auf elektronischem Weg zur Einsichtnahme zustellen, wenn die Partei oder ihr Vertreter ~~damit einverstanden ist~~ dies verlangt. Begründung: Dem elektronischen Rechtsverkehr kann nur Erfolg beschieden sein, wenn auch dieVerfahrensakten elektronisch geführt werden. Dann ist auch eine Akteneinsicht auf elektronischem Weg leicht realisierbar. Die heutige Kann-Vorschrift soll neu als Behördenpflicht formuliert werden. Soweit Ubergangsregelungen notwendig wären, könnte man sie auf dem Verordnungsweg treffen. Im Weiteren wird auf die Begründung der nachstehenden Anderung von Art. 34 Abs. 1 Satz 1 VwVG verwiesen.	SAV
Art. 34 VwVG: Änderung Abs. 1 bis Satz 1 ibis ~~Mit dem Einverständnis~~ Auf Verlangen der Partei (kann)muss für diese die Eröffnung auf dem elektronischen Weg erfolgen. Begründung Die Kann-Vorschrift, dies es im Belieben der Behörde belässt, ob sie elektronisch zustellen will, ist aus Sicht des SAV ein weiteres Hindernis für die Verbreitung des elektronischen Rechtsverkehrs. Dank ihr erweist er sich derzeit mit wenigen Ausnahmen (u.a. beim Bundesgericht) als Einweg-Verkehr, Die Vorschrift soll neu als Behördenverpflichtung formuliert werden, die aber nicht generell für jede Zustellung gilt, sondern nur, wenn es eine Partei für sich verlangt. Die beantragte Anderung schafft — wie die beantragte Streichung von Art. 130 Abs. 3 ZPO, Art. 110 Abs. 2 letzter Satz ZPO und Art. 33a Abs. 3 SchKG — einen Anreiz für Behörden, auf die elektronische Aktenführung umzustellen. Soweit es ein Bedürfnis gäbe, Behörden in Ein zelfällen von elektronischen Zustellungen zu dispensieren, wäre dies nicht auf Gesetzesstufe, sondern auf Stufe Verordnung zu regeln.	SAV
Art. 21a Abs. 2 Verwaltungsverfahrensgesetz (VwVG): Es ist nicht einsichtig, warum nicht eine qualifizierte Signatur gefordert wird. Folgende Formulierung könnte die Verständlichkeit, wann welcher Zertifikatstyp einzusetzen ist, erhöhen: Die ganze Sendung ist von der Partei oder ihrem Vertreter mit einer qualifizierten elektronischen Signatur zu versehen; wo das Bundesrecht es verlangt, sind zudem einzelne Dokumente auf die gleiche Art zu unterzeichnen.	Die Post
Art. 34 Abs. 1bis VwVG: Es ist nicht einsichtig, warum nicht eine qualifizierte Signatur gefordert wird. Folgende Formulierung könnte die Verständlichkeit, wann welcher Zertifikatstyp einzusetzen ist, erhöhen: Mit dem Einverständnis der Partei kann die Eröffnung auf dem elektronischen Weg erfolgen. Die Verfügungen sind mit einer qualifizierten elektronischen Signatur zu versehen. Der Bundesrat regelt die Anforderungen an die elektronische Eröffnung.	Die Post

Obligationenrecht	
Art. 59a OR Haftung für Signaturschlüssel	
Im Allgemeinen lässt sich weder der Botschaft zum geltenden ZertES noch der einschlägigen Literatur entnehmen, weshalb es diese Haftungsbestimmung überhaupt braucht. Wir haben ferner keine Informationen darüber, ob sie jemals angewendet wurde. Es ist daher zu prüfen, ob und inwiefern nicht bereits die allgemeinen vertraglichen bzw. ausservertraglichen Haftungsbestimmungen des OR genügen. Die Erläuterungen sollten sich jedenfalls klar und verständlich zu dieser Frage äussern. Im Übrigen ist Art. 59 Abs. 1 OR nun missverständlich formuliert: Die Formulierung legt den Schluss nahe, dass für die Authentisierung mittels geregelten Zertifikats die gleiche Haftungsregelung (d. h. implizite Beweislastumkehr) wie für die Signatur gelten soll. Der erläuternde Bericht enthält dagegen die Aussage, die Haftung mit Beweislast umkehr sei auf Signatur-Anwendungen beschränkt.	ZH
Weiter beantragen wir Artikel 59a Absatz 1 DR ersatzlos zu streichen. Mit dieser Haftungsklausel ergäbe sich eine Beweislastumkehr. Diese Beweisführung kann ein Inhaber eines geheimen kryptografischen Schlüssels kaum leisten, da er ggfs. den Herstellern von Anwendungen und Betriebssystemen Sicherheitslücken nachweisen muss. Auch Bedrohungen durch Malware sind für Inhaber nicht ohne weiteres erkenn- und mit den gängig technischen Möglichkeiten abwehrbar. Für alifällige Schäden bietet nach unserem Dafürhalten Artikel 41 OR eine ausreichende Grundlage.	GL
Nous formulons pour le surplus deux remarques de forme: - le commentaire de l'article 59a CO ne correspond pas au texte de l'avant-projet.	JU
Die Haftungsklausel im Obligationenrecht Art. 59a Abs. 1 führt jedoch zu einer rechtlichen Ungleichbehandlung der elektronischen und handschriftlichen Signatur und schiesst klar über das Ziel hinaus. Deshalb ist diese ersatzlos zu streichen.	FDP
Zu Artikel 59a OR wird auf Seite 15 im Bericht gesagt, dass hier der Begriff „Signaturschlüssel" nicht durch den generellen Begriff „kryptografischer Schlüssel" ersetzt werde. Tatsächlich ist im Entwurf dann aber vom Inhaber eines geheimen kryptografischen Schlüssels" die Rede. Nach unserer Ansicht müsste Artikel 59a OR, um die Haftung wie beabsichtigt auf Signaturanwendungen zu beschränken, weiterhin der Begriff „Signaturschlüssel" verwendet werden.	Städteverband
Bereits die heutige Haftung für Signaturschlüssel wird stark kritisiert. Diese Gefährdungshaftung wird unter anderem als einen der wesentlichen Gründe für die ungenügende Akzeptanz der elektronischen Signatur im Rechtsverkehr betrachtet. Die zusätzliche Ausdehnung der Haftung auf geregelte Zertifikate wird einhellig abgelehnt. Jeder Benutzer von elektronischen Signaturen bzw. Zertifikaten kommuniziert im Rahmen der gesetzlichen und vertraglichen Regelungen grundsätzlich rechtlich verbindlich. Dies ergibt sich aber bereits aus Art. 14 Abs. 2 DR. Eine zusätzliche Haftungsklausel in der Form von Art. 59a Abs. 1 DR ist deshalb weder sinnvoll noch nötig. economiesuisse fordert daher die ersatzlose Streichung von Art. 59a OR.	economiesuisse
Aus Sicht des SAV ist zumindest zu prüfen, ob die Bestimmung von Art. 59a OR nicht ein Killerkriterium für den Einsatz qualifizierter elektronischer Signaturen darstellt. Dies jedenfalls nach Einführung der geregelten Signatur. Nach Ansicht des SAV liegen die Vorteile der geregelten Signatur v.a. in der Massen- und Alltagstauglichkeit, sodass die qualifizierte Signatur im Geschäftsalltag nie an erheblicher Bedeutung gewinnen könnte. Sofern der Einsatz der qualifizierten elektronischen Signatur auf das Notwendige (siehe nachstehende Ausführungen) beschränkt wird, liesse sich ein Beibehalten der Bestimmung von Art. 59a OR rechtfertigen.	SAV

Die Zielsetzung von Art. 1 Abs. 3 RevE ZertES kann insbesondere durch die nachstehenden vorgeschlagenen Änderungen des bisherigen Rechts realisiert werden: Begründung: Die Bestimmung widerspiegelt die Faszination, aber auch die Besorgnisse des historischen Gesetzgebers über den Umgang mit modernen technischen Verfahren. Sie ist dazu angetan, von der Nutzung der digitalen Unterschrift nach ZertES abzusehen und Signaturverfahren ausserhalb der Regelungen des ZertES zu entwickeln. Weder die europäische Signaturrichtlinie 1999/93/EG, noch das deutsche Gesetz über Rahmenbedingungen für elektronische Signaturen vom 16.05.2011 (GE-SigG), noch das österreichische Bundesgesetz über elektronische Signaturen vom 19.08.1999 (A-SigG), noch das liechtensteinische Gesetz über elektronische Signaturen vom 18.09.2003 (FL-SiG) kennen eine derartige verschuldensunabhängige Gefährdungshaftung des Inhabers des von einer anerkannten Anbieterin von Zertifizierungsdiensten mit einem Zertifikat ausgestellten Signaturschlüssels. Angesichts der strengen gesetzlichen Haftung von Art. 59a OR stellt sich die Frage, wie der Schlüsselinhaber sich vor der verschuldensunabhängigen Haftung aufgrund von Bedrohungen, z.B. durch das Einschleusen von Maiware, schützen kann, die nicht erkennbar sind und mit den gängigen technischen Verfahren auch nicht abgewehrt werden können. Die geltende Regelung schiebt das Risiko für solche Bedrohungen durch den Einsatz von Malware einseitig dem Schlüsselinhaber zu. In Anbetracht dieses Risikos erscheint es richtig und zwingend, in diesem Punkt keine vom Recht der EU und der genannten Nachbarstaaten abweichende Haftungsregelung vorzusehen. Antrag: Ersatzlose Streichung von Art. 59a OR.	ISSS
Hinweis zur Neuformulierung von OR Art. 59a (implizite Beweislastumkehr): Im erläuternden Bericht wird bezüglich Haftung nach OR 59a ausgeführt: „Art. 59a Haftung für Signaturschlüssel: Die bisherige Haftung des Schlüsselinhabers für qualifizierte Zertifikate soll auch auf geregelte Zertifikate ausgedehnt werden, weil diese Haftung eine der essentiellen Grundlagen für die Akzeptanz beim Dritten ist; ohne diese Haftung wäre das geregelte Zertifikat in den Augen dessen, der sich darauf verlassen soll, wenig wert. Allerdings soll die Haftung auf Signatur-Anwendungen beschränkt sein und für Authentisierung oder weitere Anwendungen nicht gelten. Aus diesem Grund wird hier (in OR Art. 59a neu) der Begriff «Signaturschlüssel» NICHT durch den generellen Begriff «kryptografischer Schlüssel» ersetzt.“ Die Neufassung von OR Art. 59a, Abs. 1 im Entwurf lautet aber: „Der Inhaber eines geheimen kryptografischen Schlüssels (anstelle des Begriffs Signaturschlüssel in OR Art. 59a alt) haftet Drittpersonen für Schäden, die diese erleiden, weil sie sich auf ein gültiges geregeltes Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom … über die elektronische Signatur verlassen haben.“ Diese widersprüchliche Formulierung im Entwurf von OR Art. 59a lässt vermuten, dass für Authentisierung die gleiche Haftungsregelung (d.h. implizite Beweislastumkehr) wie für Signatur gilt. Dieser Widerspruch sollte beseitigt werden! Wir sind der Meinung, dass die Aussage im erläuternden Bericht im Gesetz klar zum Ausdruck kommt, wonach die Haftung im Sinne einer Beweislastumkehr auf Signatur-Anwendungen beschränkt ist.	CI AG

Den Inhaber der geheimen kryptographischen Schlüssel in die Haftung zu nehmen, ist nur sinnvoll, wenn auch die Drittperson in die Pflicht genommen wird. Daher erachten wir es als wichtig, dass im Gesetz alle Akteure und deren Rechte und Pflichten im Gesetz erwähnt sind. Sofern – wie in diesem Entwurf – die gesetzlich verankerte Sicherheitsanforderung herabgestuft wird, sollte dies in Haftungsklausel berücksichtigt werden.	Die Post
Wir erachten die durch das geltende ZertES eingeführte Gefährdungshaftung als einen der wesentlichen Gründe für die ungenügende Akzeptanz der elektronischen Signatur im Rechtsverkehr. Eine derartige Haftung der Schlüsselinhaber ist auch dem harmonisierten europäischen Signaturrecht fremd. Darüber hinaus stellt der in Art. 59a Abs. 2 und 3 OR vorgesehene Entlastungsbeweis hohe Anforderungen an den Schlüsselinhaber. Es ist nicht einzusehen, weshalb der Inhaber eines Signaturschlüssels, der auf einem qualifizierten Zertifikat beruht, einer strengeren Haftung unterstellt sein soll als die Anwender der von der Praxis entwickelten ungeregelten elektronischen Signaturmittel im Privatrechtsverkehr. Wir empfehlen daher, Art. 59a DR ersatzlos zu streichen.	SWICO
Da sich ein Nutzer der elektronischen Signatur eines der handschriftlichen Unterschrift gegenüber technisch überlegenen und genuin weniger missbrauchsanfälligen Unterschriftsmittels bedient, muss die Haftung keinesfalls erhöht sondern – wenn überhaupt – gesenkt werden.	PS
Wir erachten die durch das geltende ZertES eingeführte Gefährdungshaftung als einen der wesentlichen Gründe für die ungenügende Akzeptanz der elektronischen Signatur im Rechtsverkehr. Eine derartige Haftung der Schlüsselinhaber ist auch dem harmonisierten europäischen Signaturrecht fremd. Darüber hinaus stellt der in Art. 59a Abs. 2 und 3 OR vorgesehene Entlastungsbeweis hohe Anforderungen an den Schlüsselinhaber. Es ist nicht einzusehen, weshalb der Inhaber eines Signaturschlüssels, der auf einem qualifizierten Zertifikat beruht, einer strengeren Haftung unterstellt sein soll als die Anwender der von der Praxis entwickelten ungeregelten elektronischen Signaturmittel im Privatrechtsverkehr. Wir empfehlen daher, Art. 59a OR ersatzlos zu streichen.	SwissH
La modification de l'article 59a alinéa 1 du Code des obligations (ci-après CO) liée aux changements de la SCSE pose toutefois problème. Dans sa version nouvelle, cet article stipulera que 'Je titulaire d'une clé cryptographique privée répond envers les tiers des dommages que ces demiers ont subis parce qu'ils se sont fiés à un certificat réglementé valable délivré par un fournisseur de services de certification reconnu au sens de la loi (...)". La version actuelle du meme articele est plus précise: "Le titulaire d'une clé de signature répond envers (es tiers des dommages que ces derniers ont subis parce qu'ils se sont fiés à un certificat qualifié valable délivré per un fournisseur de services de certification reconnu au sens de la loi (...)" La révision de l'article 59a alinéa 1 CO note une volonté d'étendre la responsabitité des détenteurs de clés cryptographiques aux certificats réglementés. Ii est vrai que cette manière de faire renforcerait la légitimité et la solidité juridiques de la signature des entreprises et autorités. Le CC, à son article 14 alinéa 2bis révisé, continue toutefois à stipuler que seule "la signature électronique qualifiée (...) est assimilée la signature manuscrite' Vouloir mettre (es certificats qualifiés et régiementés sur un pied d'égalité dans l'article 59a alinéa 1 CO contredit l'article 14 alinéa 2bis CO. La CVCI préconise par consquent de préciser dans le nouvel article 59a alinéa 1 CO que la responsabilité n'est engagée que pour les certificats qualifiés. En conclusion, la CVCJ sautient la modification de la SCSE telle que proposée. Elle demande toutefois d'apporter des précisions de manière à limiter la responsabilité des titulaires de clés cryptographiques aux certificats qualifiés (art. 59a al. 1 nouveau CO)	CVCI

Artikel 14 OR "Eigenhändige Unterschrift"	
Die Idee, die qualifizierte Signatur mit einem Zeitstempeldienst zu versehen, ist weiterzuverfolgen. Zwar kann auch bei der eigenhändigen Unterschrift nicht festgestellt werden, wann genau sie angebracht wurde. Allerdings ist die eigenhändige Unterschrift gerade durch ihre Eigenhändigkeit besser gegen Fälschungen geschützt. Dieser Schutz entfällt bei der elektronischen Signatur. Aus diesem Grund begrüssen wir die Idee, die qualifizierte Signatur mit einem Zeitstempeldienst zu versehen, um Betrugs- und anderen Fälschungsszenarien vorzubeugen. Ob der Zeitstempel nun allerdings als zwingendes Erfordernis für die qualifizierte elektronische Signatur gemäss ZertES vorgesehen wird oder nur bei Bedarf im entsprechenden Sacherlass verlangt wird, spielt aus unserer Sicht keine zentrale Rolle.	ZH
Die vorgesehenen Anpassungen der ZertES-Revision sind insgesamt zeitgemäss und sinnvoll. Insbesondere die damit verbundene terminologische Bereinigung bei der Regelung der elektronischen Signatur in den verschiedenen Gesetzen und Verordnungen findet Zustimmung. Betreffend Zeitstempel sind wir damit einverstanden, dass das ZertES sich zu dieser Frage nicht äussert und erst die konkrete Anwendung bei Bedarf dieses Erfordernis stellt. Mit einer eigenhändigen Unterschrift soll eine elektronische Signatur demgegenüber nur gleichgestellt sein, wenn sie mit einem Zeitstempel versehen ist. Dementsprechend bevorzugen wir bei der Änderung von Artikel 14 Absatz 2b des Obligationenrechts den Variantenvorschlag mit obligatorischem Zeitstempel.	LU
Mit der Einführung einer "Behördensignatur" (geregelte elektronische Signatur) entsteht eine zusätzliche Signatur-Kategorie, welche neue, unerwünschte "Brüche" in der Rechtsordnung verursacht. Während für Prozesseingaben von Parteien künftig einfache geregelte Signaturen verwendet werden können (Art. 130 Abs. 2 VE-ZPO; Art. 110 Abs. 2 VE-StPO), bedarf es zur Schriftlichkeit nach Art. 14 Abs. 2bis VE-OR weiterhin einer qualifizierten geregelten Signatur. Elektronisch eingereichte Parteieingaben würden derselben nicht genügen. Die Variante von Art. 14 Abs. 2bis VE-OR, wonach die qualifizierten elektronischen Signaturen jeweils zwingend mit einem qualifizierten Zeitstempel zu versehen sind, wäre unseres Erachtens mit Blick auf die höhere Rechtssicherheit zu bevorzugen. Die (Beweis-)Problematik bei Verwendung lokaler Systemzeiten dürfte den meisten Verkehrsteilnehmern nicht bewusst sein. Zudem wäre auch eindeutig geklärt, welche Time Stamp Authorities (TSA) als vertrauenswürdig anzusehen sind.	SZ
Betreffend Zeitstempel unterstützen wir den Vorschlag, dass sich das ZertES selbst zu dieser Frage nicht äussert und erst die konkrete Anwendung bei Bedarf dieses Erfordernis anstellt, z.B. das OR für die Verwendung der elektronischen Signatur als Ersatz der eigenhändigen Unterschrift.	OW
Bei den Anpassungen im Obligationenrecht unterstützen wir in Artikel 14 Absatz 2bs die Variante “qualifizierte elektronischer Signatur mit obligatorischem Zeitstempel“.	GL
Wo das Gesetz die einfache Schriftform verlangt, ist die Angabe der Zeit grundsätzlich nicht erforderlich (vgl. BGE 95 II 432). Relevant ist somit die rechtsgültige digitale qualifizierte Unterschrift und nicht das Datum der Unterschrift. Auch bei der elektronischen Übermittlung von Eingaben und Entscheiden ist nicht der Zeitstempel der elektronischen Signatur massgebend für die Bestimmung des Fristablaufs bzw. für den Zeitpunkt der Mitteilung, sondern der Zeitpunkt, in dem eine anerkannte Zustellplattform oder das Informatiksystem der Behörde den Empfang der Eingabe bestätigt hat, bzw. der Zeitpunkt in dem der Entscheid durch die Adressatin oder den Adressaten heruntergeladen wird. Zwar könnten mit einem Zeitstempel Beweisprobleme, die sich gerade in Gerichtsverfahren immer wieder stellen, entschärft werden.	ZG

Ein obligatorischer offizieller Zeitstempel ist für die Bürgerin bzw. den Bürger jedoch nicht gratis, was der Akzeptanz elektronischer Signaturen abträglich ist. Hinzu kommt, dass man für die Einbettung eines Zeitstempels in die elektronische Signatur zum Zeitpunkt des Signierens mit dem Internet verbunden sein muss und daher allenfalls auch noch technische Probleme bei der Online-Anbindung zur offiziellen Zeitabfrage hinzukommen können. Wir bevorzugen daher Variante 1 ohne obligatorischem Zeitstempel, bei der ein solcher Zeitstempel durch entsprechende gesetzliche oder vertragliche Regelung vorbehalten werden kann. Antrag: Art. 14 Abs. 2bis OR sei der Bundesversammlung der Schweizerischen Eidgenossenschaft in der Variante ohne obligatorischen Zeitstempel zu unterbreiten.	
Was schliesslich die unter der Rubrik „Aufhebung und Änderung bisherigen Rechts“ vorgeschlagenen Varianten zu Art. 14 Abs. 2bis des Obligationenrechts anbelangt, favorisieren wir die Grundvariante ohne qualifizierten Zeitstempel.	TG
Riguarde alla revisione dell'articolo 14 capoverso 2'"® del Codice délie obbligazioni, prediligiamo la variante che contempla la firma elettronica qualificata con sistema marcatempo obbligatorie.	TI
Article 14 al. 2bis CO: la variante avec prise en compte de l'horodatage nous semble la seule souhaitable, car l'horodatage est essentiel dans plusieurs applications possibles de la signature électronique impliquant le respect des délais. Par, analogie, une des principales fonctions du cachet de la Poste, en particulier pour les recommandés, réside précisément dans son horodatage. Cet aspect est crucial pour le développement des transactions entre administrés et les autorités, notamment dans le cadre de la cyberadministration en ligne. Cette variante doit en outre impérativement s'appliquer à la signature réglementée et pas seulement à la signature qualifiée. Cela permettrait notamment d'harmoniser cette disposition avec l'art. 13 SCSE. En effet, il n'est pas logique de préconiser dans l'art. 13 SCSE l'horodatage qualifié pour la signature électronique réglementée tout en prônant à l'article 14, alinéa 2bis CO un horodatage qualifié pour la signature électronique qualifiée. Enfin, en limitant l'horodatage qualifié à la seule signature qualifiée, laquelle est exclusivement réservée aux personnes physiques (art. 8 al. 1 SCSE), on perd l'intérêt du nouveau certificat ouvert aux personnes morales, partant aux administrations, alors que le premier objectif poursuivi par la présente révision est justement d'introduire ce type de certificat, notamment dans le cas des opérations de masse.	GE
Nous nous opposons à la variante proposée à l‘article 14, alinéa 2bis, Co et privilégions la proposition principale, étant entendu que nous sommes favorables à ce que la SCSE rende elle-meme obligatoire l'horodatage (point 6 ci-dessus). La solution qui consisterait à ne pas rendre obligatoire l'horodatage par le biais de la SCSE, mais de l‘exiger dans une disposition du Code des obligations nous parait en effet piégeuse pour l‘utilisateur. La signature électronique quaiifiée ne serait pas automatiquement horodatée, et l‘utilisateur devrait lui-meme veiller à obtenir l‘horodatage de sa signature, respectivement de celle de son partenaire contractuel, pour que l‘acte soit valable en la forme écrite. Cela n'est pas satisfaisant: dès lors qu‘une personne utilise la signature électronique qualifiée, elle doit pouvoir sans autre admettre que es formes de l'article 14 CO sont respectées. il faut éviter dajouter des conditions supplémentaires.	JU

Das bestehende Bundesgesetz über die elektronische Signatur (ZertES) vom 19.12.2003 definiert die qualifizierte elektronische Signatur im Sinne einer eigenhändigen Unterschrift gemäss OR 14 Abs. 2bis. Es definiert die dazu notwendigen qualifizierten Zertifikate und regelt die zu erfüllenden Voraussetzungen für die Anerkennung von Zertifizierungsdienstanbieterinnen, welche qualifizierte Zertifikate ausstellen. Der Fokus des bestehenden ZertES ist somit ausgerichtet auf eine ganz bestimmte Anwendung von digitalen Zertifikaten, nämlich die elektronische Unterschrift, gleichgestellt der eigenhändigen Unterschrift gemäss OR 14, wenn eine solche überhaupt erforderlich ist.	CI AG
Das Anbringen eines qualifizierten Zeitstempel bedingt eine Online-Verbindung. Die Praxiserfahrung zeigt, dass diese Online-Verbindung nicht immer gegeben ist. Des Weiteren gibt es keinen Grund die Anforderung an eine Willensäusserung zu erhöhen, nur weil diese elektronisch geschieht. Daher empfehlen wir, auf einen obligatorischen Zeitstempel zu verzichten, d. h. die Variante 1 umzusetzen.	Die Post
Wie wir auch hierzu bereits 2001 festgehalten haben, erachten wir Zeitstempel als einen ganz wesentlichen Teil einer elektronischen Signatur. Diese sind bei einer längeren Aufbewahrung von ursprünglich gültigen digitalen Signaturen ohne Zeitstempel nämlich weitge hend nutzlos. Wir bevorzugen deshalb zu Art. 14 Abs. 2bis DR die Variante ‘qualifizierte elektronische Signatur mit obligatorischem Zeitstempel‘.	SWICO
Technologien für die Anwendung von Zeitstempeln haben abgesehen vom PDF Format noch keine Verbreitung gefunden sofern sie überhaupt existieren. Auch bewirkt eine Zeitstempelungspflicht, dass elektronische Signaturen nicht mehr „offline“ erstellt werden können. Aus diesem Grund ist die Pflicht jeder qualifizierten elektronischen Signatur einen qualifizierten Zeitstempel beizufügen aktuell abzulehnen. Allenfalls wäre eine Kann-Formulierung ins Auge zu fassen, nach der der Bundesrat die qualifizierten Zeitstempel zu einem späteren Zeitpunkt obligatorisch erklären könnte.	PS
SwissHoldings erachtet Zeitstempel als einen wesentlichen Teil der elektronischen Signatur. Diese sind bei einer längeren Aufbewahrung von ursprünglich gültigen digitalen Signaturen ohne Zeitstempel kaum werthaltig. Wir bevorzugen deshalb zu Art. 14 Abs. 2bis OR die Variante "qualifizierte elektronische Signatur mit obligatorischem Zeitstempel".	SwissH

Zivilprozessordnung	
Art. 130 ZPO: Streichung Abs. 3 (im Vernehmiassungsentwurf nicht vorgesehen) ~~Bei elektronischer Übermittlung kann das Gericht verlangen, dass die Eingabe und die Beilagen in Papierform nachgereicht werden.~~ Begründung: Die Kann-Vorschrift, dass das Gericht jede Eingabe samt Beilagen noch in Papierform nachfordern kann, behindert die Entwicklung des elektronischen Rechtsverkehrs und steht dem Ziel einer elektronischen Aktenführung, die es nach unserer Uberzeugung zum Durchbruch des ERV braucht, entgegen. Selbstredend schliesst diese Streichung nicht aus, dass ein Gericht die Vorlage einer Originalurkunde zu Beweiszwecken verlangt. Ebenso gehen wir mit den Erläuterungen zu den beiden VO über die elektronische Ubermittlung davon aus, dass ein Dokument auf Papier nachverlangt werden kann, wenn es elektronisch nicht lesbar oder nicht in nützlicher Form ausdruckbar ist. Dem kann durch entsprechende Formatvorgaben auf Verordnungsstufe begegnet werden. Art. 139 ZPO (SR 272): Änderung Abs. 1 (im Vernehmlassungsentwurt nicht vorgesehen) 1 ~~Mit dem Einverständnis~~ Auf Verlangen der betroffenen Person kannmuss jede Zustellung elektronisch erfolgen. Begründung: Es gilt das zu Art. 26 Abs. 1 bis und 34 Abs. ibis VwVG sowie zu Art. 60 BGG Gesagte. Anstelle von der “Partei“ wird hier von der “betroffenen Person“ gesprochen. Stossend erscheint dem SAV, dass es heute Kantone gibt, die gestützt auf Art. 139 Abs. 1 ZPO bzw. Art. 86 StPO erklären können, es erfolge keine elektronische Zustellung von Behördenmitteilungen an die Verfahrensbeteiligten, sondern die Gerichtsbehörden würden weiterhin auf herkömmlichem, postalischem Weg an die Parteien gelangen. Art. 143 ZPO: Änderung Abs. 2 Satz 1 (im Vernehmiassungsentwurf nicht enthalten) 2 Bei elektronischer Übermittlung ist die Frist eingehalten, ~~wenn der Empfang bei der Zustelladresse des Gerichts spätestens am letzten Tag der Frist durch das betreffende Informatiksystem bestätigt worden ist~~,wenn das anerkannte Informatiksystem, über welches die elektronische Zustelladresse des Gerichts erreichbar ist, spätestens am letzten Tag der Frist den Empfang bestätigt hat. Begründung: Auch diese Begründung entspricht jener für die Änderung von Abs. 3 von Art. 21a Abs. 2 VwVG. Ob man zur weiteren Koordination auch hier “vor ihrem Ablauf“ statt “spätestens am letzten Tag der Frist“ einsetzen will, lassen wir bewusst offen.	SAV
Art. 130 Abs. 2 ZPO: Sowohl für die Übermittlung von Parteieingaben im Zivilprozess, wie auch im Strafverfahren, wird neu die “geregelte elektronische Signatur“ verlangt. Dies ist zu begrüssen. Aufgrund der Erfahrungen mit dem ZertES 2003 dürfte dies jedoch nicht ausreichen, damit sich in der Praxis der elektronische Verkehr mit den Zivil- und Strafgerichten ohne grosse Einschränkungen und Verzögerungen durchsetzen wird. Antrag: Daher sollten verfahrensbeteiligte Private das Recht erhalten, die elektronische Kommunikation zu verlangen. Dies im Gegensatz zu der heutigen Praxis, welche die elektronische Kommunikation nur mit solchen Behörden erlaubt, welche der Aufnahme in eine entsprechende Liste zugestimmt haben. Dieser Grundsatz kann rasch, d.h. innert einer angemessenen Übergangsfrist, einfach und kostengünstig so umgesetzt werden, dass sich Behörden und Amtsstellen des Bundes im Sinne der vorstehenden Überlegungen (siehe vorne A.3) einer Zustellplattform anschliessen, welche elektronische Eingaben entgegen nimmt und in dem mit der betreffenden Behörde vereinbarten Format an diese weiterleitet, bzw. behördliche Mittelungen, Entscheide und Verfügungen an die Subjekte des Privatrechts zustellt. b) Weiter enthält die neue ZPO in Art. 143 Abs. 2 eine versteckte Falle für die Benutzer elektronischer Übermittlungsverfahren: Die Frist gilt nämlich nur dann als eingehalten, wenn der Empfang bei der Zustelladresse des Gerichts spätestens am letzten Tag der	ISSS

Frist durch das betreffende Informationssystem bestätigt worden ist. Damit trägt der Benutzer das ganze Risiko der elektronischen Übermittlung (Störungen, Unterbrechungen, Umleitungen, Verlust der elektronischen Sendung etc.) bis zum Eingang der Übermittlung in der Mailbox des Gerichts. Dies ist wesentlich ungünstiger als bei der konventionellen Zustellung von Eingaben durch Übergabe bei einer schweizerischen Poststelle. Dort ist die Frist eingehalten, wenn die Eingabe nach Schliessung der Postschalter vor namentlich bekannten Augenzeugen, welche den Vorgang bestätigen, am letzten Tag der Frist um 23:59 Uhr in den Briefkasten eingeworfen wird (BGE 115 la 8 f). Somit stellt sich die Frage, wer denn überhaupt noch, aufgrund solcher Unsicherheiten der Übermittlung, das Mittel der elektronischen Übermittlung wählen wird. Antrag: Um die Übereinstimmung mit der Postaufgabe herbeizuführen, ist die Bestimmung so abzuändern, dass die Eingabefrist nach Art. 143 ZPO bei elektronischer Ubermittlung eingehalten ist, wenn das System des Absenders (z.B. durch elektronischen Zeitstempel) bestätigt, dass die Sendung zu einem bestimmten Zeitpunktinnerhalb der Frist an die gültige elektronische Adresse des Gerichtes bzw. die bezeichnete Zustellplattform versandt worden ist.	
Art. 130 Abs. 2 Zivilprozessordnung (ZPO): Es ist nicht einsichtig, warum nicht eine qualifizierte Signatur gefordert wird. Folgende Formulierung könnte die Verständlichkeit, wann welcher Zertifikatstyp einzusetzen ist, erhöhen: Bei elektronischer Übermittlung muss die Eingabe mit einer qualifizierten elektronischen Signatur der Absenderin oder des Absenders versehen sein. Der Bundesrat bestimmt das Format der Übermittlung.	Die Post

SchKG	
Art. 33a SchKG: Änderung Abs. 2 Satz 1 (im Vernehmiassungsentwurf nicht enthalten) 2 ~~Das Dokument, das die Eingabe und die Beilagen enthält, muss mit einer anerkannten elektronische Signatur~~ Bei elektronischer Ubermittlung muss die Eingabe mit einer geregelten elektronischen Signatur der Absenderin oder des Absenders versehen sein. Begründung: Auch Art. 33a SchKG, der im Vernehmlassungsentwurf nicht erwähnt ist, muss gleichermassen wie Art. 130 Abs. 1 ZPO und Art. 110 Abs. 1 StPO an die die neue Terminologie der geregelten Signatur angepasst werden. Streichung Abs. 3 (im Vernehmiassungsentwurf nicht vorgesehen) ~~Die Betreibungs- und Konkursämter und die Aufsichtsbehörden können verlangen, dass die Eingabe und die Beilagen in Papierform nachgereicht wird.~~ Begründung: Zur Begründung dieses Vorschlags gilt das zur Streichung von Abs. 3 von Art. 130 ZPO und Art. 110 Abs. 2 letzter Satz StPO Gesagte. Art. 34 SchKG: Änderung Abs. 2 Satz 1 (im Vernehmlassungsentwurf nicht vorgesehen) 2 ~~Mit dem Einverständnis~~ Auf Verlangen der betroffenen Person kannmuss jede Zustellung elektronisch erfolgen. Begründung: Der Wortlaut entspricht genau jenem der vorgeschlagenen Änderung von Art. 139 Abs. 1 ZPO und Art. 86 StPO. Eine zusätzliche Begründung erübrigt sich deshalb auch hier. Die Verordnungskompetenz des Bundesrats bleibt unangetastet.	SAV

Strafprozessordnung	
Art. 86 StPO: Änderung (im Vernehmlassungsentwurf nicht vorgesehen) ~~Mit dem Einverständnis~~ Auf Verlangen der betroffenen Person (kann)muss jede Zustellung elektronisch erfolgen. Begründung: Der Wortlaut entspricht jenem der vorgeschlagenen Änderungen von Art. 139 Abs. 1 ZPO und Art. 34 Abs. 2 Satz SchKG. Auf die vorstehenden Begründungen wird verwiesen. Allenfalls könnte die Vorschrift wie in Art. 34 Abs. 2 Satz SchKG mit einem Hinweis auf die bundesrätliche Kompetenz für Detailregelungen ergänzt werden.	SAV
Art. 110 StPO: Streichung Abs. 2, letzter Satz (im Vernehmiassungsentwurf nicht vorgesehen) 2 ~~Die Strafbehörde kann verlangen, dass die Eingabe in Papierform nachgereicht wird.~~ Begründung: Zur Begründung dieses Vorschlags gilt das zur Streichung von Abs. 3 von Art. 130	SAV
StPO Art. 110 Abs. 2: a) Sowohl für die Übermittlung von Parteieingaben im Zivilprozess, wie auch im Strafverfahren, wird neu die "geregelte elektronische Signatur" verlangt. Dies ist zu begrüssen. Aufgrund der Erfahrungen mit dem ZertES 2003 dürfte dies jedoch nicht ausreichen, damit sich in der Praxis der elektronische Verkehr mit den Zivil- und Strafgerichten ohne grosse Einschränkungen und Verzögerungen durchsetzen wird. Antrag: Daher sollten verfahrensbeteiligte Private das Recht erhalten, die elektronische Kommunikation zu verlangen. Dies im Gegensatz zu der heutigen Praxis, welche die elektronische Kommunikation nur mit solchen Behörden erlaubt, welche der Aufnahme in eine entsprechende Liste zugestimmt haben.	ISSS
Art. 110 Abs. 2 StPO: Es ist nicht einsichtig, warum nicht eine qualifizierte Signatur gefordert wird. Folgende Formulierung könnte die Verständlichkeit, wann welcher Zertifikatstyp einzusetzen ist, erhöhen: Bei elektronischer Übermittlung muss die Eingabe mit einer qualifizierten elektronischen Signatur versehen sein. Der Bundesrat bestimmt das Format der Übermittlung. Die Strafbehörde kann verlangen, dass die Eingabe in Papierform nachgereicht wird.	Die Post
ATSG (AT Sozialversicherungsrecht)	
Art. 38 ATSG (SR830.1): Änderung Abs. 2bis (im Vernehmlassungsentwurf nicht vorgesehen) 2 Eine Mitteilung, die nur gegen Unterschrift des Adressaten oder der Adressatin oder einer anderen berechtigten Person beziehungsweise gegen eine gleichwertige elektronische Empfangsbestätigung überbracht wird, gilt spätestens am siebenten Tag nach dem ersten erfolglosen Zustellungsversuch als erfolgt. Begründung: Es gilt auch hier die Begründung zur Änderung von Art. 20 Abs. 2bis VwVG sowie zu Art. 44 Abs. 2 BGG.	SAV

Ergänzende Bestimmungen	
Gleich wie beim heute geltenden ZertES bleibt es ein wichtiges Ziel des Gesetzesentwurfes, ein breites Angebot an sicheren Zertifizierungsdiensten zu fördern. Ausgehend von diesem Ziel ist aus Sicht des Datenschutzes nicht nur die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift von Bedeutung, sondern auch (oder gerade) die hierbei zu Grunde liegende Technologie und deren Förderung. Kryptographische Verfahren gewährleisten Vertraulichkeit, Integrität und Authentizität beim elektronischen Geschäftsverkehr. Sie dienen damit zentralen Anliegen des Datenschutzes. Die rasante technologische Entwicklung führt nicht nur im Bereich der Kryptographie zu immer neueren und sichereren Verfahren, sondern eröffnet auch potenziellen Angreifern immer neue Möglichkeiten, vorhandene Verschlüsselungen oder Sicherheitsmechanismen aufzubrechen oder zu umgehen. Im Bereich der Kryptographie muss die Forschung deshalb laufend mögliche Angriffe antizipieren und wirksame Gegenmassnahmen entwickeln. In Anbetracht der Wichtigkeit der kryptographischen Verfahren für die Erreichung der gesetzlichen Ziele und für den Datenschutz wäre es angemessen, auch die Förderung der Weiterentwicklung dieser Verfahren in das Gesetz aufzunehmen. Dafür wären weniger Mittel notwendig als für die Entwicklung und Vermarktung von Zertifizierungsdienstleistungen für den Privatrechtsverkehr, und sie wären erst noch sinnvoller investiert. <u>Vorschlag ergänzende Bestimmung für den Bereich der Kryptologie</u> Wir regen an, die Forschung und Entwicklung im Bereich der Kryptographie durch spezifische (zweckgebundene) finanzielle Beiträge oder durch andere Massnahmen gezielt zu fördern und eine entsprechende Bestimmung in den Gesetzesentwurf aufzunehmen.	SZ
Die Nichteinhaltung der Vorschriften des ZertES, beispielsweise durch Anbieterinnen von Zertifizierungsdiensten, muss angesichts des hohen Risikos nicht nur eines finanziellen, sondern auch eines volkswirtschaftlichen Schadens nebst haftungs- auch strafrechtliche Folgen haben. Dazu bedarf es der Einfügung einer spezialgesetzlichen Strafnorm. <u>Antrag</u>: Es sei ein neuer Artikel mit einer Strafandrohung bei Zuwiderhandlung gegen die Bestimmungen des ZertES einzufügen.	ZG
EID-IV, GeBüv und Verwaltungsrecht: Es fehlen Anwendungsbestimmungen für die EID-IV, GeBüv und das Verwaltungsrecht.	Die Post

Keine Bemerkungen	
Begrüssen die Vorlage und verzichten auf eine detaillierte Stellungnahme.	UR
Nach Anhörung des Volkswirtschaftsdepartementes, des Departementes des Innern und des Finanzdepartementes sowie des Kantonsgerichtes teilen wir Ihnen mit, dass wir keine Bemerkungen zur Vorlage haben.	SG
Nach Durchsicht der Unterlagen können wir Ihnen mitteilen, dass die Regierung des Kantons Graubünden mit der geplanten Revision des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur einverstanden ist und auf eine Stellunnahme verzichtet.	GR
Die SP Schweiz verzichtet auf die Einreichung einer Vernehmlassungsantwort zum Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur. Persönlich gehe ich nach einer gründlichen Durchsicht der Unterlagen nicht davon aus, dass es von unserer Seite her Einwände gegen die Vorlage geben wird.	SP
Nach Durchsicht des erläuternden Berichts teilen wir Ihnen mit, dass der SGV auf die Abgabe einer inhaltlichen Stellungnahme zur Totalrevision von ZertES verzichtet.	SGV
Da diese Frage gemäss Arbeitsteilung mit economiesuisse — Verband der Schweizer Unternehmen — in dessen Zuständigkeitsbereich fällt, verzichten wir auf eine eigene Eingabe. Wir schliessen uns indessen vollumfänglich der Stellungnahme des Verbandes der Schweizer Unternehmen an.	Arbeitgeber
Wir danken für die Gelegenheit, uns zu dieser Vorlage äussern zu können. Leider sehen wir uns aber aufgrund unserer beschränkten Ressourcen zeitlich nicht in der Lage, uns eingehend damit auseinanderzusetzen. Wir müssen daher leider auf eine Stellungnahme verzichten. Wir danken Ihnen für Ihr Verständnis.	KV Schweiz
Die IG lOT Zürcher Gemeinden begrüsst die schweizweite, verbindliche Regelung der elektronischen Signaturen sowie der entsprechenden Schlüssel und Zertifikate. Unsererseits gibt es keine fachlichen Einwände gegen das Gesetz. Wir empfehlen jedoch, nebst dem schweizerischen Bundesgericht weitere Gerichte sowie die Betreibungsämter zur Vernehmlassung einzuladen. Diese Stellen sind von der neuen Regelung stark betroffen, da sie bereits heute eine grosse Anzahl vertraulicher Dokumente austauschen.	IG ICT