

Gesetzgebungspaket zur Förderung des elektronischen Geschäftsverkehrs

Bericht über die Abklärung des Regelungsumfangs

Ergebnis	Bericht über die Abklärung des Regelungsumfangs (Studie)
Klassifizierung *	nicht klassifiziert
Status **	Abgeschlossen
Projektname	Gesetzgebungspaket zur Förderung des elektronischen Geschäftsverkehrs
Projektabkürzung	GP-FeGV
Projektleiter	U. P. Holenstein
Auftraggeber	D. Gruber
Autor	Holenstein/Bürge (HUP/BUE)
Prüfende	Agr. AUGABES

* Nicht klassifiziert, Intern, Vertraulich

** In Arbeit, In Prüfung, Abgeschlossen

Änderungskontrolle, Prüfung, Genehmigung

Version	Datum	Beschreibung, Bemerkung	Name oder Rolle
0.2	30.04.2012	Bereinigter Entwurf für 1. Sitzung Arbeitsgruppe	HUP / BUE
0.5	15.06.2012	Erster offizieller Entwurf für 3. Agr.-Sitzung	HUP / BUE
0.6	14.08.2012	Vollständiger Entwurf für 4. Agr.-Sitzung	HUP / BUE
0.7	14.09.2012	Gemäss 4. Agr.-Sitzung überarbeitete Version	HUP / BUE
0.8	21.09.2012	Vollständiger Entwurf für Ämterkonsultation	HUP / BUE
1.0	29.10.2012	Version nach Ämterkonsultation	HUP / BUE

Definitionen, Akronyme und Abkürzungen

Wort	Bedeutung
BAKOM	Bundesamt für Kommunikation
BJ	Bundesamt für Justiz
BRB	Bundesratsbeschluss
eCH	Verein für E-Government- und E-Health-Standards für die Schweiz (www.ech.ch)
eID (-Funktion)	Elektronische Identität (s-Funktion); Set von identifizierenden Attributen inklusive der Verfahren zum Beweis dieser Identität (Authentisierung)
IAM	Identity und Access Management; Identitätsmanagement; System für die Verwaltung von Identitäten und dem Zugriff auf Dienste
ISB	Informatik-Steuerungsorgan Bund, im EFD
SR	Systematische Rechtsammlung (www.admin.ch/ch/d/sr/sr.html)
STORK	„Secure Identity Across Borders Linked“ (https://www.eid-stork.eu/); EU-Projekt zur grenzüberschreitenden Authentisierung mit eID-Karten.
VeÜ-VwV	Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens vom 18. Juni 2010, SR 172.021.2
VeÜ-ZSSV	Verordnung über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren vom 18. Juni 2010, SR 272.1
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektr. Signatur; SR 943.03
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (SR 210)

Zweck des Dokuments

Gemäss Ziffer 6 des Bundesratsbeschlusses vom 28. März 2012 wird das EJPD beauftragt, zusammen mit der BK, dem VBS, dem EFD, dem EVD und dem UVEK den Umfang einer umfassenden Gesetzgebung im Anwendungsbereich der elektronischen Signatur abzuklären und dem Bundesrat bis Ende 2012 einen Vorschlag zum weiteren Vorgehen zu unterbreiten.

Die vorliegende Studie fasst die Überlegungen der mit dieser Abklärung befassten bundesinternen Arbeitsgruppe zusammen, welche bei der Klärung der Ziele und Einflussfaktoren, beim Sammeln, Bewerten und Strukturieren des Themas und beim Entwickeln der Lösungsvarianten und Abgrenzungen angestellt wurden.

Während der Arbeit der Arbeitsgruppe diente das Dokument als Gefäss für die Diskussion des Themas, nach Abschluss dokumentiert es die wichtigsten Überlegungen und Schlüsse als Beilage zum formellen Antrag an den Bundesrat.

Inhaltsverzeichnis

Definitionen, Akronyme und Abkürzungen.....	2
Zweck des Dokuments.....	2
1 Zusammenfassung.....	4
2 Auftrag, Problemstellung, Ziele.....	5
3 Quellen für Regelungsbedarf.....	6
3.1 Die einzelnen Quellen und ihre Hauptforderungen im Überblick	6
3.1.1 Priorisierte Vorhaben B1.02: Rechtsgrundlagen für E-Government in der Schweiz	6
3.1.2 SECO-Analyse zu Sicherheit und Vertrauen im elektronischen Geschäftsverkehr	6
3.1.3 Aktueller Entwurf für ein deutsches E-Government-Gesetz	7
3.1.4 Sechs ‚key enablers‘ aus EU-Studie ‚Digitizing Public Services in Europe‘.....	7
3.1.5 Weitere Quellen.....	8
3.2 Vorschlag für eine EU-Verordnung über elektr. Vertrauensdienste im Besonderen.....	8
3.3 Überblick über Themenfelder	10
3.4 Gliederung der Themen	11
4 Förderlicher Rechtsrahmen für den elektronischen Geschäftsverkehr als Kernthema des Gesetzgebungsvorhabens	13
4.1 Prozess-Modell des elektronischen Geschäftsverkehrs	13
4.2 Infrastruktur-Modell des elektronischen Geschäftsverkehrs.....	14
4.3 Ordnungspolitische Betrachtung des Regelungsbedarfs	14
5 Die einzelnen Gesetzgebungspakete.....	16
5.1 Anpassung des ZertES an die Nachfolge-Verordnung der EU-Signatur-Richtlinie	16
5.2 Konzept und Rechtsrahmen für eine staatliche elektronische Identität (eID)	17
5.3 Komplettierung und Harmonisierung der Zustell-Gesetzgebung	19
5.4 Gesetz zur Zertifizierung von elektronischen Mail-Diensten („CH-Mail“)......	20
5.5 Erweiterung der Dokument-Formen („Textform“)......	20
5.6 Regelung der e-Apostille gemäss Haager Konferenz.....	21
5.7 Gesetzgebung zur Zertifizierung von elektr. Aufbewahrungs-Diensten („eSafe“)......	21
5.8 Einführung der obligatorischen elektronischen Rechnungsstellung.....	21

1 Zusammenfassung

Im Kontext der Freigabe der Revision des ZertES zur Vernehmlassung mit BRB vom 28. März 2012 wurde darüber diskutiert, ob die vorgeschlagene Revision zielführend sei oder ob nicht vielmehr eine breite E-Government-Gesetzgebung notwendig wäre. Der Bundesrat hat sich dafür entschieden, die schon lange diskutierten und minimalen Verbesserungen am ZertES in einem ersten Revisionspaket separat in die Vernehmlassung zu schicken. Er hat aber im gleichen BRB dem EJPD den Auftrag erteilt, zusammen mit der BK, dem VBS, dem EFD, dem EVD und dem UVEK den *Umfang einer umfassenden Gesetzgebung im Anwendungsbereich der elektronischen Signatur abzuklären* und dem Bundesrat bis Ende 2012 einen *Vorschlag zum weiteren Vorgehen* zu unterbreiten.

Für diese Abklärungen wurde unter Leitung des BJ eine Arbeitsgruppe mit Vertretungen von FEDPOL, GS VBS, ISB, ESTV, BIT, SECO und BAKOM gebildet. Um eine möglichst umfassende Sicht auf mögliche Regelungs-Inhalte zu erhalten, wurden in einer ersten Phase zahlreiche nationale und internationale Untersuchungen und Vorhaben im Bereich Informationsgesellschaft, E-Business und E-Government bezüglich Forderungen nach gesetzlichen Regelungen ausgewertet. Anschliessend wurden die gesammelten Forderungen verglichen, bewertet, strukturiert und priorisiert.

Als Zentrum und als verbindendes Glied des gesamten Gesetzgebungspaketes wurde das Ziel erkannt, *dafür zu sorgen, dass alle vom Staat geforderten Elemente für einen raschen und flächendeckenden Übergang zum elektronischen Geschäftsverkehr zwischen Privaten und mit Behörden bereitstehen.*

Die sachlogische und systematische Gliederung des Gesetzgebungs-Bedarfs führte zur nachstehenden Liste von einzelnen zu schaffenden Regelungen:

1. Anpassung der schweizerischen Gesetzgebung (ZertES) an die EU-Verordnung zur Ablösung der Signatur-Richtlinie (mit den beiden Schwerpunkten: Gegenseitige Anerkennung von elektronischen Identifikationen und Regelung verschiedener elektronischer Vertrauens-Dienste).
2. Ausarbeitung des Konzepts und der rechtlichen Regelung für ein zusammen mit der neuen Identitätskarte angebotenes, international anerkanntes elektronisches Identifizierungsmittel (eID).
3. Komplettierung und Harmonisierung der Zustell-Gesetzgebung zur Regelung der wichtigsten und juristisch relevanten Elemente der Übermittlung, wie Vertraulichkeit, Nachweise der Zustellung und des Empfangs, inkl. Zeitpunkte, etc.
4. Schaffung einer Regelung zur Zertifizierung von E-Mail-Diensten und ihren Anbietern.
5. Erweiterung der Dokument-Formen um eine ‚Textform‘ im schweizerischen Recht.
6. Schaffung einer Regelung für eine e-Apostille gemäss Haager Konferenz
7. Schaffung einer Regelung zur Zertifizierung von Aufbewahrungs-Diensten (‚eSafe‘)
8. Einführung der obligatorischen elektronischen Rechnungsstellung an Bundesbehörden

2 Auftrag, Problemstellung, Ziele

Der Auftrag für die vorliegende Abklärung leitet sich aus Ziffer 6 des Bundesratsbeschlusses (BRB) vom 28. März 2012 ab, welche lautet: Das EJPD wird beauftragt, zusammen mit der BK, dem VBS, dem EFD, dem EVD und dem UVEK 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 Hauptgegenstand des erwähnten BRB war die Eröffnung der Vernehmlassung zum Vorentwurf für eine *Revision* des Bundesgesetzes über die elektronische Signatur (ZertES). Während diese Revision eher minimal konzipiert war, sollten mit dem Auftrag in Ziffer 6 die ersten Arbeiten für eine weit umfassendere, aber auch längerfristig angelegte Gesetzgebung eingeleitet werden.

In der aktuellen Phase geht es also darum, das Feld dieses neuen, *umfassenden* Gesetzgebungsvorhabens auszuleuchten und Vorschläge für sinnvolle Pakete zu erarbeiten. Dabei ist zu berücksichtigen, dass ein erfolgversprechendes Gesetzgebungs-Paket ganz verschiedene Anforderungen erfüllen muss. Es muss insbesondere einem wichtigen und vertretbaren Bedürfnis entsprechen, einen sachlogischen Zusammenhang aufweisen und politisch richtig liegen.

Schon allererste Überlegungen zeigten, dass selbst der Kern des Vorhabens nicht völlig klar ist. Im Auftrag ist in materieller Hinsicht der ‚Anwendungsbereich der elektronischen Signatur‘ vorgegeben. Weitere Hinweise dürfte die Stellungnahme der verwaltungsinternen Redaktionskommission (VIRK) im Rahmen der Ämterkonsultation zum Vorentwurf der ZertES-Revision liefern, die den Anlass zur Aufnahme des Auftrags in den BRB bildete.

Wenn man die hauptsächliche Motivation für die bisherigen Gesetzgebungsarbeiten zum ZertES bezieht, so könnte in einer ersten Annäherung etwa nachstehend formulierte Zielsetzung den Kern und auch die materielle Klammer für das hier zu definierende Gesetzgebungsvorhaben bilden:

*Einen Rechtsrahmen schaffen,
der die elektronische Abwicklung von Geschäften
umfassend ermöglicht und unterstützt.*

Der hier angesprochene elektronische Geschäftsverkehr umfasst gleichermaßen Geschäfte zwischen Privaten (E-Business mit Business-to-Business und Business-to-Consumer) wie auch den Behördenverkehr (E-Government mit Government-to-Business und Government-to-Citizen). Die meisten Infrastrukturen und Dienste für einen sicheren elektronischen Geschäftsverkehr sind in beiden Bereichen gleichermaßen notwendig und nützlich.

Dies vorausgesetzt, besteht der Abklärungsauftrag nun primär noch darin, unter Anwendung der vorstehend erwähnten Eckpunkte das ganze Feld der Bedürfnisse und Erwartungen an den Gesetzgeber in diesem Bereich zu erheben, zu bewerten, zu strukturieren und in sinnvolle, machbare Gesetzgebungspakete zusammenzufassen.

3 Quellen für Regulierungsbedarf

Nebst dem vorstehend erwähnten BRB und seinen Materialien gibt es eine Reihe von weiteren Vorhaben, Strategien, Studien und anderen Elementen, die bei der Frage nach dem Inhalt des Gesetzgebungs-Pakets beigezogen werden können, weil sie im thematischen Umfeld Forderungen nach Erlassen oder nach staatlich regulierten Infrastrukturen gestellt haben.

3.1 Die einzelnen Quellen und ihre Hauptforderungen im Überblick

Nachstehend werden einige der wichtigeren Quellen kurz mit ihren wesentlichen Inhalten aufgeführt. Ein besonders wesentlicher Input, nämlich der aus der Revision der europäischen Signatur-Richtlinie entstandene Vorschlag für eine ‚Electronic Trust Service Regulation‘, wird nachstehend in einem separaten Kapitel behandelt.

3.1.1 Priorisierte Vorhaben B1.02: Rechtsgrundlagen für E-Government in der Schweiz

Im Mai 2012 wurden die Arbeiten in diesem Vorhaben mit einem Abschlussbericht über Lösungsansätze und Massnahmen abgeschlossen. Von den untersuchten Themen und vorgeschlagenen Massnahmen passen einige in den Kontext dieses Gesetzgebungsverfahrens:

- **Textform:** Schaffung einer weiteren Form von Dokumenten zwischen Formlosigkeit und Schriftform. Eine bedeutende Barriere für den elektronischen Geschäftsverkehr ist immer wieder die Tatsache, dass in der Schweiz ‚unterhalb‘ der Schriftform keine Form mit einer definierten rechtlichen Bedeutung existiert. Ein Schriftstück ohne Unterschrift, ein E-Mail, ein Gespräch und Rauchzeichen sind in dieser Hinsicht alle gleichwertig. Dies bedeutet, dass im elektronischen Geschäftsverkehr die unterste juristisch definierte Form die elektronische Signatur nach ZertES ist, was eine sehr hohe Hürde darstellt. Diese juristische ‚Bedeutungslosigkeit‘ aller anderen Formen steht auch in deutlichem Kontrast zur täglichen Praxis, wo gerade E-Mails im Geschäftsverkehr eine grosse Bedeutung zukommt. Als ein mögliches Modell steht hier die ‚Textform‘ nach deutschem Recht, [§ 126b BGB](#) zur Verfügung.
- **Zustellungs-Gesetz:** Sowohl im privaten Geschäftsverkehr wie auch im Behördenverkehr hat sich durch die Entwicklung der Technik auf der einen Seite und durch die Liberalisierung der Postdienste auf der anderen Seite die Situation bezüglich der sicheren und rechtsgültigen Zustellung von Dokumenten wesentlich geändert, ohne dass die diesbezüglichen rechtlichen Regelungen genügend nachgezogen haben. Wichtige und juristisch relevante Elemente der Übermittlung, wie Vertraulichkeit, Zustellungsbestätigung und Abgrenzung der Zuständigkeiten bzw. der Haftung sind unter Einbezug der neuen Akteure und Techniken zu regeln.
- **Regelung Trägerwandel:** Der in den nächsten Jahren des Übergangs zur elektronischen Abwicklung von Geschäften noch sehr oft und in den verschiedensten ‚Branchen‘ benötigte Trägerwandel von Papierdokumenten zu elektronischen Dokumenten und umgekehrt soll durch Vorgaben und Standards schweizweit möglichst einheitlich geregelt werden. Durch einheitliche Normen, Standards und eine gemeinsame Terminologie entstehen grosse Synergien sowohl in der Ausbildung wie auch für die Anbieter von Systemen.

3.1.2 SECO-Analyse zu Sicherheit und Vertrauen im elektronischen Geschäftsverkehr

Das SECO hat in den letzten Jahren im Kontext seiner Arbeiten für eine E-Business-Strategie verschiedentlich die fehlenden Elemente für die Durchsetzung des elektronischen Geschäftsverkehrs (eGV) ausgeleuchtet und dabei u.a. ein Modell für einen sicheren eGV und einen Katalog von ‚e-Essentials‘ entwickelt.

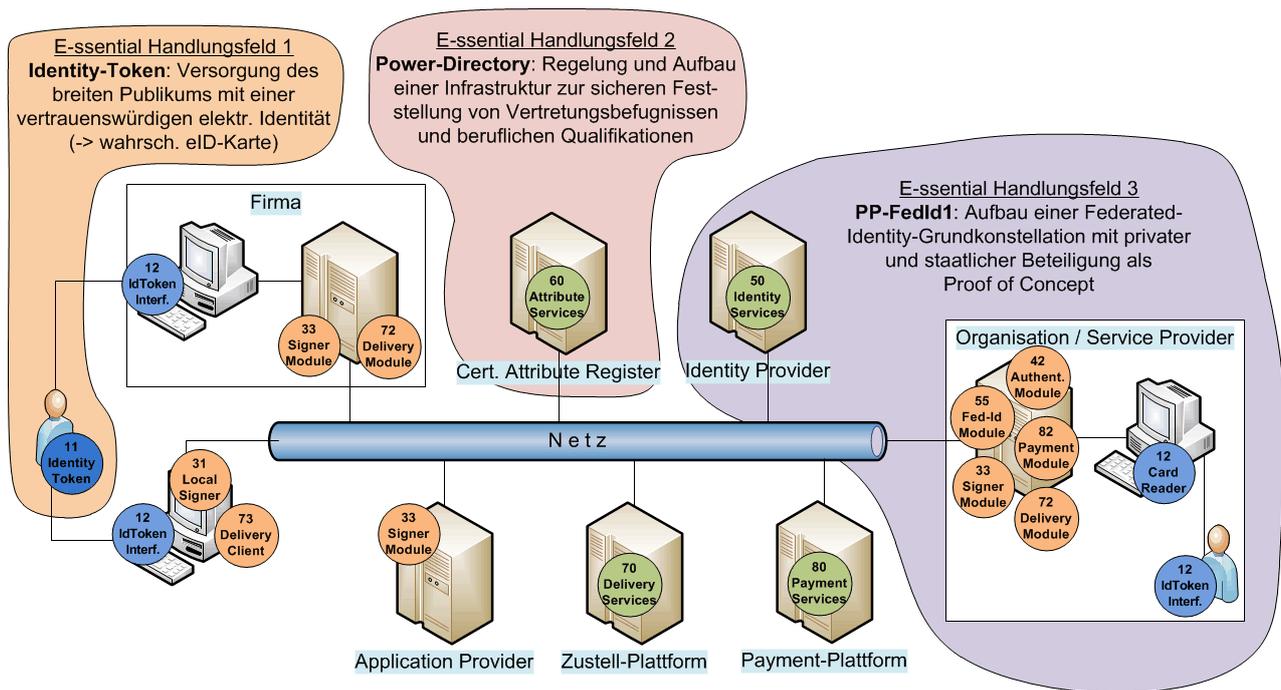


Abbildung 1: Die drei Handlungsfelder gemäss E-Business-Strategie des SECO, Stand 2009

3.1.3 Aktueller Entwurf für ein deutsches E-Government-Gesetz

In Deutschland laufen aktuell Gesetzgebungsarbeiten für ein E-Government-Gesetz, das insbesondere auf die flächendeckende Durchsetzung des elektronischen Behördenverkehrs abzielt und daher in diesem Kontext von Interesse ist. Als Zielsetzung sollen ‚*Rechtsunsicherheit beseitigt werden um innovative elektronische Verwaltungsdienste zu ermöglichen*‘. Da die geltenden Schriftformerfordernisse als Haupthindernis für die Durchsetzung des elektronischen Behördenverkehrs angesehen werden, sollen wo immer möglich die Anforderungen an die Form herabgesetzt werden. Zurzeit liegt ein sogenannter [Expertenentwurf](#) mit Bearbeitungsstand 5.3.2012 vor. Die wichtigsten Postulate¹ im Kontext unseres Vorhabens sind:

- **Aufhebung von Schriftform-Erfordernissen** wo immer möglich;
- Eingaben auf Web-Formularen unter Benutzung des neuen elektronischen Personalausweises ([eID-Funktion](#)) für eine sichere Identifikation
- **Eingaben und Zustellungen über DE-Mail**, die gesetzlich geregelten E-Mail-Dienste mit technisch und juristisch sicheren Beweis-Funktionen.

3.1.4 Sechs ‚key enablers‘ aus EU-Studie ‚Digitizing Public Services in Europe‘

Die Studie der EU von 2010² befasst sich über weite Teile mit den Erfordernissen für eine gedeihliche Entwicklung des elektronischen Geschäftsverkehrs bzw. Behördenverkehrs. Auf Seite 113 nennt sie die

¹ Eine kurze, übersichtliche [Zusammenstellung](#) der wichtigsten Inhalte des Gesetzes-Entwurfs findet sich aktuell auf der entsprechenden Seite des Bundesministerium des Innern (BMI).

² [Digitizing Public Services in Europe](#): Putting ambition into action; 9th Benchmark Measurement, December 2010, European Commission, Directorate General for Information Society and Media.

folgenden 6 ‚key enablers‘ oder ‚horizontal building blocks‘ (aus einem Katalog von 9) als *conditio sine qua non* für Fortschritte im E-Government:

- **Authentic Sources** (staatliche Basis-Register)
- Secure and Formal Delivery (**eDelivery**)
- **eIdentity** („government-issued document for online identification and authentication“)
- **Single Sign On** (SSO)
- Electronic Save (**eSave**, a legally recognized system for secure storage of electr. documents)
- **ePayment**

3.1.5 Weitere Quellen

Nebst den vorgängig einzeln aufgeführten Quellen wurden zahlreiche weitere Vorhaben und Publikationen aus der Schweiz und aus dem Ausland im Hinblick auf möglichen Regelungsbedarf mehr oder weniger intensiv ausgewertet, darunter insbesondere:

- o Verschiedene Strategie-Dokumente und Berichte aus der [Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz](#), deren Sekretariat im BAKOM angesiedelt ist.
- o Strategie-Dokumente, Berichte und Vorhaben-Verzeichnisse aus dem Umfeld der [E-Government-Strategie Schweiz](#)
- o E-Government-Gesetze verschiedener Kantone und ausländischer Staaten. Wobei E-Government-Gesetze sehr verschiedene Stossrichtungen und Inhalte aufweisen können und oft sehr spezifisch ausgerichtet sind, z.B. auf den Betrieb von gemeinsamen Infrastrukturen oder auf die elektronische Publikation.
- o Das [European Interoperability Framework](#)‘ (EIF), ein Architektur- und Standardisierungs-Vorhaben der EU für die Kommunikation zwischen Behörden, Wirtschaft und Privaten, das inzwischen beendet ist aber einige einschlägige [Studien und Architektur-Dokumente](#) hinterlassen hat.

3.2 Vorschlag für eine EU-Verordnung über elektr. Vertrauensdienste im Besonderen

Die gemeinsame europäische Regelung der elektronischen Signatur und ihrem Umfeld, bisher enthalten in der europäischen Richtlinie 1999/93/EG über ‚gemeinschaftliche Rahmenbedingungen für elektronische Signaturen‘³, war für die Schweiz immer von besonderer Bedeutung. Im Bewusstsein, dass elektronischer Verkehr von seiner Natur her die nationalen Grenzen leicht sprengen kann und dass daher künftig eine Interoperabilität mit den wichtigsten Handelspartnern wichtig sein würde, versuchte man von Beginn weg, das ZertES wo immer möglich kompatibel mit der Richtlinie zu gestalten und so eine spätere gegenseitige Anerkennung zu erleichtern.

Aus der laufenden Revision der europäischen Signatur-Richtlinie ist ein Verordnungs-Entwurf geworden. Am 4. Juni 2012 hat die Kommission den ‚**Vorschlag** für eine Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt‘⁴ zuhanden des Parlaments und des Rats verabschiedet und in Englisch, Französisch und Deutsch [publiziert](#). Eine zuge-

³ [ABl. L 13 vom 19.1.2000, S. 12](#) oder [Sammlung mit verschiedenen Sprachversionen auf EUR-Lex](#).

⁴ Englischer Titel: ‚Regulation on electronic identification and trusted services for electronic transactions in the internal market‘.

hörige [Pressemitteilung](#) fasst die wichtigsten Absichten und Inhalte der Regelung in allen offiziellen Sprachen der EU zusammen.

Hinweise zum Regelungsbedarf und -umfang ergaben sich aus der öffentlichen Konsultation zu den Themen elektronische Identifikation, Authentisierung und Signatur, welche die Europäische Kommission im Kontext der ‚Digital Agenda for Europe 2‘⁵ im Frühjahr 2011 mit dem Ziel durchführte, Vorgaben für die Anpassung der Signatur-Richtlinie zu erhalten.

Bemerkenswert ist, dass die neue Regelung nun nicht mehr eine Richtlinie wäre, sondern eine in den Mitgliedsländern direkt anwendbare Verordnung (E: ‚Regulation‘). Als primäre Legitimation für die Regelung wird an zahlreichen Stellen immer wieder ihre Notwendigkeit für die Durchsetzung des europäischen (‚digitalen‘) Binnenmarktes aufgeführt.

In inhaltlicher Hinsicht geht der Verordnungsvorschlag deutlich über die bisherige Signatur-Richtlinie hinaus. Die ersten beiden Erwägungen des Vorschlags beschreiben die Absicht und den Inhalt recht gut:

- (1) Die wirtschaftliche Entwicklung setzt Vertrauen in das Online-Umfeld voraus. Mangelndes Vertrauen führt dazu, dass Verbraucher, Unternehmen und Verwaltungen nur zögerlich elektronische Transaktionen durchführen oder neue Dienste einführen, bzw. nutzen.
- (2) Diese Verordnung dient der Stärkung des Vertrauens in elektronische Transaktionen im Binnenmarkt, indem eine sichere und nahtlose elektronische Interaktion zwischen Unternehmen, Bürgern und öffentlichen Verwaltungen ermöglicht wird, wodurch die Effektivität öffentlicher und privater Online-Dienstleistungen, des elektronischen Geschäftsverkehrs und des elektronischen Handels in der Union erhöht werden.

Ein besonderes und neues Thema ist die Notifikation und damit gegenseitige Anerkennung von staatlichen Schemen für die elektronische Identifizierung (eID, bzw. Authentifizierung) in den Artikeln 5 ff. Die Bestimmung verpflichtet die Mitgliederstaaten nicht zur Einführung oder Notifikation eines elektronischen Identifizierungssystems. Alle Mitgliedstaaten sind jedoch verpflichtet, dort wo sie für den Zugang zu Behördendiensten eine eID verlangen, auch die ausländischen eIDs aller notifizierten eID-Systeme zu akzeptieren. Technisch würde die Interoperabilität unterschiedlicher eID-Systeme nach Art der bisherigen [STORK](#)-Projekte umgesetzt. Die Schweiz könnte ein Interesse daran haben, künftig an diesem System für die Interoperabilität von eIDs beteiligt zu sein, sei es, damit Inhaber schweizerischer

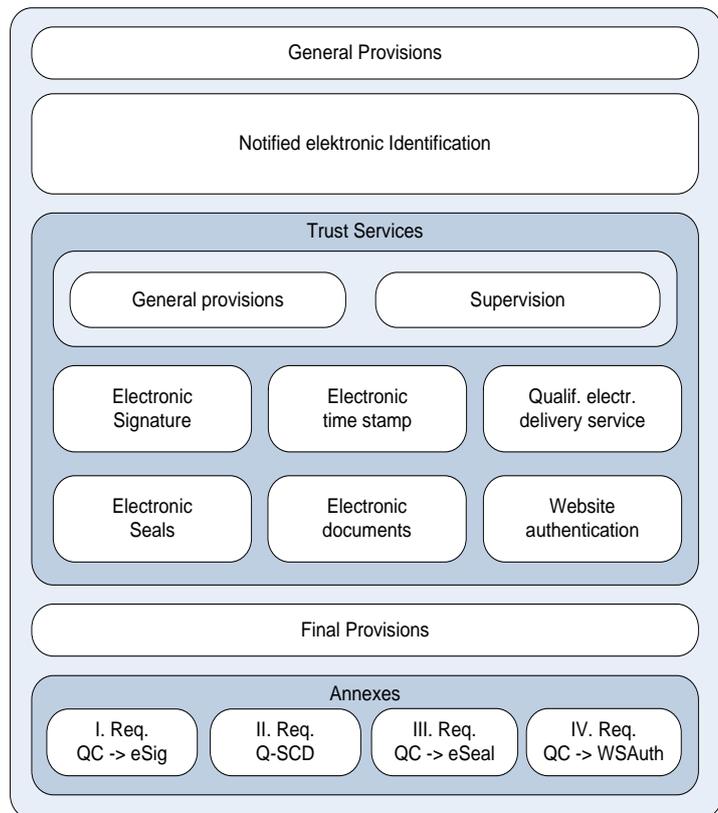


Abbildung 2: Inhaltlicher Aufbau des EU-Verordnungsvorschlags

⁵ Siehe http://ec.europa.eu/information_society/digital-agenda/index_en.htm

eIDs mit ausländischen Behörden verkehren können, sei es, dass Ausländer mit ihrer nationalen eID mit Schweizer Behörden sicher verkehren können.

Die restlichen Bestimmungen betreffen die Anerkennung und Beaufsichtigung von nicht-qualifizierten und qualifizierten Anbietern verschiedener ‚Vertrauensdienste‘ nach der Art der bisherigen Anerkennung von Zertifizierungsdienste-Anbietern. Die näher geregelten Vertrauensdienste sind nebst der Elektronischen Signatur: das Elektronische Siegel, der Elektronische Zeitstempel, das Elektronische Dokument, der Elektronische Zustelldienst und die Website-Authentifizierung.

3.3 Überblick über Themenfelder

Eine grafische Zusammenstellung der in den verschiedenen vorstehend erwähnten Quellen erkannten Lücken, Postulate und Forderungen im Kontext der Gesetzgebung für einen sicheren elektronischen Geschäftsverkehr (für E-Business und E-Government) präsentiert sich etwa wie folgt:

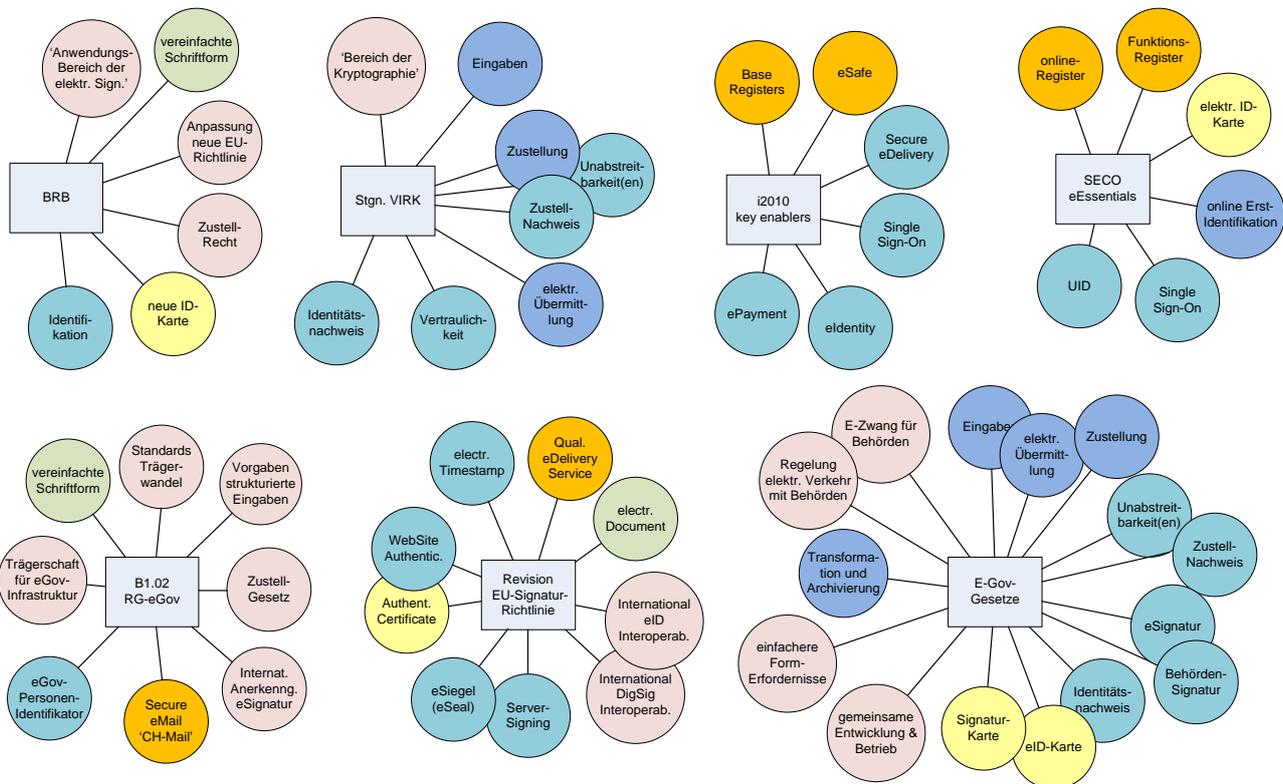


Abbildung 3: Die Vorhaben mit ihren Themen-Feldern (blau/türkis: Funktionen, gelb/orange: Infrastruktur, rosa: Rechtsetzung)

Verschiedenste Aufgabenstellungen, Abklärungen und Überlegungen führten teilweise zu immer etwa den gleichen Postulaten, wie z.B. das Bedürfnis nach einer sicheren Identifikation der Teilnehmenden am elektronischen Geschäftsverkehr oder der Möglichkeit, gewisse Kommunikations-Sachverhalte beweisen zu können. Zu anderen Teilen führten sie aber auch zu sehr spezifischen und u.U. auch sehr komplexen Anliegen, wie z.B. der Erweiterung des Repertoires der vom Gesetz vorgesehenen Formen, das sich heute in der Schweiz im Wesentlichen auf die einfache und die qualifizierte Schriftlichkeit beschränkt.

3.4 Gliederung der Themen

Wenn man die festgestellten Lücken oder Forderungen bezüglich ihrer Intention etwas näher betrachtet, stellt man fest, dass sie sich auf ganz unterschiedliche Ergebnisse beziehen können.

Es kann ein einzelnes **Infrastruktur-Element** wie eine eID-Karte oder ein elektronisches Urkunden-Safe verlangt werden. Oder die Regelung einer **Funktion**, wie z.B. der Signatur oder des Zustell-Nachweises. Es kann aber auch die Regelung und/oder Unterstützung eines bestimmten (elektr.)



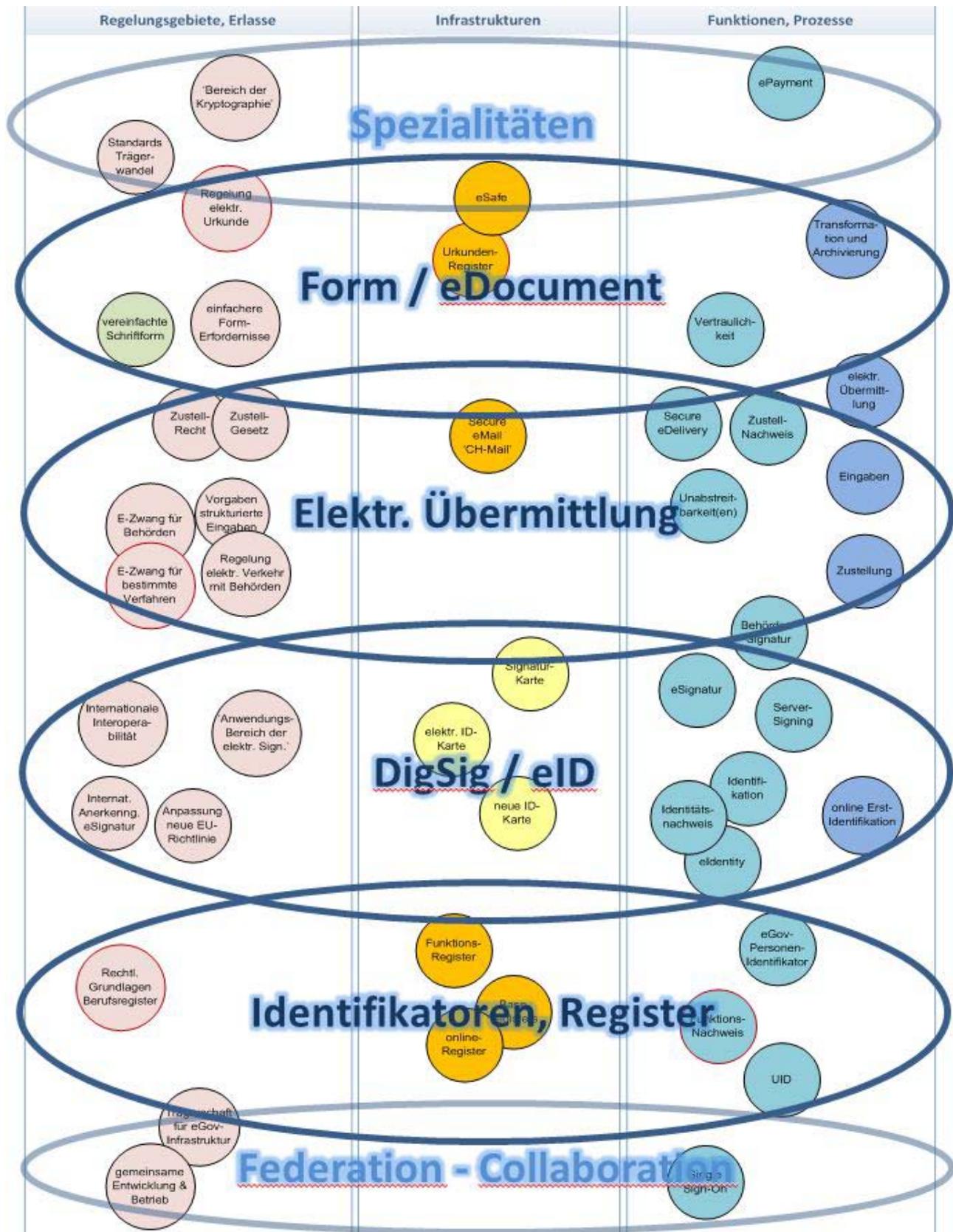
Geschäftsprozesse angestrebt werden oder die Forderung bezieht sich direkt auf einen **Erlass**, wie z.B. eine ‚Zustell-Gesetzgebung‘, welche die elektronische Zustellung von Meldungen umfassend regeln soll.

Dabei besteht in gesetzgebungs-politischer Hinsicht eine gewisse Hierarchie unter diesen Aspekten, die sich wie folgt beschreiben lässt:

- Zur elektronischen Abwicklung gewisser **Geschäftsprozesse**
- sind bestimmte Sicherheits-**Funktionen** notwendig
- welche bestimmte **Infrastruktur-Teile** benötigen,
- die ihrerseits u.U. **rechtliche Regelungen** benötigen, damit sie überhaupt oder in einer bestimmten Qualität zur Verfügung gestellt werden.

In dieser Konstellation ist die Raison d’Être für eine bestimmte rechtliche Regelung somit im Prinzip immer, dass sie notwendig ist, um die elektronische Abwicklung eines Geschäftsprozesses möglich und/oder sicher zu machen.

Dieser Einteilung entsprechend gegliedert und zusammengestellt, lässt sich das Gesamtbild der angesprochenen Funktionalitäten, Infrastrukturen und Regelungen wie folgt darstellen:

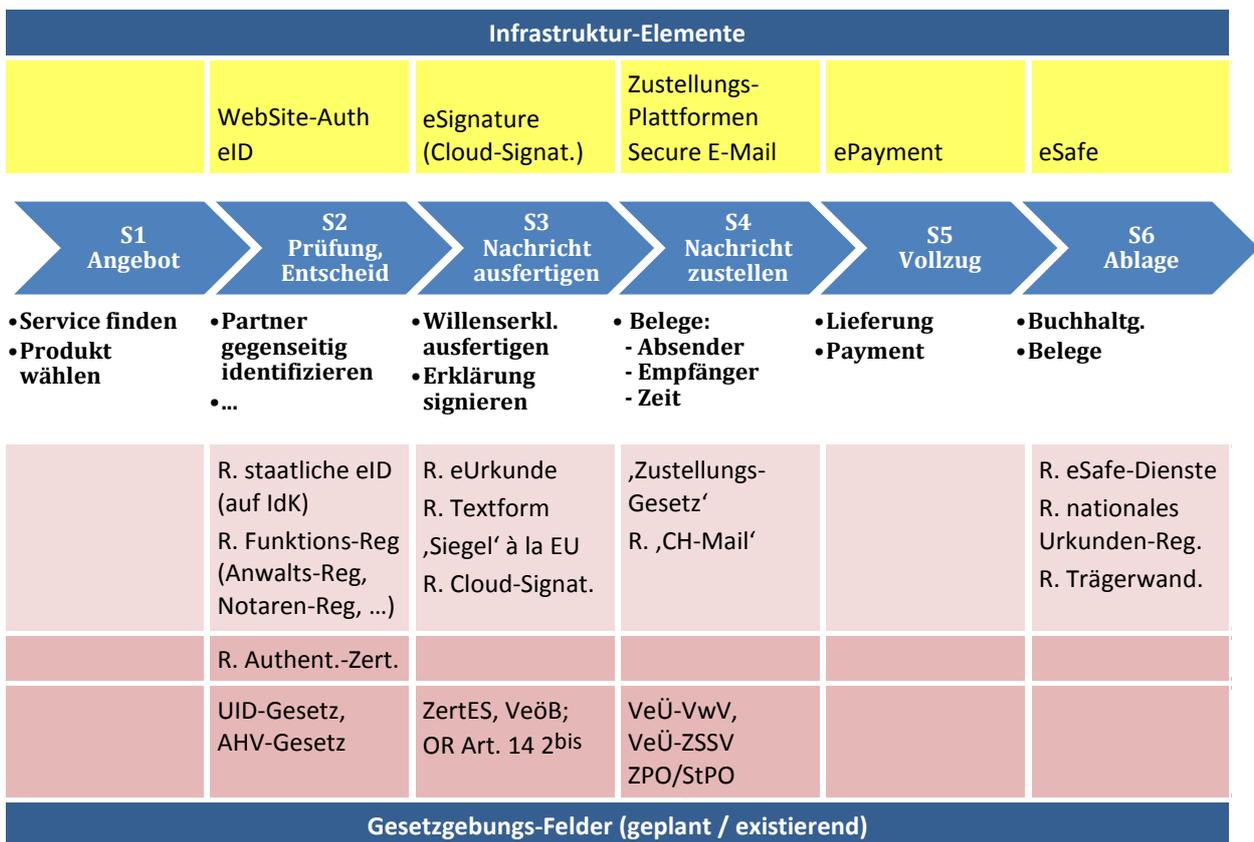


4 Förderlicher Rechtsrahmen für den elektronischen Geschäftsverkehr als Kernthema des Gesetzgebungsvorhabens

Schon eingangs in der Problemstellung wurde erläutert, dass das mutmasslich sinnvollste Generalthema für das gesamte Gesetzgebungsvorhaben und auch die überzeugendste sachlogische Klammer in der Formulierung *‘Schaffung eines vollständigen Rechtsrahmens zur Ermöglichung und Unterstützung der elektronischen Abwicklung von Geschäften’* besteht. Ob Geschäftsverkehr unter Privaten oder Behördenverkehr, ob Umstellung bisheriger Prozesse von Papier auf elektronische Abwicklung oder neue Geschäftsmodelle, die nur in der elektronischen Welt möglich sind, alle diese Ausprägungen von elektronischem Geschäftsverkehr sollen unter optimalen rechtlichen Rahmenbedingungen, einfach und sicher stattfinden können.

4.1 Prozess-Modell des elektronischen Geschäftsverkehrs

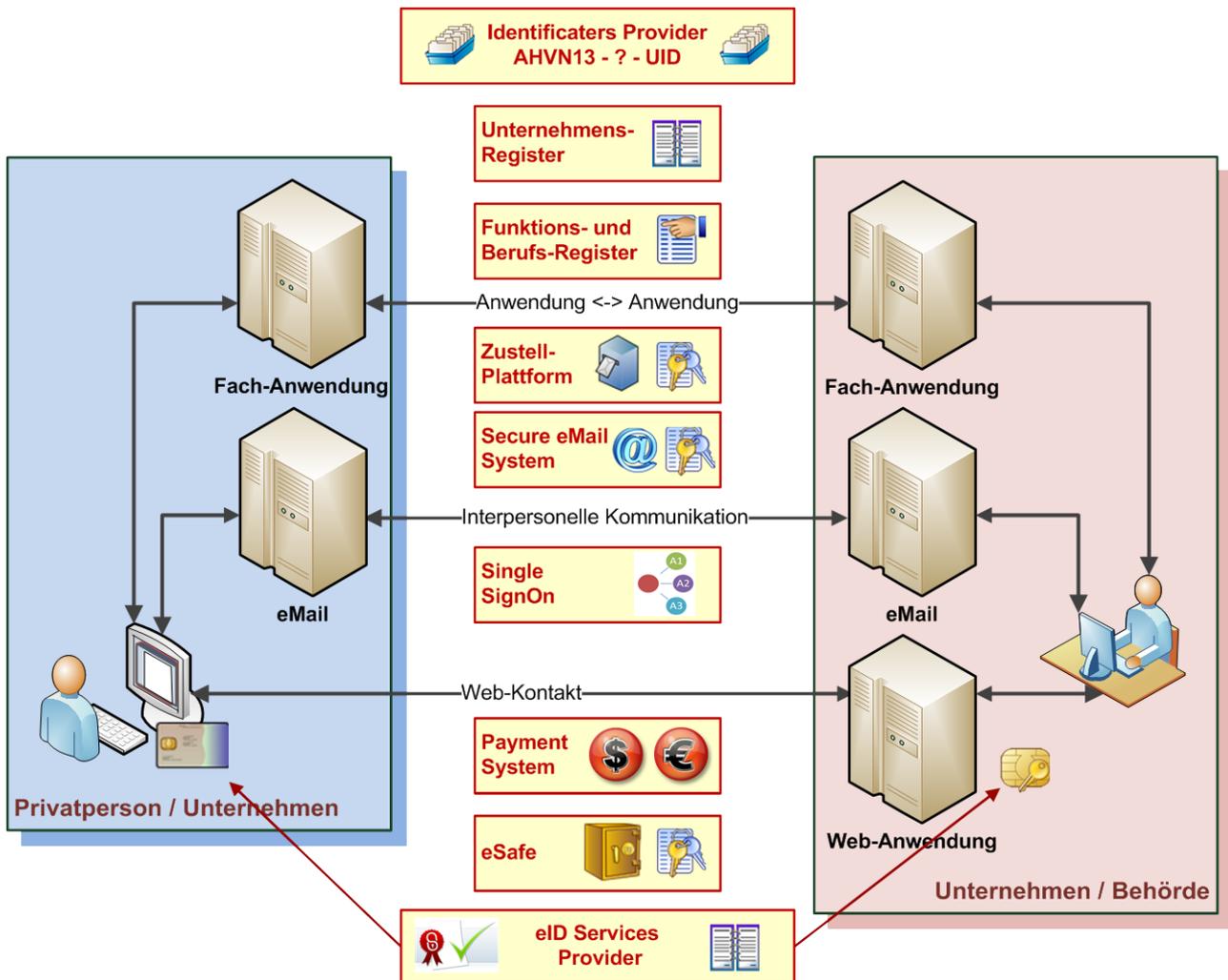
Die notwendigen Funktionalitäten und Infrastruktur-Elemente für die sichere elektronische Abwicklung von Geschäften können nach den Phasen gegliedert werden, welche gebräuchliche Modelle für E-Business-Prozesse aufweisen. Mit diesem Ansatz ist der Bezug zur eingangs geschilderten Zielsetzung direkt hergestellt.



Legende:	(Titel)	Funktion
	Infrastruktur-Elemente	Regelung (fehlend)
	Prozess-Schritt	Regelung (bestehend)

4.2 Infrastruktur-Modell des elektronischen Geschäftsverkehrs

Aus Sicht der für einen sicheren und vertrauensvollen elektronischen Geschäftsverkehr benötigten Infrastrukturen (oder ‚Vertrauens-Dienste‘) kann die gesamte Konstellation mit vorhandenen, teilweise vorhandenen und fehlenden Elementen wie folgt dargestellt werden:



4.3 Ordnungspolitische Betrachtung des Regulierungsbedarfs

Wirtschaft und Staat entwickeln sich Richtung Informationsgesellschaft. Ein immer grösserer Teil von Geschäften unter Privaten oder zwischen Privaten und dem Staat wird mit elektronischer Kommunikation unterstützt oder läuft sogar vollständig elektronisch ab. Dabei werden sowohl bisherige Geschäfte auf elektronische Abwicklung umgestellt, wie auch neue Geschäftsmodelle⁶ entwickelt, die nur mit elektronischer Abwicklung möglich sind. Den Unternehmen, die auf dem Heimmarkt rechtzeitig solche Modelle entwickeln können, stehen später auch internationale Märkte offen. In der Summe kommen diese Umstellungen und Neuentwicklungen einem eigentlichen Strukturwandel gleich.

⁶ Beispielsweise Verkaufsplattformen wie eBay, amazon, ricardo.ch oder soziale Netzwerke wie facebook, aber auch spezialisierte Dienste wie die Termin- und Umfrageplattform Doodle.

Die Umstellung auf elektronische Abwicklung kann grosse Einsparungen an Zeit, Aufwand und Geld bewirken. Trotzdem wird auch in der Schweiz erst ein kleinerer Teil an Rechnungen elektronisch abgewickelt, was auf weiterhin existierende Barrieren und Unsicherheiten schliessen lässt. Es ist bekannt, dass Unternehmen nur dann in neue Abläufe und Geschäftsmodelle investieren, wenn die Rechtsgültigkeit der neuen Verfahren eindeutig und sicher ist. Jede Unsicherheit in faktischer oder rechtlicher Hinsicht hemmt Investitionen in eine solche Umstellung.

Die Infrastrukturen und Dienste für einen für alle Beteiligten sicheren und vertrauenswürdigen elektronischen Geschäftsverkehr werden grösstenteils im Markt entwickelt und bereitgestellt. An gewissen neuralgischen Stellen braucht es jedoch den Staat, sei es in der Rolle als klassischer Gesetzgeber, z.B. im Vertragsrecht, sei es als letzte Instanz oder Anker für die Vertrauenswürdigkeit von privaten Akteuren (Zertifizierungen), oder sei es in der Bereitstellung gewisser Basis-Infrastrukturen, die unter rein marktwirtschaftlichen Gegebenheiten nicht oder nicht in erwünschter Form bereitgestellt werden (Ausweise, Register). Der Staat muss rechtzeitig einen klaren Rechtsrahmen und die notwendigen Basis-Vertrauens-Dienste bereitstellen.

Die europäische Signatur-Richtlinie und das ZertES in der Schweiz sind gute Beispiele dafür, wie der Gesetzgeber zwar tätig wird, aber eben sehr zurückhaltend. Der Staat anerkennt, dass gewisse vertrauenswürdige Dienste nötig sind, stellt diese aber nicht selber zur Verfügung, sondern formuliert zusammen mit der Branche inhaltliche Qualitätsmassstäbe und bietet den Anbietern eine freiwillige und nicht exklusive Zertifizierung gemäss diesen geregelten Vorgaben an.

Etwas näher betrachtet lassen sich vier grundsätzlich verschiedene Zielsetzungen eines Gesetzgebungs-Vorhabens zur Förderung des elektronischen Geschäftsverkehrs unterscheiden:

1. Barrieren beseitigen

Es werden in den bestehenden Gesetzen und anderen Erlassen Hindernisse für den elektronischen Rechtsverkehr beseitigt, etwa indem die Formvorschriften auch elektronische Formen vorsehen oder – wie hier weiter hinten unter Punkt 5.5 behandelt – indem neue, angepasste Formen definiert und übermässig hohe Anforderungen an die Form reduziert werden.

2. Sicheren Rechtsrahmen schaffen

Es werden neue, den aktuellen (technischen) Gegebenheiten angepasste Rechtsvorschriften geschaffen, sodass grössere Rechtssicherheit besteht und nicht jahrelang Unsicherheit besteht, bis sich via Rechtsprechung und Doktrin Antworten auf wichtige Fragen und neue Regeln gebildet haben. In diesem Paket wird dieses Ziel vor allem in der Forderung nach einer angepassten Zustell-Gesetzgebung in Punkt 5.3 angesprochen.

3. Förderung, Pilotierung

Gesetzgebung kann – schwergewichtig im Bereich E-Government – auch dazu eingesetzt werden, neuen Verfahren zum Durchbruch zu verhelfen, indem der Staat sie selber anwendet oder im Behördenverkehr verlangt. So etwa, wenn die Behörden verpflichtet werden, elektronische Eingaben entgegenzunehmen oder wenn für bestimmten Verfahren gar die elektronische Abwicklung auch für alle Beteiligten zwingend vorgeschrieben wird, wie das z.B. im Punkt 5.8 für die Rechnungsstellung an den Staat vorgeschlagen wird.

4. Missbrauch bekämpfen

Der Staat kann durch Gesetzgebung dafür sorgen, dass elektronische Kommunikationsmittel und Verfahren nicht missbräuchlich benutzt werden. Beispiele sind das Computer-Strafrecht und die Datenschutz-Gesetzgebung. Im hier behandelten Paket gibt es keinen Schwerpunkt in dieser Richtung.

5 Die einzelnen Gesetzgebungspakete

Nachdem die vorstehend geschilderten Postulate für gesetzliche Regelungen zwar alle in der einen oder andern Form Erfordernisse für die sichere und vertrauenswürdige elektronische Abwicklung von Geschäften darstellen, auf der anderen Seite aber doch recht verschiedene Felder abdecken und vermutlich auch politisch unterschiedlich dringend oder opportun eingeschätzt werden, geht es in den nachfolgenden Überlegungen darum, wie die verschiedenen potentiellen Regelungsinhalte mit ihren jeweiligen Zielen unter sachlogischen und systematischen Gesichtspunkten sinnvoll auf einzelne Gesetzgebungsvorhaben aufgeteilt werden können.

Es wäre dann dem Antrag an den Bundesrat vorbehalten, diese Vorhaben unter rechtspolitischen und Machbarkeits-Überlegungen zu politisch erfolgversprechenden Paketen zu gruppieren.

5.1 Anpassung des ZertES an die Nachfolge-Verordnung der EU-Signatur-Richtlinie

Die wichtigsten Inhalte des aktuell vorliegenden Vorschlags der EU für eine Verordnung über die elektronische Identifizierung und Vertrauensdienste – als Ablösung der EU-Signatur-Richtlinie – sind vorstehend in Kapitel 3.2 beschrieben.

Ein beträchtlicher Teil der Neuerungen dieses Vorschlags deckt oder überlappt sich mit einer der vorstehend aufgeführten Forderungen. Teile davon wurden schon in der laufenden ZertES-Revision aufgegriffen. So z.B. die Regelung des Einsatzes von Zertifikaten für die Authentisierung von Personen oder Websites oder die elektronische Unterschrift für Behörden, im neuen Vorschlag treffend als ‚elektronisches Siegel‘ bezeichnet. Weitere Teile, wie die Zertifizierung von elektronischen Zustell- und anderen Diensten, wurden so oder ähnlich auch hier gefordert und können somit im Rahmen dieses Paketes – möglichst in Übereinstimmung mit der europäischen Lösung – geregelt werden.

In diesen Bereich fällt auch die Teilnahme der Schweiz am Notifizierungs-Schema für die grenzüberschreitende gegenseitige Anerkennung von elektronischen Identitäten, wodurch sich ausländische Personen bei schweizerischen Behörden und Schweizerinnen und Schweizer bei ausländischen Behörden mit ihrem nationalen elektronischen Identifikations-Mittel authentisieren könnten. In Anbetracht der starken und weiter steigenden Vernetzung der Schweiz mit dem europäischen Umfeld wäre eine solche Interoperabilität eine grosse Erleichterung und Effizienzsteigerung sowohl für die Inhaber der eIDs wie auch für die Behörden im In- und Ausland.

Selbst in den Fällen, wo die neue EU-Verordnung Regelungen enthält, die hier bisher nicht auf der Traktandenliste standen, ist für jedes Element zu prüfen, ob es mit Hinblick auf Konformität mit der europäischen rechtlichen Situation auch in der Schweiz einzuführen sei.

Verhältnis zur laufenden ZertES-Revision: Nachdem nun eher überraschend schon heute ein fortschrittlicher und konkreter Vorschlag der EU für die Nachfolge der Signatur-Richtlinie vorliegt, drängt sich die Frage auf, ob die schon laufende, ‚kleine‘ ZertES-Revision weiter zu Ende geführt werden soll, oder ob sie nicht wieder mit der hier explorierten, umfassenden Gesetzgebung zusammengeführt werden soll.

Für eine Zusammenlegung sprechen nachstehende Gründe:

- Harmonisierung: Es kann vermieden werden, dass die vorangehende, ‚kleine‘ Revision Änderungen vornimmt, die später mit Rücksicht auf Kompatibilität mit der EU-Verordnung wieder zurückgenommen werden müssen.
- Evidenz: Der Einwand liegt auf der Hand. Auf jeder Stufe wird wieder die Frage gestellt werden, warum in der gleichen Materie zweimal so nahe hintereinander legiferiert wird.

- Effizienz: Alle Beteiligten, von der Verwaltung, über die Interessengruppen und Kantone bis hin zum Parlament und schliesslich dem Volk, sollten mit möglichst wenigen Gesetzgebungsvorlagen belastet werden.

Gegen eine Zusammenlegung sprechen nachstehende Gründe:

- Vorteile sichern: Die laufende Revision greift seit langem bekannte Anliegen der einschlägigen Akteure auf, hat in der Vernehmlassung gute Unterstützung erfahren und könnte rasch umgesetzt werden. Die dringend gewünschten Korrekturen könnten etwa innert eines Jahres in Kraft sein.
- Unsicherheit: Weder ist sicher, dass der Verordnungs-Vorschlag inhaltlich so bleibt wie er ist, noch ist bisher mit einer gewissen Sicherheit absehbar, wann er in Kraft treten wird. Die schweizerische, auf diese Verordnung abgestützte Revision, könnte aber frühestens dann in die Vernehmlassung gehen, wenn die Verordnung in trockenen Tüchern ist. Auch die seit Langem erwarteten und unbestrittenen Verbesserungen am ZertES könnten somit frühestens etwa in 2-3 Jahren in Kraft treten.

Nach aktueller Einschätzung könnte die laufende ZertES-Revision ohne allzu grosse Eingriffe soweit an den Verordnungs-Vorschlag der EU angepasst werden, dass die beiden Revisionen kein Hin und Zurück bewirken werden. In erster Linie würden von der Menge der neu vorgeschlagenen ‚geregelten‘ Zertifikate und Signaturen *die* Sachverhalte abgespaltet, die nach dem EU-Vorschlag das ‚elektronische Siegel‘ betreffen, und neu ebenso benannt. Nach der Terminologie der laufenden Revision wären das die ‚geregelten Signaturen‘ von juristischen Personen und Behörden.

Der vorliegende Bericht geht im Weiteren davon aus, dass die laufende ZertES-Revision wie geplant weiterverfolgt wird. Sollte diese Frage anders entschieden werden, kämen zu den hier aufgeführten Gesetzgebungsvorhaben zusätzlich noch die Änderungen der Revisions-Vorlage hinzu.

Kurz zusammengefasst würde der Auftrag also darin bestehen, eine Gesetzgebung zur selektiven Anpassung des schweizerischen Rechts an die neue EU-Verordnung zu entwerfen und dem Bundesrat eine entsprechende Vernehmlassungsvorlage zu unterbreiten. Unter Umständen könnten gewisse nachstehend erläuterte Regelungen aufgrund ihrer sachlichen Nähe später ebenfalls in dieses Vorhaben gepackt werden, so z.B. die weitergehende Regelung einer schweizerischen eID sowie die Zertifizierung von Systemen und Anbietern für E-Mail- und eSafe-Systeme.

5.2 Konzept und Rechtsrahmen für eine staatliche elektronische Identität (eID)

Eine vertrauenswürdige Identifikation in der virtuellen Welt ist eine der Voraussetzungen für E-Government- und E-Business-Anwendungen. Ein elektronisches Identifizierungsmittel („elektronische Identität“, eID) bietet diese Möglichkeit. Eine eID kann auf einer Chipkarte, einem USB-Stick, einer SIM-Karte oder auf dem Prozessor eines Smartphones, Tablet-Computers oder PCs gespeichert sein. Sie besteht im Wesentlichen aus zwei zusammenhängenden Zahlen („Schlüsselpaar“), einer öffentlichen und einer geheimen. Die geheime Zahl stellt dabei das elektronische Identifizierungsmittel dar. Mit ihr authentifiziert sich der Besitzer in der virtuellen Welt, ohne dabei die geheime Zahl selbst preisgeben zu müssen. Der Kommunikationspartner wiederum kann mit der öffentlichen Zahl (im ‚Zertifikat‘ enthalten) die entsprechende elektronische Identität prüfen, ohne die geheime Zahl des Besitzers zu kennen.

Die Mehrzahl der europäischen Staaten gibt seinen Einwohnerinnen und Einwohnern eine offizielle elektronische Identität (eID) ab, in den meisten Fällen auf der Identitätskarte. Diese eID kann in erster Linie für die sichere und rechtsverbindliche Anmeldung auf Websites von Behörden verwendet werden. Oft wird sie auch für die Authentisierung im Verkehr mit privaten Diensteanbietern eingesetzt.

In der Schweiz gibt es bisher keine staatliche eID. Mit der SuisseID (www.SuisseID.ch) wurde jedoch vor drei Jahren – im Kontext des 3. Pakets der konjunkturellen Stabilisierungsmassnahmen – zusammen mit der Privatwirtschaft und auf der Basis der staatlich regulierten Prozesse für die elektronische Signatur (ZertES) eine standardisierte eID lanciert, die sich technisch bewährt hat und in professionellen Nischen etablieren konnte.

Eine eID muss zwischenstaatlich anerkannt sein, um ihr volles Potenzial zu entfalten. Nur dann können grenzüberschreitende Geschäfte ohne Medienbruch abgewickelt werden. Hier liegt nach Einschätzungen der Wirtschaft ein sehr grosses Einsparvolumen. Das von der EU mitfinanzierte STORK-Konsortium (<https://www.eid-stork.eu/>) hat dieses Ziel. Die Fachhochschule Bern beteiligt sich im Auftrag der SuisseID-Trägerschaft an diesen Arbeiten.

Der im Kapitel 3.2 vorgestellte EU-Verordnungsentwurf sieht im Kapitel II ein Schema für die Notifizierung und gegenseitige Anerkennung von nationalen Identifikationsmitteln vor. Gemäss Artikel 6 dieses Entwurfs sind allerdings nur Identifizierungsmittel zur Notifikation zugelassen, die ‚vom notifizierenden Mitgliedstaat, in dessen Namen oder unter dessen Verantwortung ausgestellt‘ werden. Eine auf Basis freiwilliger privatrechtlicher Vereinbarungen ausgestellte eID wird in Artikel 2 Ziffer 2 des Verordnungs-Entwurfs explizit ausgeschlossen (‚Diese Verordnung findet keine Anwendung auf elektronische Vertrauensdienste, die aufgrund freiwilliger privatrechtlicher Vereinbarungen erbracht werden.‘).

Selbstverständlich gibt es für die Schweiz keine rechtliche Verbindlichkeit zur Übernahme der EU-Verordnung. In Anbetracht der Internationalität des elektronischen Geschäftsverkehrs ist es jedoch mehr als geraten, eine künftige schweizerische eID wenn immer möglich so zu konzipieren, dass sie grundsätzlich notifiziert werden könnte. Da jedoch eine Verordnung vorgeschlagen wird, die für die EU-Mitgliedstaaten direkt anwendbar wäre, müsste die Schweiz selbständig eine Umsetzung ins nationale Recht vorsehen, ohne – wie bei der EU-Signatur-Richtlinie – auf andere nationale Umsetzungen als Beispiele zurückgreifen zu können. Schliesslich müsste zudem eine staatsvertragliche Lösung gefunden werden, wie sich die Schweiz diesem Notifikations- und Anerkennungssystem anschliessen könnte.

Eine zu prüfende Lösung wird sein, den Teil ‚elektronische Identität‘ der heutigen SuisseID in die Verantwortung des Bundes zu übernehmen. Hier stellen sich neben privatrechtlichen auch vergaberechtliche Fragen, welche genau geprüft werden müssen. Eine weitere Lösungsvariante wäre es, eine neue, vom Bund (z.B. dem BIT) herausgegebene elektronische Identität zu schaffen. Diese stünde in Konkurrenz zur SuisseID. Eine öffentliche Ausschreibung der eID wäre die dritte zu prüfende Variante.

Eine Grundvoraussetzung für das Vertrauen in eine eID ist ein sicherer Ausstellungsprozess. Der Entwurf der EU-Verordnung verlangt in Artikel 6 Buchstabe c, dass der Staat die volle Verantwortung für die Zuweisung der realen zu der virtuellen Identität übernehmen muss (‚der notifizierende Mitgliedstaat stellt sicher, dass die Personenidentifizierungsdaten der in Artikel 3 Absatz 1 genannten natürlichen oder juristischen Person eindeutig zugeordnet sind;‘).

Hier soll der sichere Ausstellungsprozess für Pass und Identitätskarte zukünftig gleichfalls für die Zuordnung der eID genutzt werden. Eventuell muss dieser Prozess für eine notifizierbare eID sogar als für verbindlich erklärt werden. Möglich erscheint aus heutiger Sicht auch ein Verfahren, bei dem im Chip auf der Identitätskarte bei der Herstellung nur ein temporärer elektronischer Schlüssel gespeichert wird, welcher das spätere Nachladen der eigentlichen elektronischen Identität ermöglicht. Gleichzeitig soll geprüft werden, ob und wie die elektronische Identität von der Identitätskarte als Primärträger sicher auf weitere Identifikationsmittel übertragen werden könnte (z.B. Smartphones).

Mit dem Beschluss vom 16. Dezember 2011 (‚Schweizer Pass und Identitätskarte: Entscheid über das weitere Vorgehen‘) hat der Bundesrat festgelegt, dass die Identitätskarte ab dem Jahr 2016 auch mit

einer elektronischen Identität angeboten werden soll. Artikel 2 Absatz 2^{quater} des heutigen Ausweisgesetzes ([SR 143.1](#)) bietet die formell-gesetzliche Grundlage, um die Identitätskarte (oder den Pass) als Träger einer eID anbieten zu können. Dies bedeutet jedoch nicht, dass die Gesamtverantwortung für die elektronische Identität (Management, Überwachung, Betrieb und Support) zwingend im EJPD liegen muss. So profitiert hauptsächlich die Volkswirtschaft von der eID. Es ist deshalb im Gesamtkontext zu prüfen, wo die Gesamtverantwortung für eine eID der Schweiz angesiedelt werden soll.

Wenn die Gelegenheit der Einführung einer neuen Identitätskarte nicht vertan werden soll, sind dringend einerseits umfassende Konzeptarbeiten für Ausgestaltung des künftigen staatlichen Identifikationsmittels (eID) und andererseits die Planung der rechtlichen Umsetzung an die Hand zu nehmen

5.3 Kompletterung und Harmonisierung der Zustell-Gesetzgebung

Wie vorstehend schon ausgeführt, ist Unsicherheit Gift für Investitionen von Privaten in neue Verfahren und Geschäftsmodelle. Genau solche Unsicherheiten bestehen aber in verschiedenen rechtlichen Aspekten des elektronischen Geschäftsverkehrs. Die schweizerische Gesetzgebung hat die sachlichen und rechtlichen Fragen rund um den Zugang von Mitteilungen im Geschäftsverkehr, wie beispielsweise den Übergang des Risikos, die zeitlichen Verhältnisse und die Beweisbarkeit der massgeblichen Tatsachen bei der Zustellung seit jeher eher stiefmütterlich behandelt. Zudem haben sich durch die Liberalisierung der Briefpost und die elektronische Kommunikation die Verhältnisse rund um die rechtskonforme Zustellung in den letzten Jahren wesentlich geändert, ohne dass die darauf aufbauenden rechtlichen Konzepte genügend klar und prominent angepasst wurden.

Bei der Geschwindigkeit mit der sich heute die Verhältnisse verändern, ist es unbefriedigend, wenn wichtige rechtliche Fragen langwierig durch die Rechtsprechung und die Doktrin beantwortet werden müssen. Es ist dringend nötig, für diesen Bereich rasch ein den heutigen Gegebenheiten angepasstes, konsistentes Regelwerk zu schaffen, auch wenn dieses einige traditionell gewachsene und vertraut gewordene Konzepte in Frage stellen kann. Wo wichtige Infrastruktur-Elemente wie z.B. vertrauenswürdige Zustelldienste noch fehlen, sind durch Regelungen von Anforderungen und Zertifizierungsschemen Anreize dafür zu schaffen. Ziel ist, dass alle Beteiligten, Private, KMUs, Grossfirmen und Behörden auf einfache Art rechtsgültige Dokumente erzeugen, sie sicher und vertraulich zustellen und von Sender- wie auch von Empfänger-Seite Inhalt und Zustellung rechtsgültig beweisen können.

Eine komplette und harmonisierte Zustell-Gesetzgebung müsste ein konsistentes System von Regeln über die Zustellung von Dokumenten, die in diesem Kontext notwendigen Funktionalitäten und die juristischen Folgen bestimmter Handlungen und Funktionen umfassen. Es soll alle existierenden Regeln umfassen, ob sie nun die konventionelle oder die elektronische Zustellung betreffen, ob sie explizit geregelt sind oder sich in der Doktrin herausgebildet haben und auch heute fehlende Regeln insbesondere im Bereich der elektronischen Zustellung. Ob dazu ein eigentliches Zustell-Gesetz geschaffen werden soll, wie das z.B. [Österreich](#) kennt, oder ob nur die zahlreichen Erlasse mit solchen Bestimmungen harmonisiert werden sollen, ist in den weiteren Arbeiten zu prüfen.

Gemäss Katalog der Umsetzungs-Massnahmen im B1.02-Abschlussbericht soll in einem ersten Schritt bis Mitte 2013 eine Projektskizze zu einer Zustellungs-Gesetzgebung inkl. staatlich reguliertem E-Mail erstellt werden. Diese Arbeiten könnten, wie hier vorgeschlagen, nahtlos in ein formelles Gesetzgebungsprojekt münden.

5.4 Gesetz zur Zertifizierung von elektronischen Mail-Diensten („CH-Mail“)

Eng mit der vorstehend geschilderten Frage der rechtlichen Konzepte für die Zustellung verknüpft ist die Frage der dazu verwendeten Zustell-*Infrastruktur*. Wie weit sollen die dafür benötigten elektronischen Dienste, z.B. eMail-Systeme, und ihre Betreiber vom Staat reguliert und zertifiziert werden? Oder soll der Staat gar selber gewisse Komponenten mit besonderen Ansprüchen an die Vertrauenswürdigkeit bereitstellen? Für den Bereich des Verkehrs mit Behörden wurde ein erster Schritt getan.

Mit der Einführung der neuen Prozessordnungen⁷ per 1. Januar 2011, der damit verbundenen Verpflichtung der Behörden, elektronische Eingaben entgegen nehmen zu müssen und den beiden Umsetzungsverordnungen [VeÜ-VwV](#) und [VeÜ-ZSSV](#) wurde ein komplettes regulatorisches Modell für den elektronischen Geschäftsverkehr eingeführt, das als Muster insbesondere auch für kantonale Regulierungen verwendet werden kann.

Soll auch für den privaten elektronischen Geschäftsverkehr eine stabile, vertrauliche und vertrauensvolle Umgebung geschaffen werden, müssten die gesetzliche Grundlage dafür geschaffen werden, dass qualifizierte Anbieter in Umfang und Qualität definierte E-Mail-Dienste zertifizieren lassen können, sodass in der Gesamtheit ein übergreifendes System von vertrauenswürdigen E-Mail-Diensten mit dem vollen Set von rechtlich klar geregelten Sicherheits- und Beweis-Funktionen ergibt.

Als Beispiel kann das in Deutschland vor kurzem konzipierte [DE-Mail](#) mit seiner rechtlichen Regelung⁸ herbeigezogen werden. Nach einem ähnlichen Akkreditierungs-Schema wie bei der Anerkennung von Anbietern gemäss EU-Signatur-Richtlinie, bzw. ZertES, können sich Anbieter von E-Mail-Diensten, die vordefinierte Funktionalitäten in einer bestimmten Qualität anbieten, zertifizieren lassen. Das Gesamtsystem dieser zertifizierten E-Mail-Dienste verschiedener Anbieter bildet eine sichere und rechtlich privilegierte Kommunikationsinfrastruktur für Bürger, Unternehmen und Verwaltung.

Je nach Umfang und Intensität einer solchen Regelung könnte sie als eigenes CH-Mail-Gesetz, als Teil der Komplettierung und Harmonisierung der Zustell-Gesetzgebung oder als ‚einfache‘ Zertifizierung eines Vertrauens-Dienstes im Paket der Anpassungen an die neue EU-Verordnung über Vertrauens-Dienste umgesetzt werden.

5.5 Erweiterung der Dokument-Formen („Textform“)

Das Fehlen einer Dokument-Form mit definierter rechtlicher Bedeutung ‚unterhalb‘ der Schriftform stellt eine bedeutende Barriere für den elektronischen Geschäftsverkehr dar. Ein Schriftstück ohne Unterschrift, ein E-Mail, ein Gespräch und Rauchzeichen sind in dieser Hinsicht alle gleichwertig. Einzig der Telefax hat – wenn auch primär nur in der Praxis und ein Stück weit in der Doktrin – in dieser Hinsicht eine gewisse Anerkennung erlangt. Die unterste juristisch definierte Form für den elektronischen Geschäftsverkehr ist das gemäss [Artikel 14 Absatz 2^{bis} OR](#) qualifiziert signierte elektronische Dokument, was eine sehr hohe Hürde darstellt. Diese juristische ‚Bedeutungslosigkeit‘ aller anderen Formen steht auch in deutlichem Kontrast zur täglichen Praxis, wo gerade E-Mails im Geschäftsverkehr eine grosse Bedeutung zukommt. Mehrere vereinzelte gesetzgeberische Vorstösse in diese Richtung zeigen, dass hier eine Form fehlt. So verwendet die neue ZPO (SR 272) im [Artikel 17 Absatz 2](#) für die Formanforderung an Gerichtsstandsvereinbarungen die Formulierung ‚Die Vereinbarung muss schriftlich oder *in*

⁷ Schweizerische Zivilprozessordnung vom 19. Dezember 2008 (ZPO, [SR 272](#)), und Schweizerische Strafprozessordnung vom 5. Oktober 2007 (StPO, [SR 312.0](#)).

⁸ Vergleiche das deutsche ‚[Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften](#)‘ vom 28. April 2011.

einer anderen Form erfolgen, *die den Nachweis durch Text ermöglicht*. Weitere Formulierungen in diese Richtung finden sich in [Artikel 5 Absatz 1](#) und [Artikel 178 Absatz 1 IPRG](#), [Artikel 8 Absatz 2 PrSV](#), [Artikel 4a Absatz 1 Buchstabe b THG](#) und einigen weiteren Erlassen.

Auch wenn eine Veränderung bei den Formvorschriften recht fundamentale juristische Konzepte berührt, muss diese Aufgaben einmal angepackt werden. Die Lösung könnte darin bestehen, dass im schweizerischen Recht eine oder mehrerer Formen von Dokumenten ‚unterhalb‘ der Schriftform eingeführt werden, nach dem Beispiel der ‚[Textform](#)‘ nach deutschem Recht ([§ 126b BGB](#)).

Gemäss Katalog der Umsetzungs-Massnahmen im B1.02-Abschlussbericht soll in einem ersten Schritt ein Gutachten zu dieser Frage erstellt werden. Diese Arbeiten könnten nahtlos in ein formelles Gesetzgebungsprojekt münden.

5.6 Regelung der e-Apostille gemäss Haager Konferenz

Unter dem Namen e-APP existiert ein internationales Pilotprogramm zur Einführung einer elektronischen Apostille gemäss Haager Übereinkommen, organisiert von der ‚National Notary Association‘ (NNA) zusammen mit der Haager Konferenz (Hcch) (siehe www.e-app.info). Mit der [Apostille](#) werden Urkunden von der zuständigen Stelle für den internationalen Verkehr zwischen Ländern des Haager Übereinkommens beglaubigt. Zurzeit sind Belgien, Kolumbien, Spanien und die US-Staaten Kansas und Rhode Island am Pilotprogramm beteiligt. Im Februar 2007 wurden erstmals tatsächlich eine e-Apostille von Kansas nach Kolumbien übermittelt und dort akzeptiert.

Die e-Apostille könnte sich relativ rasch durchsetzen, da der Apostille an sich im internationalen Verkehr eine sehr grosse Bedeutung zukommt und elektronische Urkunden hier einen besonders grossen Nutzen aufweisen.

In der Schweiz könnte die e-Apostille im Zusammenhang mit der bundesgesetzlichen Regelung der elektronischen Beurkundung, die sich zur Zeit in Vorbereitung befindet, geregelt werden.

5.7 Gesetzgebung zur Zertifizierung von elektr. Aufbewahrungsdiensten (eSafe)

Voraussichtlich wird mit der bundesintern laufenden gesetzlichen Regelung der originären elektronischen öffentlichen Urkunde auch die Verwendung eines zertifizierten Urkundenregisters für die Ablage der elektronischen öffentlichen Urkunden vorgeschrieben. Daneben besteht aber nach den Erfahrungen in fortgeschrittenen Ländern zusätzlich ein Markt für zahlreiche weitere eSafe-Dienste von privaten Anbietern. Eine Regulierung ähnlich der ZertES-Gesetzgebung könnte die Grundlagen dafür legen, dass Anbieter mit einer definierten Qualität bestimmte Dienste in diesem Kontext als qualifizierte eSafe-Dienste zertifizieren lassen können.

Eine solche Zertifizierung von eSafe-Diensten und deren Anbieter könnte entweder im Zusammenhang mit der Regelung der elektronischen Urkunde oder im Paket der Anpassungen an die neue EU-Verordnung über Vertrauens-Dienste geregelt werden.

5.8 Einführung der obligatorischen elektronischen Rechnungsstellung

Wie vorstehend unter Punkt 4.3 erwähnt, kann der Staat den elektronischen Geschäftsverkehr fördern, indem er ihn selber praktiziert oder indem er seine Kommunikationspartner – Behörden oder Private – dazu anleitet oder gar verpflichtet, mit ihm elektronisch zu verkehren. In einigen Bereichen wird dies schon praktiziert (SchKG) oder es bestehen mindestens schon die gesetzlichen Grundlagen dazu (Handelsregister), in anderen Bereichen müssen die gesetzlichen Grundlagen noch geschaffen werden. Ein Bereich mit grossen Volumen, grosser Signalwirkung und auch grossem Einsparungs-Potential ist die Rechnungsstellung. So hat u.a. Dänemark im Jahr 2005 für alle Rechnungen an Behörden die Pflicht

zur elektronischen Rechnungsstellung (E-Invoicing) eingeführt und dazu auch die Standards vorgegeben. Inzwischen wird dieser Standard zunehmend auch für Rechnungsstellungen unter Privaten verwendet. Bei richtiger Ausgestaltung des Verfahrens mit strukturierten Daten, rechtsverbindlicher Übermittlung und weitgehend automatisierter Verarbeitung kann eine grosse Einsparung beim Personalaufwand bewirkt werden. Dänemark schätzt die Einsparung auf rund 200 Mio. Franken jährlich. Bei geschätzten 30 Mio. Rechnungen jährlich an Behörden in der Schweiz und typischen Einsparungen von mindestens 10 Franken pro elektronischer Rechnung, winken auch hier namhafte Einsparungen. Für Rechnungsstellungen an Bundesbehörden könnte der Bund relativ einfach ein solches Obligatorium einführen, indem er – soweit erforderlich – die gesetzlichen Grundlagen schafft und auch die konkrete organisatorische und technische Ausgestaltung festlegt. Eine entsprechende Motion (Motion Noser, [09.3396](#), E-Billing für Lieferanten der Bundesverwaltung) wurde vom Parlament nur stark abgeschwächt überwiesen. Es stünde dem Bund aber offen, hier einen Schritt weiter zu gehen. Für kleinere Lieferanten, die keinen automatisierten elektronischen Datenaustausch betreiben, ist ggf. ein Portal für die Eingabe der Rechnungen zu bauen, sodass schliesslich alle Rechnungen elektronisch und auf die gleiche Art strukturiert eingehen und automatisch verarbeitet werden können.