www.jusletter-it.eu

Reinhard Posch

Dokumente und Identifikation in der elektronischen Verwaltung

Qualitativ hochwertige Dokumente stehen im Zentrum einer vertrauenswürdigen Verwaltung und sind in gleicher Weise zentral für eine funktionierende Wirtschaft. Die unterschiedlichen Anforderungen an Dokumente aus der Verwaltung und an die verlässliche Zugänglichkeit sind die Eckpfeiler jedes elektronischen Verwaltungssystems. Wie in nahezu allen Staaten haben sich die Systeme der allgemeinen Verwaltung in den verschiedenen Sparten sowie der Justiz parallel und mit Rücksicht auf die spezifischen gesetzlichen Vorgaben entwickelt. Die Anstrengungen, diese in der Nutzung und in der Sicht der BürgerInnen und Unternehmen möglichst einheitlich und bereichsübergreifend verwendbar zu gestalten, sind für alle Betroffenen enorm wichtig. Grundelemente einer effizienten, übergreifenden und nutzerzentrierten Verwaltung sind in Österreich besonders ausgeprägt und fortgeschritten.

Category: Articles
Region: Austria
Field of law: Legal Informatics; Information Technology

Citation: Reinhard Posch, Dokumente und Identifikation in der elektronischen Verwaltung, in: Jusletter IT 19. November 2015

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

1. Grundbausteine der Verwaltung

[Rz 1] In der elektronischen Verwaltung geht es darum, Informationen und Dokumente von und zur Verwaltung sicher, nachvollziehbar und authentisch zu kommunizieren und dabei Grundprinzipien wie etwa den Datenschutz entsprechend zu beachten. Zudem ist der Umstand zu beachten, dass es sich beim Übergang zur «Elektronik» auf der Seite der BürgerInnen und Unternehmen um einen Prozess handelt, der sich über einen beachtlichen Zeitraum erstreckt, da wir unterschiedliche Bereitschaft und Notwendigkeiten beobachten. In jedem Fall müssen die Grundelemente der elektronischen Verwaltung auch den Anforderungen der Papierwelt standhalten und dabei auch die grenzüberschreitenden Aspekte beachten, die im geschäftlichen Bereich aber auch in vielen die BürgerInnen betreffenden Bereichen, wie zum Beispiel der Gesundheitsverwaltung, dem Standeswesen, dem Unterrichtswesen etc. eine wichtige Rolle spielen. Generell sind daher die Elemente Dokumente, elektronische Identifikation und Archivierung vorrangig zu beachten.

2. Prozesse und Dokumente

[Rz 2] Aus den verschiedensten Portalen des privaten Sektors sind wir gewohnt, dass im Unterschied zu Papier allein das «Blättern im Netz» und das «Klicken von Links» Auswirkungen im wirtschaftlichen Handeln hat und damit Waren bestellt bzw. Aktivitäten ausgelöst werden. Auch im Verwaltungshandeln gehen wir bei der Nutzung des Internet immer mehr von der expliziten und in Dokumenten festgehaltenen Form hin zum konkludenten Handeln. Dieser Trend wird sich mit der Zunahme an mobilen Geräten – man erwartet zweistellige Prozentsätze von Nutzern, die den Schwenk vom PC bzw. Laptop zu Tablet und Smartphone bei der Nutzung von Internet machen – verstärken und dies ist auch nach Möglichkeit zu unterstützen.

[Rz 3] Dennoch existiert ein deutlicher Unterschied zwischen dem prozessorientierten und dem dokumentorientierten Handeln. Dies vor allem in der Dokumentation und in der Nachweislichkeit, aber auch aus dem Blickwinkel der Sicherheit, des Übereilungsschutzes etc.

[Rz 4] Der grundsätzliche Unterschied zwischen den beiden Ansätzen liegt in den Zeitpunkten, den Abfolgen und damit im Nachweis des Willensaktes. Ganz allgemein ist festzustellen, dass Identifikation vor der Eingabe der bestimmenden Daten und Parameter durch den Benutzer stattfindet, wohingegen Dokumente mit Authentifizierung und Unterschrift nach dem Festlegen der Daten wirksam werden und damit auch unterschiedliche Eigenschaften umsetzen. Jedenfalls kann man mit dem Werkzeug «Dokumente und Unterschrift» Identifikation ebenfalls umsetzen. Umgekehrt ist dies nicht bzw. nur sehr eingeschränkt der Fall.

2.1. Anforderungen an Dokumente

[Rz 5] Dokumente, die eine Unterschrift tragen, legen die Vermutung nahe, dass die unterzeichnende Person den Inhalt des Dokumentes in einer gewissen Form bestätigt – z.B. mit dem Inhalt eines Vertrages Einverständnis erklärt. Es wird demnach implizit davon ausgegangen, dass die Inhalte des Dokumentes vor der Unterschrift entstanden sind und nicht verändert wurden. Dieser Umstand wird in der Praxis in unterschiedlichen Formen und Stufen sichergestellt. Eine Form dieses Festlegens ist das Herstellen zweier Exemplare und das Unterzeichnen beider Exemplare bzw. ähnliche bilaterale Prozeduren. Damit kann durch Übereinstimmung der außer Zweifel stehende Fall abgesichert werden. Sind verbindlichere Festlegungen erforderlich, dann kann eine Hinterlegung bei Dritten, der unverändertes Aufbewahren zusichern kann und entsprechendes Vertrauen genießt, eine Lösung sein.

[Rz 6] Ein weiterer Sicherheitsaspekt ist die Beglaubigung, die Identität der Person mit jener der Unterschrift feststellt. Diese Prozeduren sind im Papierfall notwendig, da eine Prüfung der Unterschrift nur bei Vorliegen eines Vergleichsmusters möglich ist und – wie der Fall des Unterschriftautomaten zur Unterzeichnung des Patriot Act[1] gezeigt hat – auch nur in sehr eingeschränkter Form, selbst, wenn graphologische Gutachten erstellt werden. Die Zeugenschaft bei der Unterschrift auf Papier hat demnach eine wesentliche Funktion.

[Rz 7] Der elektronische Fall stellt sich grundsätzlich etwas anders dar. Zum Zeitpunkt der Unterschrift (elektronische Signatur) sind aufgrund der eingesetzten Technologien[2] die Vollständigkeit und Unverändertheit des Dokumentes mit der Signatur besiegelt. Aus der Natur elektronischer Dokumente ist auch ein beliebiges Vervielfachen des signierten Dokumentes möglich. Es kann demnach nicht von einem Original im Sinne des Unikates gesprochen werden, womit Übergeberpapier, Banknoten, Wechsel etc. prima vista ohne zusätzliche, in der Regel komplexe Technologien nicht möglich sind.[3]

[Rz 8] Die elektronische Signatur ist allerdings mit folgenden drei wesentlichen Annahmen behaftet:

- Technologische Qualität: Die Qualität und die Art der Anwendung der Algorithmen muss Eigenschaften aufweisen, die ein Wiederholen bzw. Anwenden auf andere Daten ausschließt. Diese Anforderung trifft die Schlüssellängen und kryptographischen Algorithmen[4].
- Sicherung des Geheimnisses: Es muss vorzugsweise technisch – dies ist bei qualifizierten Signaturen auch vorgeschrieben – sichergestellt sein, dass ein Durchsickern des der Kryptographie zugrundeliegenden Geheimisses nicht möglich ist[5].
- Die Person, der eine elektronische Signatur durch technische Mittel – Wissen und Besitz[6] – zugeordnet ist, gibt diese Mittel nicht an Andere weiter. Diese Voraussetzung ist in einem gewissen Masse auch bereits in der Papierwelt existent, wie das zitierte Beispiel des Unterschriftenautomaten zeigt oder auch durch Blanko-Unterschriften verletzt wäre.

---

1 Unterschriftenautomat verlängert «Patriot Act», http://derstandard.at/1304553115212/Unterschriftenautomat-verlaengert-Patriot-Act.

2 Zur Technologie elektronische Signatur siehe etwa http://de.wikipedia.org/wiki/Digitale_Signatur.

3 Vgl. etwa elektronisches Geld http://de.wikipedia.org/wiki/Elektronisches_Geld.

4 Empfohlene Algorithmen und Parameter für elektronische Signaturen http://www.a-sit.at/pdfs/rtr-algorithms-20070601-de.pdf.

5 http://www.commoncriteriaportal.org/pps/.

6 http://www.commoncriteriaportal.org/files/ppfiles/pp0059b_pdf.pdf.

[Rz 9] Die Natur der Materie, die mathematische Einwegfunktionen erfordert und die Erkenntnisse der Komplexitätstheorie[7] sowie die Halbleitertechnologie[8] sagen uns, dass diese Aussagen nicht auf unbeschränkte Zeitdauer getroffen werden können[9]. Da aber auch Papierdokumente über sehr lange Zeiträume eher durch Referenz und das Wissen um die Dokumente Authentizität sichern und auch in diesem Fall – etwa bei verstorbenen Personen – sich die Prüfung schwierig bis unmöglich gestaltet, wird kein Grund gegeben sein, elektronischen Dokumenten andere Wirkungen beizumessen als den Papierdokumenten. Generell wird man ohnehin annehmen müssen, dass elektronische Dokumente eine allgemein höhere Sicherheit aufweisen als Papier.

[Rz 10] An sich treffen diese technologischen Aspekte in gleicher Weise auf den Bereich der Identifikation zu, doch haben sie dort einen deutlich anderen Stellenwert, da wegen der Tatsache «Identifikation findet vorab statt» kaum Auswirkungen auf Transaktionen der Zukunft zu bedenken sind. Die Auswirkungen betrieblicher Art sind dennoch auch im Falle der elektronischen Identifikation zu bedenken. Daher sind technologische Zertifizierungs- und Anerkennungsprogramme vor allem im Bereich der Signatur existent[10].

[Rz 11] Die genannten Eigenschaften und Verschränkungen machen verständlich, dass die Europäische Rechtsordnung bereits 1999 mit der Signaturrichtlinie[11] auf diese Themen eingegangen ist und dass mit der nunmehr in Verhandlung befindlichen Regulierung für elektronische Identifikation und Signaturen ein einheitlicher und die beiden Themen umspannender rechtlicher Zugang gewählt wird[12].

3. Natürliche und nicht natürliche Personen

[Rz 12] In der angreifbaren Welt ist die Trennung dieser beiden Begriffe augenscheinlich, da nur natürliche Personen auftreten können und nicht natürliche Personen eben zwangsläufig durch solche vertreten werden müssen. Erst durch das vorhin erwähnte «Weitergabeargument» kann man im elektronischen Fall theoretisch auch einer nicht natürlichen Person die Funktionen Identifikation und Signatur zuordnen. Bei genauerer Betrachtung ist allerdings das «Weitergeben» der Authentifizierungsmechanismen ebenfalls als eine Form einer Vollmacht anzusehen. Eine allerdings relativ ungünstige Form, da diese die tatsächlich einschreitende natürliche Person verdeckt und daher eine Prüfung, ob die Person zu Recht einschreitet oder eine Befugnis dafür eben nicht vorliegt, nicht mehr möglich ist. In der nachfolgenden Abhandlung wird von nicht natürlichen Personen gesprochen und nicht der Begriff der juristischen Person verwendet, da ersterer etwas weiter greift (vgl. auch E-GovG[13]).

[Rz 13] Es wird damit verdeutlicht, dass es sich damit um ein Innehaben von technischen Mitteln handelt und die Wirkung – so man Signaturen und Identifikationen auch nicht natürlichen Per-

7 http://amadousarr.free.fr/crypto/PracticalCryptography.pdf.

8 The State-of-the-Art in IC Reverse Engineering, http://dl.acm.org/citation.cfm?id=1617758.

9 Selecting Cryptographic Key Sizes, http://infoscience.epfl.ch/record/164526/files/NPDF-22.pdf.

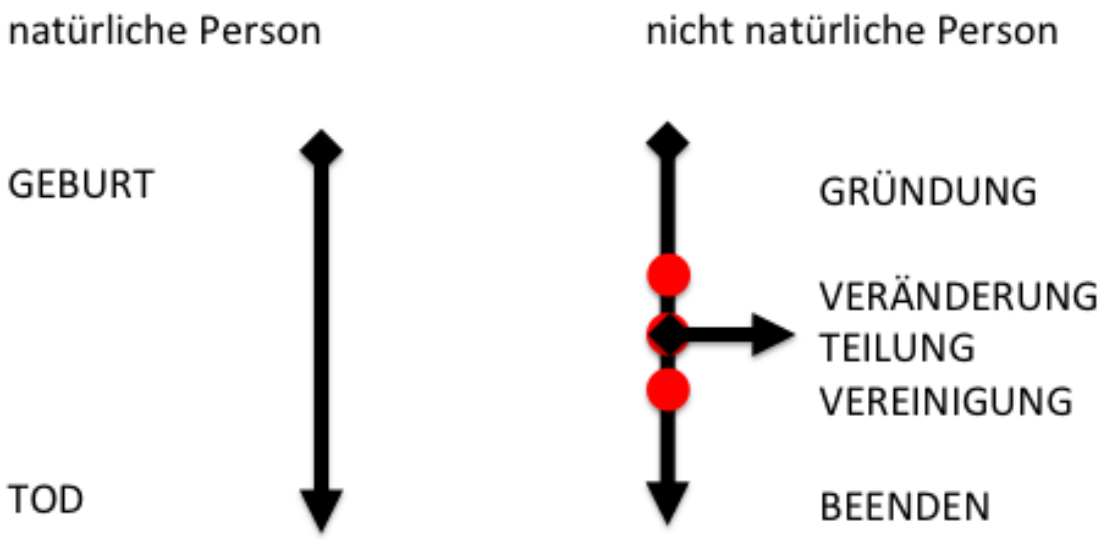
10 http://www.commoncriteriaportal.org/files/ppfiles/pp0059b_pdf.pdf.

11 Signaturrichtlinie, http://www.signatur.rtr.at/de/legal/directive.html.

12 Digital Agenda, http://europa.eu/rapid/press-release_IP-12-558_en.htm.

13 E-GovG, http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230.

sonen zuordnet – die des Innehabens wird. Dieses Gedankengebäude hätte allerdings erhebliche Komplikationen bei der Abbildung in die angreifbare Welt.



[Rz 14] Wie aus der vorhergehenden Skizze ersichtlich, sind nicht natürliche Personen wesentlich dynamischer zu sehen und zeigen weder in ihrer Art, noch in der Zuordnung von natürlichen Personen zu diesen eine dauerhafte Situation.

[Rz 15] In der Praxis führte dies zu bestandgebenden Daten in der Verwaltung[14]. In der Umsetzung in elektronischer Form führt dies zu einigen Besonderheiten etwa dann, wenn man ein Modell des Innehabens von Identität und Signatur zulässt, da damit die technischen und rechtlichen Zuordnungen von natürlichen zu nicht natürlichen Personen zwangsläufig auseinanderlaufen. Aus dieser Sicht ist «dem Modell der Vollmachten[15]» zweifelsfrei der Vorzug zu geben, da es mit den bestandsgebenden Daten gekoppelt werden kann und damit in gleicher Aktualität wirksam wird. Zudem ist dieses Modell auch auf Beziehungen zwischen natürlichen Personen anwendbar. Solche Beziehungen sind etwa bei noch nicht geschäftsfähigen Kindern, besachwalteten Personen, aber auch im gewillkürten Fall oder im Fall einer gesetzlich geregelten Vertretung durch Rechtsanwälte etc. notwendig.

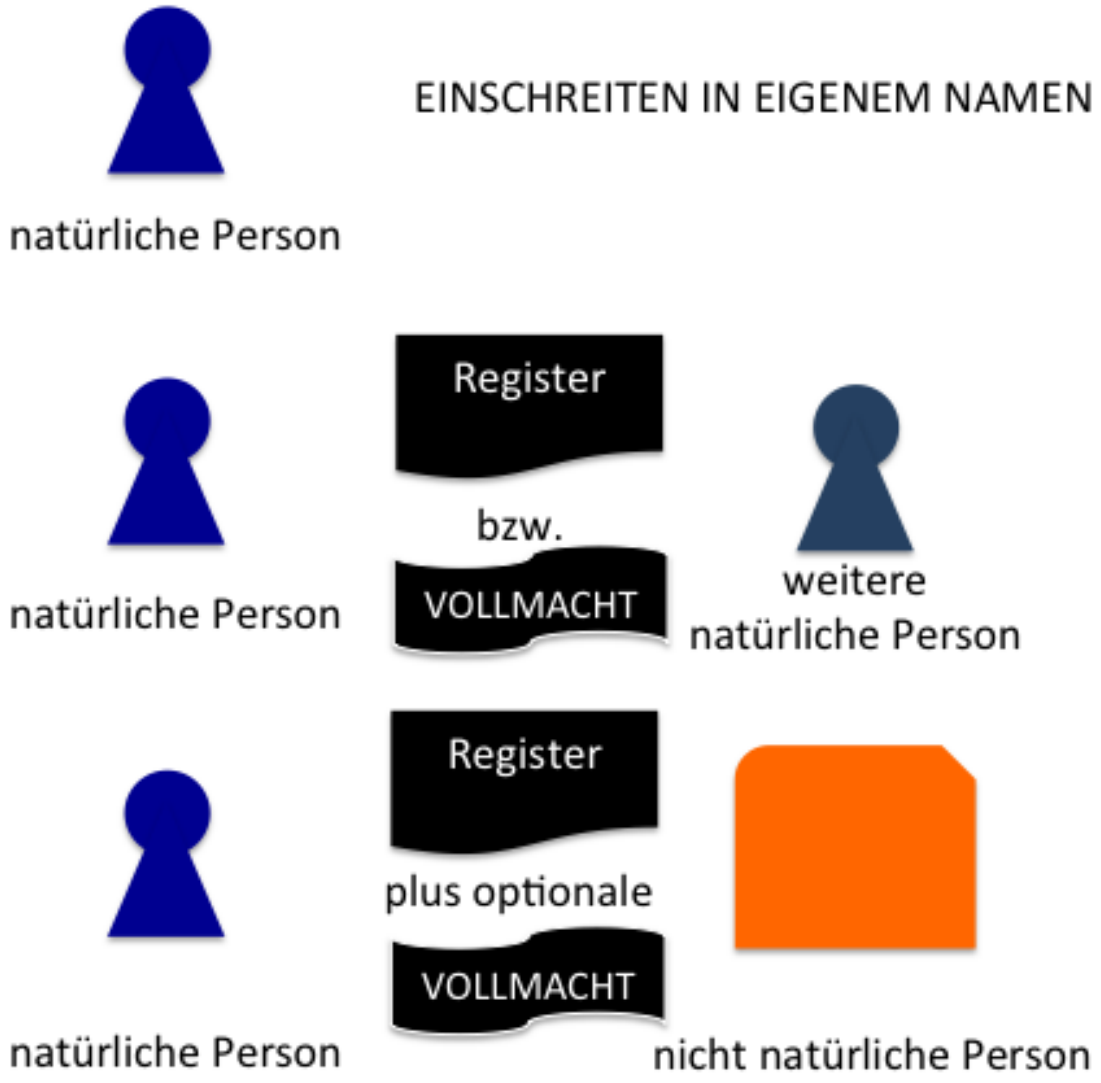
[Rz 16] Insgesamt entsteht damit ein Bild des Einschreitens bzw. der Identifikation, wie nachfolgend dargestellt. Die Unterschrift bleibt – wie auch in der Papierwelt – der natürlichen Person zugeordnet und vorbehalten. Elektronische Signaturen neben der qualifizierten Signatur[16] sind dabei als technische Sicherung der Ausfertigung ähnliche einem Firmenstempel etc. zu sehen, die bei aller technischen Güte eine besondere Regelung vertraglicher oder gesetzlicher Natur benötigen,

14 Firmenbuch, http://www.justiz.gv.at/internet/html/default/8ab4a8a422985de30122a90fc2ca620b.de.html.

15 Das österreichische E-Government ABC, http://oesterreich.gv.at/site/5618/default.aspx.

16 Signaturgesetz, http://www.signatur.rtr.at/de/legal/sigg.html.

um eine besondere Wirkung zu entfalten. Eine derartige besondere Wirkung wurde beispielsweise mit der Amtssignatur[17] bzw. mit der Signatur aus Archiven[18] der Justiz eingeräumt.



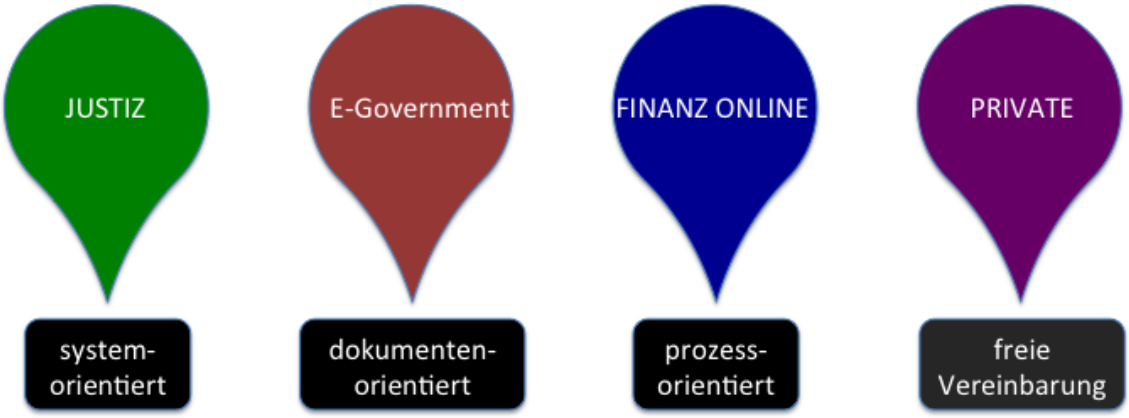
[Rz 17] Im elektronischen Umfeld wird Identifikation in vielen Fällen mit den mit der Identität verbundenen Attributen vermengt bzw. verbunden. An dieser Stelle werden in vielen Fällen Datenschutzprobleme releviert. Daher sollte man die Trennung von Attributen und Identifikation in jedem Fall ermöglichen – auch dann wenn diese technisch gemeinsam auftreten z.B. bei der Kombination vom elektronisch ausgestatteten Personalausweis und der elektronischen Identifikation. Eine derartige Umsetzung könnte durchaus als «Datenschutz by Design» qualifiziert werden.

17 Amtssignatur, http://www.oesterreich.gv.at/site/5318/default.aspx.

18 Urkundenarchiv, http://www.notar.at/notar/de/home/infoservice/lexikon/lexikonu/urkundenarchiv/.

4. Verwaltungslandschaften in Österreich

[Rz 18] Österreich hat eine langjährige Erfahrung mit der Einführung von elektronischen Möglichkeiten in die Verfahren der Verwaltung. Generell wurden hier drei Ansätze seit den 90er Jahren verfolgt in der Justiz, in der Finanzverwaltung und in der allgemeinen Verwaltung. Um dabei auch rasch erfolgreich zu sein, waren diese Ansätze zu Beginn parallel entstanden und daher auch unterschiedlich und sind es in manchen Aspekten auch heute noch. Diese Situation entstand vor allem aus den unterschiedlichen Zugängen heraus.



[Rz 19] Im Bereich der Justiz war Österreich ein deutlicher Vorreiter und die Anwendungen auf den Basiselementen Grundbuch, Firmenbuch später auch allgemeines Urkundenarchiv aufgebaut und diesen systemorientierten Ansatz mit dem Kommunikationssystem «elektronischer Rechtsverkehr» ergänzt. Dadurch ist ein sehr homogenes System entstanden, das die professionellen Einrichtungen der Justiz nahezu vollständig umspannt.

[Rz 20] Im Finanz- und Steuerbereich kommen durch die steuerbaren Personen viele hinzu, die nicht dem Kreis der professionellen aus diesem Bereich zuzurechnen sind. Daher wurde in diesem Bereich ein eher prozessorientierter Ansatz verfolgt.

[Rz 21] Zeitlich als letzter wurde der Bereich der allgemeinen Verwaltung systematisch umgesetzt und die gesetzliche Basis geschaffen[19]. In diesem Bereich besteht die größte Vielfalt und damit auch die breiteste Anforderung an die Flexibilität.

[Rz 22] Um bestmöglichen Service für Bürgerinnen und Bürger anzubieten, ist eine Konvergenz dieser Bereiche vor allem in den Bereichen, die ähnliche Aufgaben lösen, wichtig. Diese Konvergenz wurde und wird schrittweise umgesetzt:

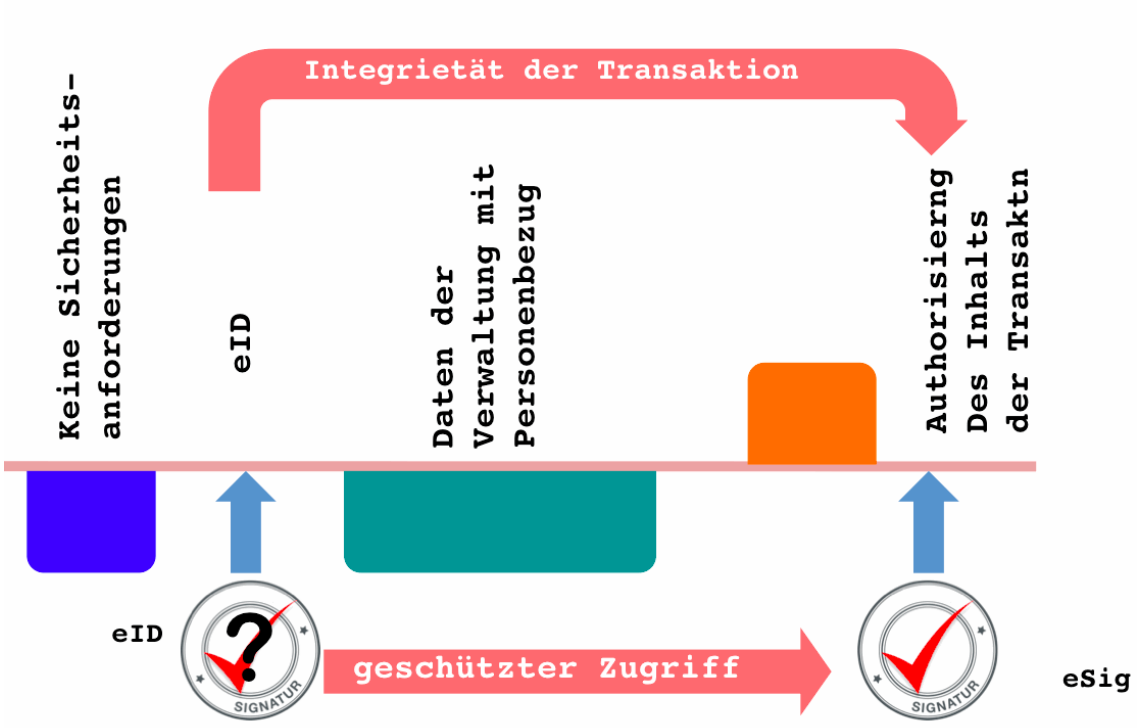
- Signatur von ausgehenden Dokumenten: Diese sind zwar auf unterschiedlichen Gesetzesgrundlagen umgesetzt, doch ist das Resultat in allen angesprochenen Bereichen technisch gleich. Damit sind diese auch für den Benutzer zwar optisch unterschiedlich, aber praktisch ident, wodurch auch die allfällige Prüfung der Signaturen über eine gemeinsame Plattform beim Telekom Regulator erfolgen kann.

19 E-GovG, http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230.

- Infrastruktur der elektronischen Identifikation: Auch hier sind die technischen Elemente gleichartig. Im Bereich der allgemeinen Verwaltung ist die «Bürgerkarte» als qualifizierte Methode der elektronischen Identifikation festgelegt und mit diesem Werkzeug kann unabhängig vom Anwendungsbereich auf Daten in der Verwaltung zugegriffen werden.
- Signatur von einkommenden Dokumenten: Die Gesetzeslage in Österreich sieht qualifizierte Signaturen in einer für jedermann erkennbaren und europaweit anerkannten Form vor. Für die übrigen Formen der Signatur von Bürgerinnen und Bürgern gibt es keinen Standard der Erkennung bzw. von Eigenschaften. Damit ist die Verwendung der gewöhnlichen Signatur sehr eingeschränkt.
- Zustellung von Dokumenten: Im Bereich der rechtswirksamen Zustellung folgen die drei genannten Bereiche unterschiedlichen gesetzlichen Rahmenbedingungen. Damit ist die Zusammenführung dieser Bereiche, obschon sie besondere Potentiale hat, langwieriger. Da sie sich aber aus der Sicht der Bürgerinnen und Bürger nicht wirklich unterscheiden, sind gemeinsame Plattformen der Zustellung äußerst wichtig, um Synergien auch in der Praxis umsetzen zu können. Für die Bereiche Justiz und allgemeine Verwaltung wurde dies durch die Übergänge zu und vom elektronischen Rechtsverkehr auch bereits vorangetrieben.

4.1. eID und Signaturen in Europa

[Rz 23] Es wurde bereits eingangs festgehalten, dass Identifikation und Signaturen in einem engen Zusammenhang stehen und deren Funktion daher auch oft vermischt werden. Daher wird hier noch einmal in einer Skizze die Funktion zusammengefasst.



[Rz 24] Bei der Umsetzung handelt es sich für beide Bereiche um Sicherheitstechnologien und im Falle der qualifizierten Umsetzung um annähernd die gleichen Technologien, wobei jeweils andere Eigenschaften der Technologie genutzt werden. Bei der Signatur steht die Bindung zu einem Dokument und bei der Identifikation die Bindung zu einer Person im Vordergrund. Dabei ist es augenscheinlich, dass die Bindung zur Person auch im Signaturfall Grundbedingung ist. Bei einer Identifikation ist die Bindung zu einem Prozess der Ausgangspunkt. In der digitalen Welt kann dies nur über einen Datensatz geschehen. Dieser Datensatz – weil nicht im primären Interesse der BenutzerIn meistens nicht gesehen oder wahrgenommen – als Dokument interpretiert zeigt den engen Zusammenhang zur Signatur bzw. den Umstand, dass aus der Sicht der Technologie Signatur und Identifikation kaum unterscheidbar sind.

4.2. Cloud eID und mobile Geräte

[Rz 25] Bereits heute verwenden viele BürgerInnen mobile Geräte – Smartphones und Tablets – und wir dürfen erwarten, dass dieser Trend voranschreiten wird und vor allem im privaten Bereich die Rolle der traditionellen PCs und Laptops zurückdrängen wird.

[Rz 26] Damit sind wir mit einer Reihe von Situationen konfrontiert:

- Derartige Geräte haben keine wirklich verwendbaren Schnittstellen für externe Gräte wie etwa Chipkartenleser.
- Derartige Geräte sind praktisch immer dem Internet und damit allfälligen Gefahren ausgesetzt.
- Ein Update aufgrund von sicherheitstechnischen Notwendigkeiten (Patches) ist zumindest zum heutigen Zeitpunkt nicht allgemein üblich und damit gibt es auch sehr viele Geräte mit technisch alten Systemen. Oft werden die Systeme überhaupt erst mit einer neuen Hardware erneuert und in vielen Fällen ist eine Kompatibilität neuer Systemversionen gar nicht im Interesse der Hersteller.
- Die Geräte sind oft ohne Bewusstwerden der Benutzer in Cloud Applikationen eingebunden und oft von diesen aus auch steuerbar.
- Mobile Geräte sind nur beschränkt anpassbar und die Nutzung der Systemfunktionen ist kaum einem Standard unterworfen.

[Rz 27] Damit erfordert jede Art von Sicherheitstechnologie einen größtmöglichen Abstand vom System, um Sicherheit und Nachhaltigkeit zu ermöglichen.

[Rz 28] Im Rahmen des STORK Projektes wurde auch dieser Aspekt eingehend betrachtet und um den genannten Problemen entgegenzuwirken, wurde die «Handy-Signatur» entwickelt und dann in Österreich durch den Provider der Zertifikate für die Bürgerkarte auch umgesetzt.

[Rz 29] Das Konzept der Handy-Signatur hat auch bei konventionellen Geräten (PC bzw. Laptop) klare Vorteile und die Zahl der Bürgerkarten auf dieser Basis hat in kurzer Zeit etwa das Doppelte der Zahl der eCard basierten Bürgerkarten erreicht. Damit ist zu erwarten, dass der Trend der mobilen Geräte dabei noch gar nicht die Hauptrolle gespielt hat.

[Rz 30] Technisch gesehen sind Signaturen mit Karte und Handy gleichartig, wobei das Handy als Tastatur für die PIN-Eingabe mit «sehr langem Kabel» zum Signaturerstellungsgerät, welches in Form eines HSM im Safe des Signaturproviders befindet, angesehen werden kann.

[Rz 31] Mit dem SMS-Kanal für die PIN, die einmalig verwendet als TAN ausgebildet ist, und dem Handy ist ein völlig getrenntes System zum eigentlichen Verarbeitungssystem und damit hohe Sicherheit gegeben. Zudem wird der Verlust des Mobiltelefons in der Regel sehr rasch bemerkt wer-

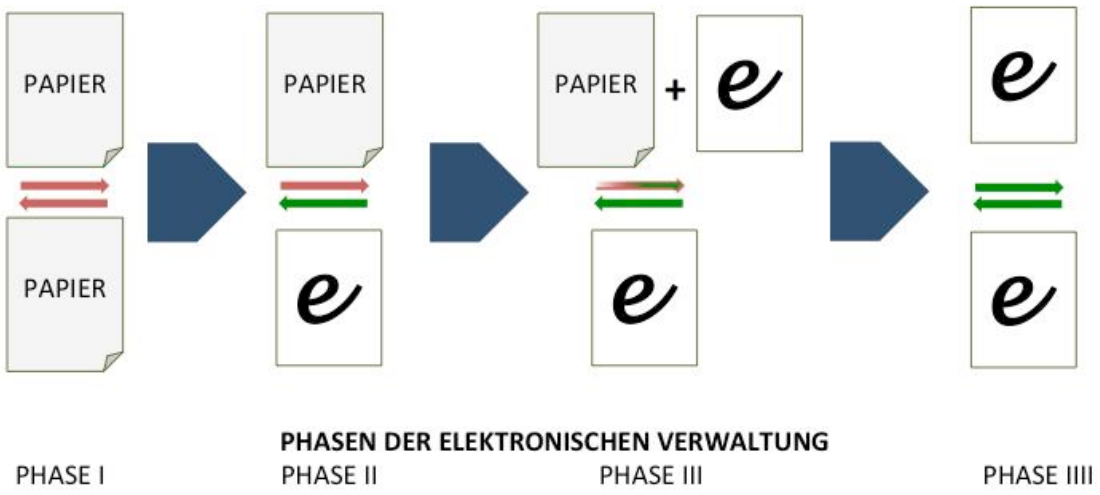
den, was zur Sicherheit beiträgt, da kryptographische Schlüssel im HSM und nicht im Mobiltelefon vorliegen und damit ein Widerruf nach Verlust eine wesentlich bessere und vor allem gesichert unmittelbarere Wirkung hat, als bei Karten.

[Rz 32] Eine potentielle Gefahr stellt die Nutzung ein und desselben Gerätes für den Internetprozess und für die Handy-Signatur dar. Dies ist nicht anzuraten und liegt in der Verantwortung des Nutzers. Anzumerken ist allerdings, dass selbst bei Missachten dieser Regel durch die Trennung des SMS vom Internet Kanal eine deutlich höhere Sicherheit verbleibt, als dies bei konventionellen Systemen der Fall ist.

5. Zyklen der elektronischen Verwaltung

[Rz 33] Ziel der elektronischen Verwaltung ist die effiziente Umsetzung und das Vereinfachen der Verwaltungsprozesse. Dies kann nur durch Vermeidung bzw. Verringerung von manuellen Schritten geschehen.

[Rz 34] Dieser Prozess muss, da es sich bei Anbringen und Antworten jeweils um Informationen handelt, die vornehmlich von der Verwaltung verarbeitet werden, in einem Vermeiden von Papierdokumenten münden.



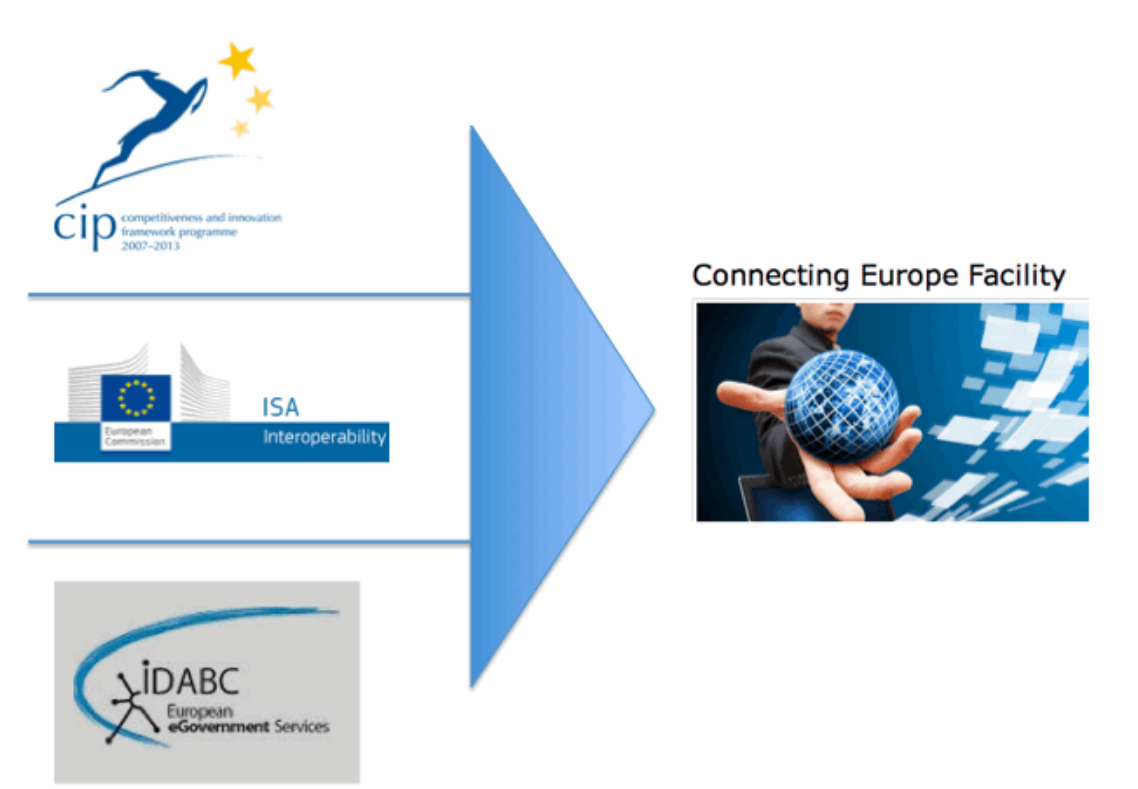
[Rz 35] In diesem Phasenmodell sind die zentralen Parameter:

- Elektronische Identifikation: diese ermöglicht das gesicherte Zuordnen und Verwenden von Daten, die im System für eine Person vorliegen. Es werden damit keine redundanten Eingaben notwendig und Eingabe von Daten muss nur einmal erfolgen. Dies kann unabhängig vom Verwaltungsvorgang an sich erfolgen.
- Elektronische Zustellung: damit können Ergebnisse in rechtswirksamer Form an den Antragsteller zurück übermittelt werden.
- Gesicherte Ablage: Archive und Langzeitarchive tragen wesentlich zur Verwaltungssicherheit bei und erlauben es, das BackOffice auf elektronische Prozesse umzustellen.

[Rz 36] Letztlich kommt es darauf an, dass die Verwaltungsunterworfenen das Recht bekommen, Eingaben und Dokumente elektronisch abzugeben und zu erhalten, um diese auch wieder im Ver-

waltungskontext verwenden zu können. Dies ist essentiell, wenn die BackOffice Systeme nicht verbunden sind. Sofern dies aus Datenschutz- oder anderen Gründen nicht verhindert werden sollte, ist eine derartige Vernetzung durch den Portalverbund innerhalb Österreich weithin gegeben. Im grenzüberschreitenden Verkehr sieht dies aber deutlich anders aus und es werden auch in diesem Bereich noch über lange Perioden Dokumente erforderlich sein.

[Rz 37] Einheitliche bzw. interoperable Formate und Prozesse werden auch auf der Europäischen Ebene mit hohen Prioritäten versehen.



[Rz 38] Mit der Umsetzung der Digitalen Agenda[20] sollen ab der nächsten Budgetperiode die unterschiedlichen und – teilweise aus der Natur der Sache und aus den Interessenslagen – parallel gewachsenen Aktivitäten aus den Large Scale Pilots[21] sowie aus den Erkenntnissen der Interoperabilitätsprogramme[22] in der Infrastrukturmaßnahme CEF[23] zusammengefasst werden.

[Rz 39] Dabei ist Österreich in mehrerlei Hinsicht ein Vorreiter. In besonderer Weise im Bereich der übergreifenden und grenzüberschreitenden Verwendung von Sicherheitstechnologien, die Nachhaltigkeit in besonderer Weise prägen. Die gesetzliche Verankerung der Anerkennung von elek-

20 Digitale Agenda http://ec.europa.eu/digital-agenda/.

21 CIP Programm http://ec.europa.eu/cip/.

22 ISA Programm http://ec.europa.eu/isa/.

23 CEF https://ec.europa.eu/digital-agenda/en/connecting-europe-facility.

tronischer Identifikation ist dabei nur ein Beispiel, das sich nun auch in den Prinzipien der EU-Gesetzgebung bzw. in den Diskussionsvorlagen wiederfindet.

6. Zusammenfassende Bemerkungen

[Rz 40] Effiziente elektronische Verwaltung erfordert ein hohes Maß an Interoperabilität und an Vereinfachung der Prozesse. Dokumente haben aus ihrer Natur eine breite Vielfalt und erfordern wegen des Anspruches der Langlebigkeit besondere Aufmerksamkeit. Beliebige Kopierbarkeit elektronischer Dokumente verändert die Bedeutung des Innehabens von Dokumenten und erfordert besondere Aufmerksamkeit bei der Identifikation bei Transaktionen und Prozessen.

[Rz 41] Der Anspruch von Dokumenten auf Authentizität, aktuell und unverändert zu sein sowie auf Haltbarkeit kann durch die Kombination von Archiven und Signaturen erreicht werden. Dabei hat der Bereich der Justiz eine lange Erfahrung besonders im Bereich von Urkunden erarbeitet.

[Rz 42] Ausweitung und bereichsübergreifende Verwendung erfordert eine Ergänzung in Richtung offener und verteilter Systeme, wodurch der Signatur und der Identifikation ein noch höherer Stellenwert zukommt. Dies muss durch Zustellsysteme ergänzt werden, die Bereichsgrenzen überwinden können, um die Vision des Rechtes auf elektronische Dokumente für BürgerInnen und Unternehmen zu ermöglichen.

[Rz 43] Innovation spielt in diesem Umfeld eine besondere Rolle, da mit den neuen Technologien und Paradigmen – Mobile Geräte, Cloud Computing sind dabei aktuelle Schlagworte – laufend neue Herausforderungen in einer mit den bestehenden Gedankenwelten und Systeme verträglichen Weise bewältigt werden müssen.

Reinhard Posch, Chief Information Officer des Bundes, Ballhausplatz 2, A-1014 Wien, Reinhard.posch@cio.gv.at, https://www.digitales.oesterreich.gv.at/.