

Elektronische Signatur I

Wahlfachkorb Computer und Recht
SoSe 2019

Peter Kustor

Bundesministerium für Digitalisierung und Wirtschaftsstandort
Leiter der Abteilung I/A/2 –
Digitales und E-Government – Internationale Beziehungen und Logistik

Peter.Kustor@bmdw.gv.at

 @PeterKustor

Agenda

1. „Unterschrift“ - „Elektronische Unterschrift“
2. Praktische Demonstration
3. Technischer Hintergrund
4. Detaillierte Darstellung des Rechtsrahmens:
EU (eIDAS-VO) und national (SVG)
5. Bürgerkartenkonzept - Elektronische Signatur
und Identitätsmanagement
6. Handy-Signatur
7. Verfahrensrechtliche Anforderungen,
Amtssignatur

„Unterschrift“ - Wikipedia

„**Unterschrift** (auch **Signatur**, von lateinisch *signatum* „das Gezeichnete“ zu *signum* „Zeichen“) ist die handschriftliche, eigenhändige Namenszeichnung auf Schriftstücken durch eine natürliche Person mit mindestens dem Familiennamen. Die Unterschriftsleistung ist zur Gültigkeit von Rechtsgeschäften, die mindestens der Schriftform bedürfen, erforderlich.“

„Unterschrift“ - VwGH

„Eine "Unterschrift" ist dabei ein Gebilde aus Buchstaben einer üblichen Schrift, aus der ein Dritter, der den Namen des Unterzeichneten kennt, diesen Namen aus dem Schriftbild noch herauslesen kann; eine Unterschrift muss nicht lesbar, aber ein "individueller Schriftzug" sein, der entsprechend charakteristische Merkmale aufweist. Die Anzahl der Schriftzeichen muss der Anzahl der Buchstaben des Namens nicht entsprechen. Eine Paraphe ist keine Unterschrift“

(Erkenntnis vom 4.9.2000 Zl. 98/10/0013 mit Hinweis auf Walter/Mayer, Grundriss des österreichischen Verwaltungsverfahrenrechts, 7. Auflage, Rz 190 ff, mit Judikaturhinweisen)

„Unterschrift“ - OGH

„Das Gebot der Schriftlichkeit bedeutet im allgemeinen "Unterschriftlichkeit", es sei denn, das Gesetz sieht ausdrücklich eine Ausnahme vor. Das Erfordernis der Schriftform soll gewährleisten, dass aus dem Schriftstück der Inhalt der Erklärung, die abgegeben werden soll, und die Person, von der sie ausgeht, hinreichend zuverlässig entnommen werden können.“

(zB 1Ob525/93 vom 2.7.1993)

„Schriftlichkeit“ - § 886 ABGB

„Ein Vertrag, für den Gesetz oder Parteiwille **Schriftlichkeit** bestimmt, kommt durch die **Unterschrift** der Parteien oder, falls sie des Schreibens unkundig oder wegen Gebrechens unfähig sind, durch Beisetzung ihres gerichtlich oder notariell beglaubigten Handzeichens oder Beisetzung des Handzeichens vor zwei Zeugen, deren einer den Namen der Partei unterfertigt, zustande. Der schriftliche Abschluß des Vertrages wird durch gerichtliche oder notarielle Beurkundung ersetzt. **Eine Nachbildung der eigenhändigen Unterschrift auf mechanischem Wege ist nur da genügend, wo sie im Geschäftsverkehr üblich ist.**“

Wirkung der Unterschrift: § 294 ZPO

„Auf Papier oder elektronisch errichtete Privaturkunden begründen, sofern sie von den Ausstellern **unterschrieben** oder mit ihrem gerichtlich oder notariell beglaubigten Handzeichen versehen sind, **vollen Beweis** dafür, **dass die** in denselben **enthaltenen Erklärungen von den Ausstellern herrühren.**“

- „Qualifizierte Echtheitsvermutung für den Erklärungsinhalt“

Funktionen einer Unterschrift

- **Identitätsfunktion:** Der Aussteller der Urkunde wird erkennbar
- **Echtheitsfunktion:** Gewähr, dass die Willenserklärung vom Aussteller stammt
- **Beweisfunktion:** Beweisführung wird durch die Urkunde erheblich vereinfacht
- **Abschlussfunktion:** Bringt zum Ausdruck, dass die Willenserklärung abgeschlossen/vollendet ist
- **Warnfunktion:** Schützt den Unterzeichner vor Übereilung

Elektronische Signatur?



Das ist eine beliebige E-Mail mit einer w
 Beste Grüße,
 Peter Kustor

**Bundesministerium für Digitalisierung
 und Wirtschaftsstandort**
 Sektion I – Digitalisierung und E-Government
 Abteilung I/A/2 – Internationale Beziehungen und I

MinR Mag. Peter Kustor
 Leiter der Abteilung

+43 1 711 00-802860
 Postadresse: Stubenring 1, 1010 Wien, Österreich
 Büroadresse: Vordere Zollamtsstraße 5/305, 1030 W
peter.kustor@oesterreich.gv.at
[facebook.com/bmdw.gv.at](https://www.facebook.com/bmdw.gv.at)
bmdw.gv.at

Besuchen Sie uns
 auf [DigitalAustria](http://DigitalAustria.at)
 im März 2019



NEELIE KROES

VICE-PRESIDENT OF THE EUROPEAN COMMISSION

Brussels, 14 October 2014

Dear Jean-Claude,

I am writing to you from the launching event on the Regulation on electronic identification and trust services (eIDAS) where I am discussing with representatives of industry, the Italian Presidency and the European Parliament, the business and growth opportunities for Europe in a fully integrated digital market.

I believe that the European Union should modernise and turn all public administrations digital. And I believe that the Commission should lead by example and become paperless both in-house, and when interacting with the public.

So my question to you is: will you accept this challenge to make the European Commission truly digital by using e-invoices, e-procurement and e-signatures under your Presidency – and call for the other EU institutions to do the same?

If we want a true Digital Single Market, we need digital EU institutions too. This should be a priority to serve our citizens, businesses and public administrations in a digital society. To this end, we can count on and leverage plenty of European good practices and technologies – and the private sector's role will be key in this.

As the outgoing digital Commissioner, I am confident that I have laid the foundation for you to build a digitally-strong house. The eIDAS Regulation was the missing stone to make cross-border electronic transactions across Europe a reality. With eIDAS we have accomplished a major milestone – and we are well ahead of the US in this.

As I like to practise what I preach, I am signing this letter electronically, with my mobile, and using technology developed thanks to the EU funded STORK project which is currently used by citizens in Austria.

Yours sincerely,

	Signature	Neelie Kroes
	Date/Time-UTC	2014-10-14T13:01:23.897Z
	Verification	Information about the verification of the electronic signature can be found at: https://www.e-signature-verification.eu
Note	This document is signed with a qualified electronic signature.	

President-Elect Jean-Claude Juncker
 Commission

+32-2) 299 24 00 - FAX (+32-2) 296 04 09

E-Kommunikation



- Vergleichbar mit einer Postkarte, kann am Postweg **gelesen** und **verändert** werden
 - Postkarte: Postmitarbeiter, ...
 - E-Mail: Systemadministratoren, Hacker, ...
- Ungewissheit des Gegenübers

Authentizität von Urheber & Daten

- Zuordnung der Daten zum Unterzeichner
- Schutz vor Abstreiten durch Unterzeichner
- Sicherung der signierten Daten vor Manipulation
 - am Übertragungsweg
 - durch den Empfänger



Dokumente elektronisch unterschreiben (Kaufverträge, etc.)

- bislang m
Dokumen
– ausdi
– händi
– einsc
Brief

PDF-Signatur

PDF-Dokument auswählen und durch Klicken auf "Karte" oder "Handy" signieren!

Signieren: PDF Dokument ▾

Dokument *: C:\fakepath\Musterbr

 Handy  Karte

- das geht auch schneller und komfortabler (mit Ihrer Handy-Signatur)
 - auf www.buergerkarte.at/pdf-signatur wird das zu unterschreibende Dokument hochgeladen und gleich elektronisch unterschrieben,
 - Dazu suchen Sie das zu unterschreibende Dokument über die Schaltfläche „Durchsuchen“ und wählen anschließend das Handy per Mausklick.

Dokumente elektronisch unterschreiben

Zum Unterschreiben geben Sie nach Auswahl des zu unterschreibenden Dokuments Ihre Mobiltelefonnummer und das von Ihnen bei der Aktivierung der Handy-Signatur gewählte Passwort ein.

PDF-Signatur
Signatur wird erstellt...

Signieren: PDF Dokument ▾

Dokument *: C:\fakepath\Musterbr

Mobiltelefonnummer: 0650*****

Signatur Passwort: ●●●●●●●● 



[Signatur abbrechen](#)

Dokumente elektronisch unterschreiben

Sie bekommen nun einen fünf Minuten gültigen TAN-Code zugesendet und geben diesen in das entsprechende Formularfeld ein. Damit bestätigen Sie, dass Sie nicht nur das Passwort wissen, sondern auch das Mobiltelefon gerade in Ihrem Besitz haben.

The screenshot shows a web interface for PDF signing. The title is "PDF-Signatur" and the status is "Signatur wird erstellt...". On the left, there are two main sections: "Signieren:" with a dropdown menu set to "PDF Dokument", and "Dokument *:" with a text input field containing "C:\fakepath\Musterbr" and a "Durchsuchen" button. On the right, there is a "Vergleichswert: tm74XP0X9z" and "Signaturdaten" section. Below this, the "TAN:" label is followed by a text input field containing "9wt2fy", which is highlighted by a red arrow. At the bottom right, there is a red circular icon with a white 'A', and the text "Eigenes Fenster" and "Hilfe". A blue link "Signatur abbrechen" is located at the bottom left of the right-hand panel.

Dokumente elektronisch unterschreiben

Machen Sie den TAN-Code eingeben und damit das Dokument

unterschriebene und damit

PKW-Kaufvertrag (Mustervertrag Autoverkauf)

zwischen Verkäufer: Heinz Gruber
(Anschrift) Grubenweg 12, 1020 Wien
Telefon

und Käufer: Beate Schneider
(Anschrift) Burgsteig 21, 1200 Wien
Telefon

Verkaufsgegenstand ist nachfolgend genanntes Kraftfahrzeug

Marke : VW
Typ : Polo
Fahrgestellnr. : 5646421154
Laufleistung : 10000
Erstzulassung : 05/2007
amtl. Kennz. : W – 1002A
TÜV bis : 07/2010
AU bis :
Ausstattung : Navi...
.....

Gewährleistung und Garantie:

Der Kaufpreis beträgt 10000 € und ist bei Übergabe des Fahrzeuges fällig.

Ort, Datum, Unterschrift Verkäufer:

Signaturwert	2e6PGYB809aZu30klFibvHSf+yzL2zUIJmUfx7+rcRnL45rv9lft8RpK+VtFs3Tvi5tCRDHWFO0BxMahJd98aA==	
	Unterzeichner	Max Mustermann
	Aussteller-Zertifikat	CN=a-sign-premium-mobile-03,OU=a-sign-premium-mobile-03,0=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,CAAT
	Serien-Nr.	655302
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	etsi-bka-atrust-1.0:ecdsa-sha256:sha256:sha1
Prüfinformation	Signaturprüfung unter: http://www.signaturpruefung.gv.at	
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument ist gemäß § 4 Abs. 1 Signaturgesetz einem handschriftlich unterschriebenen Dokument grundsätzlich rechtlich gleichgestellt.	
Datum/Zeit-UTC	2014-02-07T13:38:55Z	

SIGNATUR: DOWNLOAD

signiert!

ur-Vorgang ist abgeschlossen. Das signierte

t kann nun heruntergeladen werden.

Der Download ist nur einmalig möglich. Das Dokument

am Server gespeichert.

Das Dokument herunterladen



Dokumente elektronisch unterschreiben

Was in der Papierwelt Ihre Unterschrift ist, ist in der elektronischen Welt der „Signaturblock“, welcher die notwendigen Informationen enthält, um die Absenderin bzw. den Absender zu identifizieren und das Dokument dahingehend zu prüfen, ob keine ungewollten Änderungen am Übertragungsweg geschehen sind.

Ausstattung : Navi...

Gewährleistung und Garantie:

Der Kaufpreis beträgt 10000 € und ist bei Übergabe des Fahrzeuges fällig.

Ort, Datum, Unterschrift Verkäufer:

Signaturwert	2e6PGYBsQ9aZu3QklfibvHSf+yzL2zUIJmUfx7+rcRnL45rv9lft8RpK+VtFs3Tvi5tCRDHPQ0BxMAHJd98aA==	
	Unterzeichner	Max Mustermann
	Aussteller-Zertifikat	CN=a-sign-premium-mobile-03,OU=a-sign-premium-mobile-03,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	655302
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	etsi_bka_atrust_1.0:ecdsa-sha256:sha256:sha256:sha1
Prüfinformation	Signaturprüfung unter: http://www.signaturpruefung.gv.at	
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument ist gemäß § 4 Abs. 1 Signaturgesetz einem handschriftlich unterschriebenen Dokument grundsätzlich rechtlich gleichgestellt.	
Datum/Zeit-UTC	2014-02-07T13:38:55Z	

Signaturprüfung ganz einfach über www.signaturpruefung.gv.at

Upload des Dokuments und Anzeige des Prüfergebnisses

RTR RUNDfunk & TELEKOM REGULIERUNGS-GmbH

Über uns | Kontakt | Presse | Kompetenzzentrum | English

RUNDfunk | TELEKOMMUNIKATION | ELEKTRONISCHE SIGNATUR | FÖRDERUNGEN | VERWERTUNGS GESELLSCHAFTEN | POST

Aufsicht >> > Elektronische Signatur > Verzeichnis > Signaturprüfung

Markt >> >>

Verzeichnis >>

> Sicherheits- und Zertifizierungskonzept

> Suche

> Signaturprüfung

Signaturrecht >>

Sicherheitsinformationen >>

Informationen für Anwender >>

Dokumente >>

Links >>

Signatur-Prüfung

Info * Feld muss ausgefüllt sein
! Hinweis auf Fehler

Information und Hilfe zum Ausfüllen
Zutreffendes ankreuzen oder

auswählen
Interaktive Ausfüllhilfe

Signatur-Prüfung v1.5.0

Dokument-Signatur prüfen

Prüfbericht

Nachfolgend finden Sie Informationen über das eingereichte Dokument.

Dokument	
Dateiname	sss.pdf
Hash-Wert	68f9b220274p8KCFMLETtCd0a1eF
Größe	147,26 kB
Typ	3Drafregistrierbescheinigung

Nachfolgend finden Sie einen Überblick über die geprüften Signaturen des eingereichten Dokuments. Details zu einer Signatur können durch Klick auf den Namen des Unterzeichners eingesehen werden.

Signaturen

Unterzeichner	Prüfung
Max Mustermann	OK OK OK

Eine Signatur ist dann als "gültig" zu betrachten wenn jede der Prüfungen Signaturwert (S), Zertifikat (Z) sowie Manifest (M) mit "OK" abgeschlossen wurde.

* Das Zertifikat erfüllt die technischen Voraussetzungen für eine Amtssignatur.

[Prüfbericht](#)

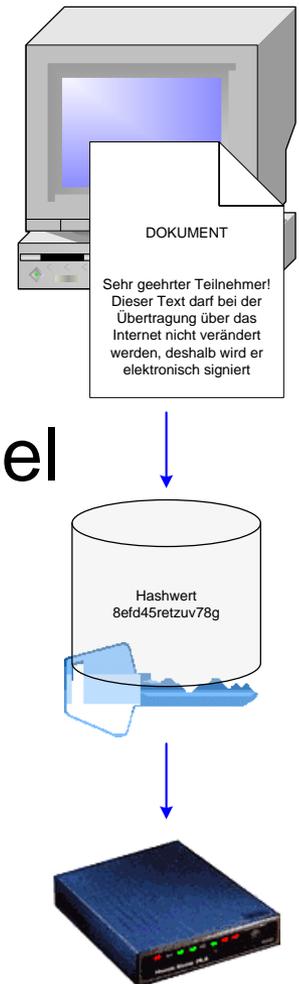
[Weitere Dokumente prüfen](#)

Signaturvorgang im Überblick (Sender)

- Erstellen eines Dokuments
- Hashwert („Fingerabdruck“ des Dok.) wird gebildet
- Hashwert wird mit dem privaten Schlüssel verschlüsselt

Signatur

- ✓ z.B.: Versand der signierten Nachricht mit dem eigenen öffentlichen Schlüssel



„Hash“

- Wird aus dem Gesamtext errechnet.
- Vergleichsbeispiel einer – primitiven - Hash-Funktion: Jeder Buchstabe wird durch seine Position im Alphabet ersetzt, am Schluss werden diese Zahlen zusammengezählt:

Buchstabe	S	C	H	M	E	T	T	E	R	L	I	N	G	Summe
Position im Alphabet	19	3	8	13	5	20	20	5	18	12	9	14	7	153

- Natürlich kommen wesentlich komplexere Verfahren zum Einsatz. ZB SHA-256, womit Hash-Werte mit einer Länge von 256 Bit erzeugt werden - üblicherweise als 64-stellige Hexadezimal-Zahl ausgedrückt werden. Der Hash-Wert für das Wort „Schmetterling“ zB lautet dann:
- d7e3dabc2c95c4c440ee57fb2883188e7f46a9cf51e94674f0e80f7d6db092c4

Anforderungen an die Hash-Funktion

- Kann auf eine Datei beliebiger Länge angewandt werden
- Erzeugt immer Ausgabe einer fixen Länge
- Für den Hashwert darf kein anderer Ausgangstext gefunden werden, als der ghashte.
- Es dürfen nicht mehrere verschiedene Ausgangstexte gefunden werden, die denselben Hashwert erzeugen.
- Auch geringe Änderungen im Ausgangstext müssen signifikante Änderungen im Hashwert erzeugen.
- Hashwert kann für beliebige Ausgangsdatei einfach und schnell errechnet werden

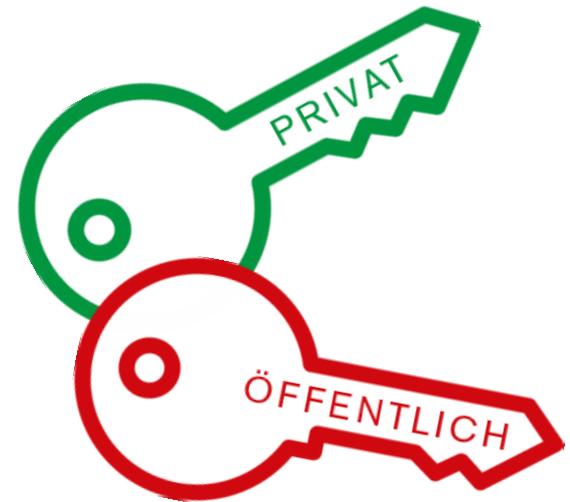
Verschlüsselung

- Symmetrische versus asymmetrische Verschlüsselung
- Schlüsselverwaltung und Schlüsselaustausch bei symmetrischer Verschlüsselung...
- Es geht bei der Signatur nicht um Verschlüsselung des Inhalts!
- Es wird der Inhalt im Klartext belassen
- Es wird lediglich der Hashwert verschlüsselt!

Asymmetrische Verschlüsselung – „PKI“

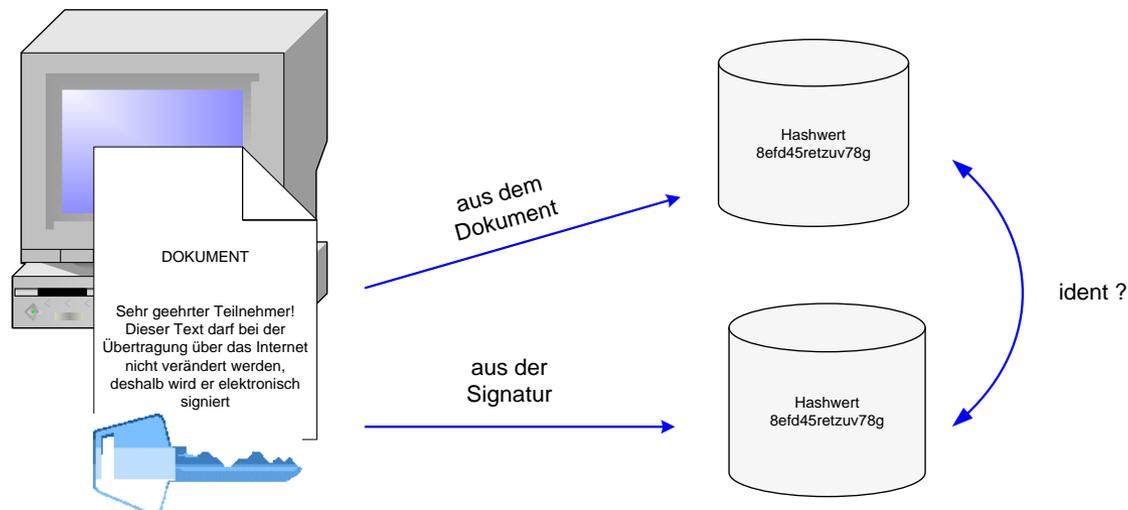
Zwei Schlüssel Prinzip

- Privater Schlüssel (Private Key)
 - Zugangsberechtigung (PIN)
 - nur dem Signator bekannt
 - „Signaturerstellungsdaten“
- Öffentlicher Schlüssel (Public Key)
 - Signaturprüfdaten
 - öffentlich zugänglich und abrufbar



Überprüfung der Signatur im Überblick (Empfänger)

- Aus dem empfangenen Dokument wird der Hashwert erneut gebildet
- Mit dem öffentlichen Schlüssel des Senders wird die Signatur entschlüsselt, der ursprüngliche Hashwert wird bekannt
- Vergleich beider Hashwerte
- ✓ Hashwerte ident \Rightarrow Nachricht vom Sender und unverfälscht



Worum geht es also?

- Es werden Daten (der Inhalt der signiert wird) so gesichert, dass eine nachträgliche Änderung sofort erkannt wird.

- „Integrität“

- Es werden Daten einer bestimmten Person zugeordnet (dem „Signator“, denn nur er hat den privaten Schlüssel)

- „Authentizität“

- Die Daten des Signators werden mit einem „Zertifikat“ dokumentiert, das von einer vertrauenswürdigen Stelle ausgestellt wird.

Rechtsquellen bis 30.6.2016

RL 1999/93/EG
„Signaturrichtlinie“

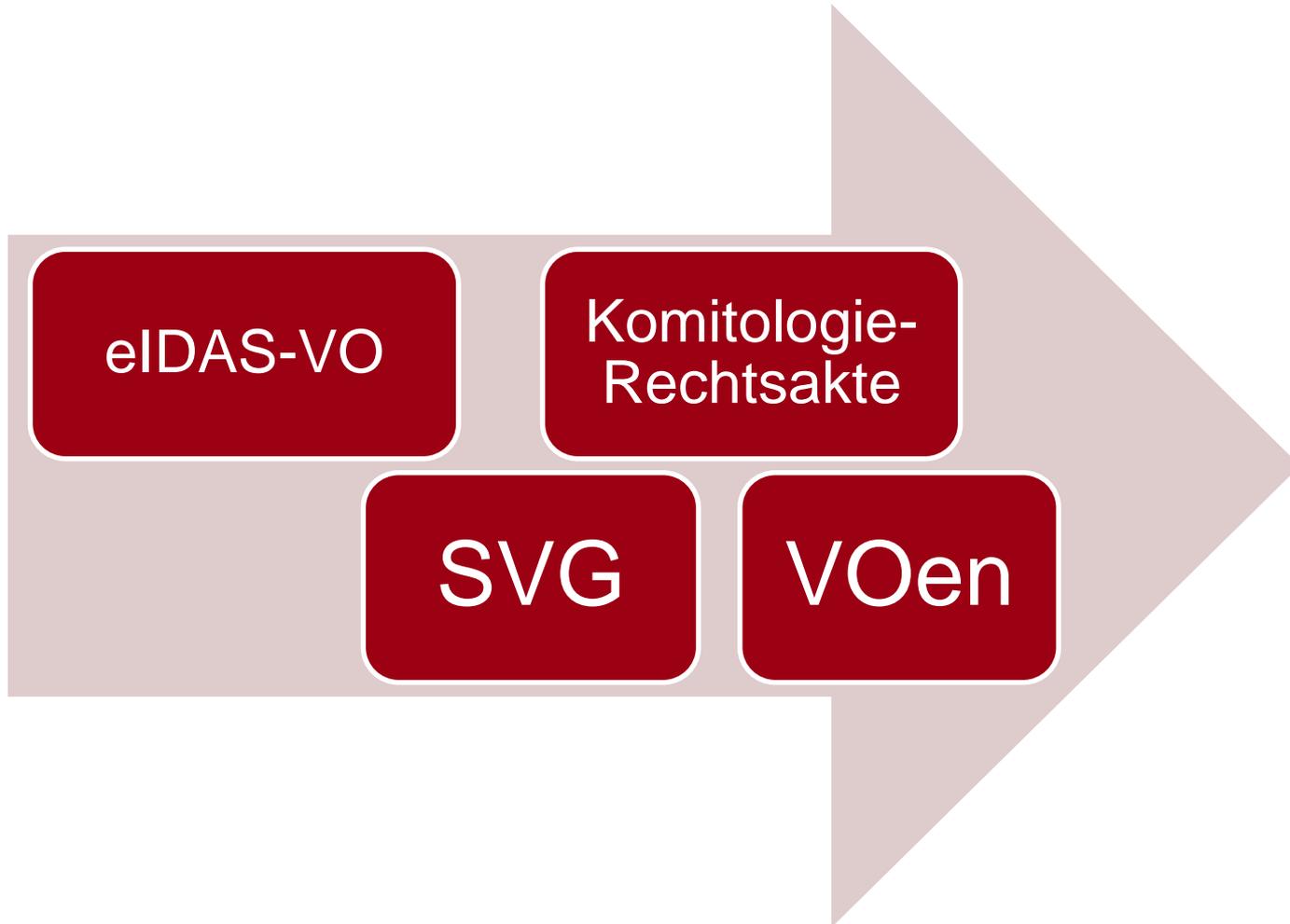
Signaturgesetz
BGBl Nr.
190/1999

Signaturverordnung 2008

VO über die Feststellung der
Eignung des Vereins
„Zentrum für sichere
Informationstechnologie -
Austria (A-SIT)“ als
Bestätigungsstelle (2000)

BestätigungsstellenVO
(2002)

Rechtsquellen ab 1.7.2016



eIDAS-VO - Hintergrund

- 13 Mio EU BürgerInnen arbeiten in einem anderen EU MS
- 21 Mio KMU – ein signifikanter Teil davon arbeitet international
- 150 Mio EU BürgerInnen shoppen Online; nur 20% davon kaufen aus einem anderen EU MGS

Ergo:

- Elektronischen Zugang erleichtern und Hürden bei der Nutzung der „eigenen“ Methoden beseitigen
- Grenzüberschreitende el. Nutzung ermöglichen
- Vertrauen und Sicherheit heben
- Elektronischen „Vertrauensdiensten“ den selben Wert verleihen wie in der „Papierwelt“

Der neue EU-Rechtsrahmen: die eIDAS-VO

28.8.2014

DE

Amtsblatt der Europäischen Union

L 257/73

VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 23. Juli 2014
über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im
Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

Eckpunkte eIDAS-VO

Ein Rechtsakt für die beiden Themen

- **elektronische Signatur** und weitere „Vertrauensdienste“ und
- **elektronische Identität** („eID“)

Die SigRL (im SigG innerstaatlich umgesetzt) wurde komplett ersetzt

- Typ des Rechtsakts: Verordnung
 - VO ist unmittelbar anzuwenden;
 - bestehende Umsetzungsvorschriften (SigG/ SigV etc.) waren zu bereinigen;
 - Umsetzungen und flankierende Regelungen waren aber notwendig - SVG

„eIDAS-VO“: Überblick

- Kapitel I: Allg. Bestimmungen
- Kapitel II: **Elektronische Identifizierung**
- Kapitel III: **Vertrauensdienste**
- Kapitel IV: Elektronische Dokumente

- Kapitel V: Befugnisübertragungen und Durchführungsbestimmungen
- Kapitel VI: Schlussbestimmungen

- 4 Anhänge (Anforderungen an qual. Zertifikate/ Signaturerstellungseinheiten/ el. Siegel/ Website-Authentifizierung)



Vertrauensdienste (1/2)

- Elektronische Signatur – nat. Person
- Elektronische Siegel – jur. Person (weiter Begriff)

Weitere Vertrauensdienste (2/2)

- Elektronische Bewahrungsdienste
- Elektronische Validierungsdienste
- Elektronische Zeitstempeldienste
- Elektronische Zustelldienste – „Dienste für die Zustellung elektronischer Einschreiben“
- Website Authentifizierung

Zu diesen fehlen derzeit noch weitgehend die relevanten internationalen Standards und damit die Durchführungsrechtsakte

Durchführungsrechtsakte - Vertrauensdienste

- EU-Vertrauenssiegel für qualifizierte Vertrauensdiensteanbieter:

- Durchführungsverordnung (EU) 2015/806, ABl. Nr. L 128 vom 23.5.2015



- Vertrauensliste

- Durchführungsbeschluss (EU) 2015/1505, ABl. Nr. L 235 vom 9.9.2015

- Signaturformate

- Durchführungsbeschluss (EU) 2015/1506, ABl. Nr. L 235 vom 9.9.2015

- Sicherheitsbewertung von QSCD

- Durchführungsbeschluss (EU) 2016/650, ABl. Nr. L 109 vom 26.4.2016

Legistische Umsetzung in Österreich 1

- nur jene Bereiche geregelt, in denen die unmittelbar anwendbare eIDAS-Verordnung den Mitgliedstaaten die Möglichkeit überlässt (oder die MS dazu verpflichtet – „hinkende VO“), nationale Vorschriften zu erlassen.
- Dies betrifft im Bereich der Vertrauensdiensteanbieter insbes.: Aufsicht, Formvorschriften, Haftung und Sanktionen bei Nichteinhaltung der Vorgaben der Verordnung.
- Kern: Elektronische Signaturen (auch Regelungen des aufgehobenen SigG sind enthalten)

Legistische Umsetzung 2 - Bundesgesetze

- Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (**Signatur- und Vertrauensdienstegesetz – SVG**)
- Aufhebung Signaturgesetz
- Novelle E-Government-Gesetz
- Legistische Anpassungen 22 weiterer Bundesgesetze

- Inkrafttreten: **1. Juli 2016**

Legistische Umsetzung 3 - Verordnung

- Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (**Signatur- und Vertrauensdiensteverordnung – SVV**)
- Aufhebung Signaturverordnung
- Verordnung über die Feststellung der Eignung des Vereins „Zentrum für sichere Informationstechnologie – Austria (A-SIT)
- Inkrafttreten: **02. August 2016**

Art. 25 eIDAS-VO - Rechtswirkung elektronischer Signaturen

- (1) Einer **elektronischen Signatur** darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt oder weil sie die Anforderungen an qualifizierte elektronische Signaturen nicht erfüllt.
- (2) Eine **qualifizierte elektronische Signatur** hat die **gleiche Rechtswirkung wie eine handschriftliche Unterschrift**.
- (3) Eine qualifizierte elektronische Signatur, die auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruht, wird **in allen anderen Mitgliedstaaten** als qualifizierte elektronische Signatur anerkannt.

§ 4 SVG – Rechtswirkungen (1/2)

(1) Eine qualifizierte elektronische Signatur erfüllt das **rechtliche Erfordernis der Schriftlichkeit im Sinne des § 886 ABGB.**

Andere **gesetzliche Formerfordernisse**, insbesondere solche, die die Beiziehung eines Notars oder eines Rechtsanwalts vorsehen, sowie vertragliche Vereinbarungen über die Form **bleiben unberührt.**

Hintergrund: Rechtsvorschriften verlangen häufig Schriftform, zB Abschluss eines befristeten Mietvertrags gem. §29 Abs. 1 Z 3 MRG; Schenkung ohne wirkliche Übergabe gem. 943 ABGB...!

§ 4 SVG – Rechtswirkungen (2/2)

(2) Letztwillige Verfügungen können in elektronischer Form **nicht** wirksam errichtet werden. **Folgende** Willenserklärungen können nur **dann** in elektronischer Form wirksam abgefasst werden, **wenn** das Dokument über die Erklärung die Bestätigung eines **Notars** oder eines **Rechtsanwalts** enthält, dass er den **Signator über die Rechtsfolgen seiner Signatur aufgeklärt** hat:

1. Willenserklärungen des Familien- und Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind;
2. eine Bürgschaftserklärung (§ 1346 Abs. 2 ABGB), die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit abgegeben wird.

§1a Notariatsordnung

Sämtliche bei den Amtsgeschäften nach § 1 entsprechend den Bestimmungen dieses Bundesgesetzes **von dem Notar oder vor dem Notar gesetzten oder bekräftigten elektronischen Signaturen** entfalten auch die Rechtswirkungen der Schriftlichkeit im Sinne des § 886 ABGB; § 4 Abs. 2 SVG ist insoweit nicht anzuwenden.

Qualifizierte Signatur - Konsumentenschutz

Stärkung des Vertrauens in die Akzeptanz qualifiziert signierter Dokumente – Beseitigung der „versteckten“ Klauseln in AGBs (vgl. die Beschwerdefälle von Konsumenten bei Vertragskündigungen)

§ 4 Abs. 3 SVG: Bei Rechtsgeschäften zwischen Unternehmern und Verbrauchern sind Vertragsbestimmungen, nach denen eine qualifizierte elektronische Signatur nicht das rechtliche Erfordernis der Schriftlichkeit erfüllt, für Anzeigen oder Erklärungen, die vom Verbraucher dem Unternehmer oder einem Dritten abgegeben werden, nicht verbindlich, es sei denn, der Unternehmer beweist, dass die Vertragsbestimmungen **im Einzelnen ausgehandelt** worden sind oder mit dem Verbraucher eine andere vergleichbar einfach verwendbare Art der elektronischen Authentifizierung vereinbart wurde .

Art. 1 eIDAS-VO - Gegenstand

Um das **ordnungsgemäße Funktionieren des Binnenmarkts** und gleichzeitig ein **angemessenes Sicherheitsniveau** bei elektronischen Identifizierungsmitteln und Vertrauensdiensten sicherzustellen, ist in dieser Verordnung Folgendes geregelt:

- a) Sie legt die Bedingungen fest, unter denen die Mitgliedstaaten **elektronische Identifizierungsmittel** für natürliche und juristische Personen, die einem notifizierten elektronischen Identifizierungssystem eines anderen Mitgliedstaats unterliegen, anerkennen.
- b) Sie **legt Vorschriften für Vertrauensdienste** — insbesondere für elektronische Transaktionen — **fest**.
- c) Sie **legt einen Rechtsrahmen für elektronische Signaturen**, elektronische Siegel, elektronische Zeitstempel, elektronische Dokumente, Dienste für die Zustellung elektronischer Einschreiben und Zertifizierungsdienste für die Website-Authentifizierung **fest**.

Art. 2 eIDAS-VO - Anwendungsbereich

(1) Diese Verordnung gilt für von einem Mitgliedstaat notifizierte elektronische Identifizierungssysteme und für in der Union niedergelassene Vertrauensdiensteanbieter.

(2) Diese Verordnung findet **keine Anwendung** auf die Erbringung von Vertrauensdiensten, die **ausschließlich innerhalb geschlossener Systeme** aufgrund von nationalem Recht oder von Vereinbarungen **zwischen einem bestimmten Kreis von Beteiligten** verwendet werden.

(3) Diese Verordnung **berührt nicht** das nationale Recht oder das Unionsrecht in Bezug auf den **Abschluss und die Gültigkeit von Verträgen oder andere rechtliche oder verfahrensmäßige Formvorschriften**.

Art. 4 eIDAS-VO - Binnenmarktgrundsatz

- (1) Die Erbringung von Vertrauensdiensten im Gebiet eines Mitgliedstaats durch einen in einem anderen Mitgliedstaat niedergelassenen Vertrauensdiensteanbieter unterliegt keinen Beschränkungen aus Gründen, die in den Anwendungsbereich dieser Verordnung fallen.
- (2) Produkte und Vertrauensdienste, die dieser Verordnung entsprechen, dürfen im Binnenmarkt frei verkehren.

Art. 5 eIDAS-VO - Datenverarbeitung und Datenschutz

- (1)** Personenbezogene Daten werden nach Maßgabe der Richtlinie 95/46/EG verarbeitet.

- (2)** Unbeschadet der Rechtswirkungen, die Pseudonyme nach nationalem Recht haben, darf die Benutzung von Pseudonymen bei elektronischen Transaktionen nicht untersagt werden.

Art. 15 eIDAS-VO - Zugänglichkeit

Soweit möglich werden Vertrauensdienste und zur Erbringung solcher Dienste verwendete Endnutzerprodukte Personen mit Behinderungen zugänglich und nutzbar gemacht.

Art. 16 eIDAS-VO - Sanktionen

Die Mitgliedstaaten legen Regeln für Sanktionen bei Verstößen gegen diese Verordnung fest. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

Siehe:

§ 16 SVG - Verwaltungsstrafbestimmungen

Art. 3 eIDAS-VO - Begriffsbestimmungen

9. „**Unterzeichner**“ ist eine **natürliche** Person, die eine elektronische Signatur erstellt.

10. „**Elektronische Signatur**“ sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet.

11. „**Fortgeschrittene elektronische Signatur**“ ist eine elektronische Signatur, die die Anforderungen des Artikels 26 erfüllt.

Art. 26 eIDAS-VO - Anforderungen an fortgeschrittene elektronische Signaturen

Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

- a) Sie ist **eindeutig** dem Unterzeichner zugeordnet.
- b) Sie **ermöglicht die Identifizierung** des Unterzeichners.
- c) Sie wird unter Verwendung elektronischer **Signaturerstellungsdaten** erstellt, die der Unterzeichner mit einem **hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann**.
- d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine **nachträgliche Veränderung der Daten erkannt werden kann**.

Art. 26 eIDAS-VO - Anforderungen an fortgeschrittene elektronische Signaturen

Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

a) Sie ist **eindeutig** dem Unterzeichner zugeordnet.

- Das Schlüsselpaar darf bei dem Aussteller nur ein einziges Mal existieren und ist der einen Person zugeordnet...

Art. 26 eIDAS-VO - Anforderungen an fortgeschrittene elektronische Signaturen

Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

- b) Sie ermöglicht die Identifizierung des Unterzeichners.**
- Die Signatur, die mit einem bestimmten öff. Schlüssel geprüft wird, kann nur mit dem korrespondierenden privaten Schlüssel erstellt worden sein.
- Es muss praktisch ausgeschlossen sein, dass der private Schlüssel aus dem öffentlichen Schlüssel errechnet werden kann.

Art. 26 eIDAS-VO - Anforderungen an fortgeschrittene elektronische Signaturen

Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

- c) Sie wird unter Verwendung elektronischer **Signaturerstellungsdaten** erstellt, die der Unterzeichner mit einem **hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann**.
- Signaturerstellung nur durch eine bestimmte dazu berechnigte Person
- Berechnigung durch PIN/ Passwort etc. bzw. zwei-Faktoren-System zur Sicherstellung (Wissen+Besitz)

Art. 26 eIDAS-VO - Anforderungen an fortgeschrittene elektronische Signaturen

Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

- d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine **nachträgliche Veränderung der Daten erkannt werden kann.**

- „Integrität“
- Unterschiedliche Daten müssen zu unterschiedlichen Hashwerten führen

Art. 26 eIDAS-VO - Anforderungen an fortgeschrittene elektronische Signaturen

Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

- a) Sie ist **eindeutig** dem Unterzeichner zugeordnet.
- b) Sie **ermöglicht die Identifizierung** des Unterzeichners.
- c) Sie wird unter Verwendung elektronischer **Signaturerstellungsdaten** erstellt, die der Unterzeichner mit einem **hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann**.
- d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine **nachträgliche Veränderung der Daten erkannt werden kann**.

Art. 3 eIDAS-VO – Begriffsbestimmungen...

12. „**Qualifizierte elektronische Signatur**“ ist eine fortgeschrittene elektronische Signatur, die von einer **qualifizierten elektronischen Signaturerstellungseinheit** erstellt wurde **und** auf einem **qualifizierten Zertifikat** für elektronische Signaturen beruht.

13. „**Elektronische Signaturstellungsdaten**“ sind eindeutige Daten, die vom Unterzeichner zum Erstellen einer elektronischen Signatur verwendet werden.

Art. 3 eIDAS-VO – Begriffsbestimmungen...

14. **„Zertifikat für elektronische Signaturen“** ist eine elektronische Bescheinigung, die elektronische Signaturvalidierungsdaten mit einer natürlichen Person verknüpft und die mindestens den Namen oder das Pseudonym dieser Person bestätigt.

15. **„Qualifiziertes Zertifikat für elektronische Signaturen“** ist ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat für elektronische Signaturen, das die Anforderungen des Anhangs I erfüllt.

Anhang I – Anforderungen an qualifizierte Zertifikate für elektronische Signaturen (1/3)

Qualifizierte Zertifikate für elektronische Signaturen enthalten Folgendes:

- a) eine Angabe, dass das Zertifikat als qualifiziertes Zertifikat für elektronische Signaturen ausgestellt wurde, zumindest in einer zur automatischen Verarbeitung geeigneten Form;
- b) einen Datensatz, der den **qualifizierten Vertrauensdiensteanbieter**, der die qualifizierten Zertifikate ausstellt, eindeutig repräsentiert und zumindest die Angabe des **Mitgliedstaats** enthält, in dem der Anbieter niedergelassen ist, sowie
 - bei einer juristischen Person: den Namen und gegebenenfalls die Registriernummer gemäß der amtlichen Eintragung;
 - bei einer natürlichen Person: den Namen der Person;
- c) mindestens den **Namen des Unterzeichners** oder ein **Pseudonym**; wird ein Pseudonym verwendet, ist dies eindeutig anzugeben;

Anhang I – Anforderungen an qualifizierte Zertifikate für elektronische Signaturen (2/3)

- d) elektronische **Signaturvalidierungsdaten**, die den elektronischen Signaturerstellungsdaten entsprechen;
- e) Angaben zu **Beginn und Ende der Gültigkeitsdauer** des Zertifikats;
- f) den **Identitätscode** des Zertifikats, der für den qualifizierten Vertrauensdiensteanbieter eindeutig sein muss;
- g) die fortgeschrittene elektronische Signatur oder das fortgeschrittene elektronische Siegel des ausstellenden qualifizierten Vertrauensdiensteanbieters;

Anhang I – Anforderungen an qualifizierte Zertifikate für elektronische Signaturen (2/2)

- h) den Ort, an dem das Zertifikat, das der fortgeschrittenen elektronischen Signatur oder dem fortgeschrittenen elektronischen Siegel gemäß Buchstabe g zugrunde liegt, kostenlos zur Verfügung steht;
- i) den **Ort** der Dienste, die genutzt werden können, um den **Gültigkeitsstatus** des qualifizierten Zertifikats zu **überprüfen**;
- j) falls sich die elektronischen Signaturerstellungsdaten, die den elektronischen Signaturvalidierungsdaten entsprechen, in einer **qualifizierten elektronischen Signaturerstellungseinheit** befinden — eine geeignete Angabe dieses Umstands, zumindest in einer zur automatischen Verarbeitung geeigneten Form.

Art. 28 eIDAS-VO – Qualifizierte Zertifikate für elektronische Signaturen

- (2) Für qualifizierte Zertifikate für elektronische Signaturen dürfen keine obligatorischen Anforderungen gelten, die über die in Anhang I festgelegten hinausgehen.
- (3) Qualifizierte Zertifikate für elektronische Signaturen können zusätzliche **fakultative spezifische Attribute** enthalten. Diese Attribute dürfen die Interoperabilität und Anerkennung qualifizierter elektronischer Signaturen nicht berühren.

Attribute in Ö. zB für Anwälte, Notare, Ziviltechniker!

Berufsspezifische Ausprägungen der elektr. Signaturen („Attribute“ im Zert.)

- Für Berufsgruppen
 - Elektronische Beurkundungssignatur der Notare
 - El. Notarsignatur
 - El. Anwaltssignatur
 - El. Beurkundungssignatur der Ziviltechniker
 - El. Ziviltechnikersignatur
- Für Behörden
 - Elektronische Signatur der Justiz
 - Amtssignatur

**Seit 1.7.2016:
„Siegel“!**

§ 13 Abs. 1 Notariatsordnung (1/2)

Zum Zweck der elektronischen Unterfertigung bei den Amtsgeschäften nach § 1 ist der Notar verpflichtet, sich einer qualifizierten elektronischen Signatur zu bedienen, die der Errichtung öffentlicher Urkunden vorbehalten ist (**elektronische Beurkundungssignatur**). Der Notar ist berechtigt, sich bei der Besorgung der Amtsgeschäfte nach § 5 einer qualifizierten elektronischen Signatur als Notar zu bedienen (**elektronische Notarsignatur**). Das Verlangen auf Ausstellung der qualifizierten Zertifikate und der Ausweiskarten für die elektronische Beurkundungssignatur und die elektronische Notarsignatur ist gemäß § 8 Abs. 1 SVG bei der zuständigen Notariatskammer einzubringen.

§ 13 Abs. 1 Notariatsordnung (2/2)

Die Eigenschaft als Notar ist in das qualifizierte Zertifikat aufzunehmen (Art. 28 Abs. 3 eIDAS-VO), wenn diese zuverlässig nachgewiesen ist. Der Inhalt der qualifizierten Zertifikate des Notars ist vom VDA im Internet gesichert abfragbar zu machen. Mit dem Erlöschen des Amtes (§ 19 Abs. 1) oder der Suspension (§§ 32 Abs. 2 lit. c, 158, 180) erlischt auch die Befugnis zur Verwendung der elektronischen Beurkundungssignatur und der elektronischen Notarsignatur. Der Notar hat die Ausweiskarten umgehend der Notariatskammer zurückzustellen und beim Vertrauensdiensteanbieter um den Widerruf der Zertifikate zu ersuchen (Art. 24 Abs. 3 eIDAS-VO).

Art. 3 eIDAS-VO – Begriffsbestimmungen...

22. „**Elektronische Signaturerstellungseinheit**“ ist eine konfigurierte Software oder Hardware, die zum Erstellen einer elektronischen Signatur verwendet wird.

23. „**Qualifizierte elektronische Signaturerstellungseinheit**“ ist eine elektronische Signaturerstellungseinheit, die die Anforderungen des **Anhangs II** erfüllt.

Anhang II – Anforderungen an qualifizierte Signaturerstellungseinheiten (1/2)

(1) Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass

- a) die **Vertraulichkeit** der zum Erstellen der elektronischen Signatur verwendeten elektronischen **Signaturstellungsdaten** angemessen sichergestellt ist, (=kein „Auslesen“)
- b) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturstellungsdaten **praktisch nur einmal vorkommen** können,
- c) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturstellungsdaten mit hinreichender Sicherheit **nicht abgeleitet** werden können und die elektronische Signatur bei Verwendung der jeweils verfügbaren Technik **verlässlich gegen Fälschung geschützt** ist, (=nicht „kompromittiert“)
- d) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturstellungsdaten vom rechtmäßigen Unterzeichner **gegen eine Verwendung durch andere verlässlich geschützt** werden können. (=PIN/ Passwort neben dem Besitz bzw. der „Kontrolle“)

Anhang II – Anforderungen an qualifizierte Signaturerstellungseinheiten (2/2)

(2) Qualifizierte elektronische Signaturerstellungseinheiten dürfen die zu unterzeichnenden Daten nicht verändern und nicht verhindern, dass dem Unterzeichner diese **Daten vor dem Unterzeichnen angezeigt** werden.
(= „Viewer“)

(3) Das Erzeugen **oder Verwalten** von elektronischen Signaturerstellungsdaten **im Namen eines Unterzeichners** darf nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt werden.

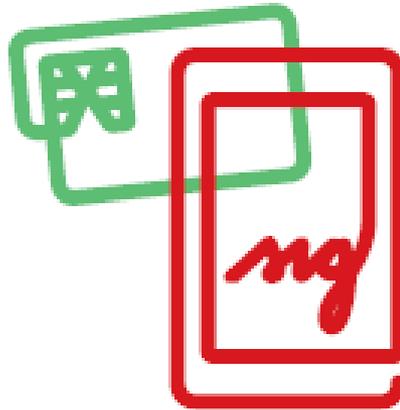
(4) Unbeschadet des Absatzes 1 Buchstabe d dürfen qualifizierte Vertrauensdiensteanbieter, die elektronische Signaturerstellungsdaten im Namen des Unterzeichners verwalten, die elektronischen Signaturerstellungsdaten ausschließlich zu Sicherungszwecken kopieren, sofern folgende Anforderungen erfüllt 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.

„Verwalten im Namen...“ (1/2)

(Erwägungsgrund 52)

Die Erstellung elektronischer **Fernsignaturen** in einer von einem Vertrauensdiensteanbieter im Namen des Unterzeichners geführten Umgebung soll aufgrund der vielfältigen damit verbundenen wirtschaftlichen Vorteile ausgebaut werden.



„Verwalten im Namen...“ (2/2)

...Damit **elektronische Fernsignaturen** tatsächlich rechtlich in gleicher Weise anerkannt werden können wie elektronische Signaturen, die vollständig in der Umgebung des Nutzers erstellt werden, sollten die Anbieter von elektronischen Fernsignaturdiensten jedoch spezielle Verfahren für die Handhabung und Sicherheitsverwaltung mit vertrauenswürdigen Systemen und Produkten anwenden, u. a. durch abgesicherte elektronische Kommunikationskanäle, um für eine vertrauenswürdige Umgebung zur Erstellung elektronischer Signaturen zu sorgen und zu gewährleisten, dass diese Umgebung unter alleiniger Kontrolle des Unterzeichners genutzt worden ist.

Art. 29 eIDAS-VO – Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten

(2) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für Normen für qualifizierte elektronische Signaturerstellungseinheiten festlegen. Bei qualifizierten elektronischen Signaturerstellungseinheiten, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs II erfüllen.

Art. 30 eIDAS-VO – Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten

- (1) Die **Konformität** qualifizierter elektronischer Signaturerstellungseinheiten mit den Anforderungen des Anhangs II wird von geeigneten, von den Mitgliedstaaten benannten öffentlichen oder privaten Stellen **zertifiziert**.

§ 7 SVG - Bestätigungsstelle

(1) Die Konformität qualifizierter elektronischer Signatur- und Siegelerstellungseinheiten mit den Anforderungen des Anhangs II der eIDAS-VO wird durch eine Bestätigungsstelle oder eine in einem anderen Mitgliedstaat der Europäischen Union gemäß Art. 30 Abs. 1 eIDAS-VO benannte Stelle zertifiziert.

.... Anforderungen an die Bestätigungsstelle

(3) Der Bundesminister für Digitalisierung und Wirtschaftsstandort hat mit Verordnung festzustellen, dass eine Einrichtung als Bestätigungsstelle geeignet ist.

Verordnung BGBl. II Nr. 208/2016

„Die Eignung des Vereins **„Zentrum für sichere Informationstechnologie – Austria (A-SIT)“**, die Aufgaben einer Bestätigungsstelle nach dem Signatur- und Vertrauensdienstegesetz (SVG) und den auf seiner Grundlage ergangenen Verordnungen wahrzunehmen, wird festgestellt.“

Erwägungsgrund 56 QSCD-Zertifizierung

... Diese Verordnung sollte **nicht die gesamte Systemumgebung** abdecken, in der die Einheit betrieben wird. Daher sollte sich der Anwendungsbereich der Zertifizierung qualifizierter Signaturerstellungseinheiten nur auf die Hardware und die Systemsoftware erstrecken, die verwendet werden, um die in der Signaturerstellungseinheit erstellten, gespeicherten oder verarbeiteten Signaturerstellungsdaten zu verwalten und zu schützen. Wie in den einschlägigen Normen angegeben, sollte der Anwendungsbereich der Zertifizierungspflicht **Signaturerstellungsanwendungen ausschließen.**

Art. 31 eIDAS-VO – Liste der QSCDs

- (1) Die MS **notifizieren** der EK Informationen über qualifizierte elektronische Signaturerstellungseinheiten, die von den in Artikel 30 Absatz 1 genannten Stellen zertifiziert worden sind.
- (2) Auf der Grundlage der erhaltenen Informationen sorgt die Kommission für die Aufstellung, Veröffentlichung und Führung einer Liste zertifizierter qualifizierter elektronischer Signaturerstellungseinheiten.

Art. 3 eIDAS-VO – Begriffsbestimmungen...

16. „**Vertrauensdienst**“ ist ein elektronischer Dienst, der **in der Regel gegen Entgelt** erbracht wird und aus Folgendem besteht:

- a) Erstellung, Überprüfung und Validierung von elektronischen **Signaturen**, elektronischen **Siegeln** oder elektronischen **Zeitstempeln**, und Diensten für die **Zustellung** elektronischer Einschreiben sowie von diese Dienste betreffenden Zertifikaten oder
- b) Erstellung, Überprüfung und Validierung von Zertifikaten für die **Website-Authentifizierung** oder
- c) **Bewahrung** von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten.

„in der Regel gegen Entgelt“

Art. 57 AEUV: Dienstleistungen im Sinne der Verträge sind Leistungen, die **in der Regel gegen Entgelt** erbracht werden, soweit sie nicht den Vorschriften über den freien Waren- und Kapitalverkehr und über die Freizügigkeit der Personen unterliegen.

Als Dienstleistungen gelten insbesondere:

- a) gewerbliche Tätigkeiten,
 - b) kaufmännische Tätigkeiten,
 - c) handwerkliche Tätigkeiten,
 - d) freiberufliche Tätigkeiten.
- „**in der Regel gegen Entgelt**“: wirtschaftlicher Charakter, Erwerbszweck

Art. 3 eIDAS-VO – Begriffsbestimmungen...

17. „**Qualifizierter Vertrauensdienst**“ ist ein Vertrauensdienst, der die einschlägigen Anforderungen dieser Verordnung erfüllt.

19. „**Vertrauensdiensteanbieter**“ ist eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt.

20. „**Qualifizierter Vertrauensdiensteanbieter**“ ist ein Vertrauensdiensteanbieter, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und dem von der Aufsichtsstelle der **Status** eines qualifizierten Anbieters **verliehen** wurde.

Art. 19 eIDAS-VO – Sicherheitsanforderungen an Vertrauensdiensteanbieter (1/2)

Qualifizierte und nichtqualifizierte VDA ergreifen geeignete technische und organisatorische **Maßnahmen zur Beherrschung der Sicherheitsrisiken** im Zusammenhang mit den von ihnen erbrachten Vertrauensdiensten. Diese Maßnahmen müssen unter Berücksichtigung des jeweils **neuesten Standes der Technik** gewährleisten, dass das Sicherheitsniveau der Höhe des Risikos angemessen ist. Insbesondere sind Maßnahmen zu ergreifen, um Auswirkungen von Sicherheitsverletzungen zu vermeiden bzw. so gering wie möglich zu halten und die Beteiligten über die nachteiligen Folgen solcher Vorfälle zu informieren.

Art. 19 eIDAS-VO – Sicherheitsanforderungen an Vertrauensdiensteanbieter (2/2)

(2) Meldung von Vorfällen an Aufsichtsstelle innerhalb von 24 Stunden; Information auch an andere Stellen und die Betroffenen/ Öffentlichkeit...

Art. 24 eIDAS-VO – Sicherheitsanforderungen an Vertrauensdiensteanbieter

... beschäftigen Personal das über das erforderliche **Fachwissen**, die erforderliche **Zuverlässigkeit**, die erforderliche Erfahrung und die erforderlichen **Qualifikationen** verfügt, in Bezug auf die Vorschriften für die **Sicherheit** und den **Schutz personenbezogener Daten** angemessen geschult worden ist und Verwaltungs- und Managementverfahren anwendet, die den anerkannten europäischen oder internationalen Normen entsprechen.

Art. 24 eIDAS-VO – weitere Anforderungen

- Ausreichende Finanzmittel, Haftpflichtversicherung
- Sie **unterrichten Personen**, die einen qualifizierten Vertrauensdienst nutzen wollen, klar und umfassend über die genauen Bedingungen für die Nutzung des Dienstes, einschließlich Nutzungsbeschränkungen, bevor sie vertragliche Beziehungen zu dieser Person eingehen.
- Vertrauenswürdige Systeme, Sicherheit, Aufzeichnungspflichten...
- **Zertifikatsdatenbank...**

§ 2 SVV – Konkretisierungen zu qual. VDA-Zuverlässigkeit

- Zutrittssicherung
- Zuverlässiges Personal
- Ausbildung und Fachwissen
- ...

Art. 21 eIDAS-VO – Beginn der Erbringung qualifizierter Vertrauensdienste (1/2)

- (1) Zulassungsverfahren** durch Aufsichtsstelle.
Vorlage eines
Konformitätsbewertungsberichts einer
Konformitätsbewertungsstelle.
- (2) Verleihung des Qualifikationsstatus** und
Veröffentlichung auf der Vertrauensliste.
- (3)** Qualif. VDA können mit der Erbringung des
qualif. Vertrauensdienstes beginnen,
nachdem der qualifizierte Status in den
Vertrauenslisten ausgewiesen wurde.

Art. 22 eIDAS-VO – Vertrauenslisten

- (1) Jeder MS sorgt für die Aufstellung, Führung und Veröffentlichung von Vertrauenslisten, die Angaben zu den qualifizierten VDA, für die er verantwortlich ist, und den von ihnen erbrachten qualifizierten Vertrauensdiensten, umfassen.
- (2) Die MS erstellen, führen und veröffentlichen auf **gesicherte Weise** el. unterzeichnete oder besiegelte Vertrauenslisten in einer für eine **automatisierte Verarbeitung geeigneten Form**.

§14 SVG – Vertrauenslisten

- (1) Die RTR-GmbH erstellt, führt und veröffentlicht für die Aufsichtsstelle auf gesicherte Weise eine von der RTR-GmbH elektronisch unterzeichnete oder besiegelte Vertrauensliste gemäß Art. 22 eIDAS-VO. Nichtqualifizierte VDA und die von ihnen erbrachten Vertrauensdienste sind auf Antrag in die Vertrauensliste aufzunehmen

„EU-Vertrauensliste“

AAA.sec.com
EU Trust Service status List (TSL) Analysis Tool

TSL Browser TSP Records Check TSL Logs

Inspect XML Data

TSL OVERVIEW		EU Trust Service List Information											
Country	Trust Service	Territory	CountryName	SigStatus	IssueDate	ExpiryDate	Seq#	QcTspCount	ServiceCount	QcCACount	TslSigCertExp	TslVer	Alerts
EU	European Commission												
AT	Rundfunk und Telekom Regulierungs-GmbH	AT	Austria	verified	2015-07-01	2015-12-31	23	3	23	3	2017-01-28	4	-
BE	FPS Economy, SMEs, Self-employed and Energy - Quality and Safety	BE	Belgium	verified	2015-06-25	2015-11-08	21	3	8	0	2024-10-14	4	-
BG	Communications Regulation Commission	BG	Bulgaria	verified	2015-07-15	2016-01-14	8	6	25	0	2017-11-15	4	-
CY	Department of Electronic Communications	CY	Cyprus	verified	2015-09-06	2016-03-03	19	0	0	0	2018-07-01	4	-
CZ	Ministry of the Interior of the Czech Republic	CZ	Czech Republic	verified	2015-07-13	2015-12-13	35	3	59	4	2016-06-02	4	-
DE	Bundesnetzagentur	DE	Germany	verified	2015-08-12	2016-02-11	22	12	412	276	2019-04-11	4	-
DK	Danish Agency for Digitalisation // CVR:34051178	DK	Denmark	verified	2015-08-24	2016-02-23	10	0	1	0	2017-08-27	4	-
EE	Estonian Technical Surveillance Authority	EE	Estonia	verified	2015-05-11	2015-11-07	25	1	29	0	2020-11-05	4	-
EL	EETT	EL	Greece	verified	2015-06-11	2015-12-10	16	5	12	0	2016-01-10	4	-
ES	MINISTRY OF INDUSTRY ENERGY AND TOURISM	ES	Spain	verified	2015-09-09	2016-03-07	32	24	79	0	2019-03-11	4	-
FI	FICORA	FI	Finland	verified	2015-03-24	2015-09-23	17	1	5	0	2017-01-29	4	tslExpiry
FR	General Secretariat for the Modernisation of Public Action	FR	France	verified	2015-06-30	2015-12-29	17	12	114	0	2017-03-26	4	-
HR	Ministry of economy	HR	Croatia	verified	2015-06-18	2015-12-17	6	1	5	0	2015-12-20	4	-
HU	National Media and Infocommunications Authority, Hungary	HU	Hungary	verified	2015-08-07	2015-10-06	26	5	158	0	2015-10-07	4	tslCertExpiry
IE	Department of Communications Energy and Natural Resources	IE	Ireland	verified	2015-07-16	2016-01-15	5	1	1	0	2017-06-18	4	-
IS	The Consumer Agency	IS	Iceland	verified	2015-02-02	2015-07-30	3	1	2	0	2016-08-20	4	tslExpiry(expired)
IT	Agencia per l'Italia Digitale	IT	Italy	verified	2015-08-31	2015-10-07	66	37	155	0	2020-05-17	4	-
LI	Office for Communications	LI	Liechtenstein	verified	2015-04-07	2015-10-06	13	2	4	1	2017-02-10	4	tslExpiry
IS	The Consumer Agency	LT	Lithuania	verified	2015-07-22	2016-01-21	27	3	35	4	2017-01-01	4	-
IT	Agencia per l'Italia Digitale	LU	Luxembourg	verified	2015-08-12	2016-02-11	24	2	7	0	2017-02-19	4	-
LI	Office for Communications	LV	Latvia	verified	2015-07-29	2016-01-28	10	1	15	8	2018-08-25	4	-
LT	Communications Regulatory Authority of the Republic of Lithuania	MT	Malta	verified	2015-06-02	2015-12-01	13	0	0	0	2018-05-19	4	-
LU	ILNAS	NL	Netherlands	verified	2015-05-21	2015-11-21	21	9	34	1	2020-03-25	4	-
LV	Data State Inspectorate	NO	Norway	verified	2015-05-29	2015-11-29	22	13	13	0	2018-01-13	4	-
MT	Malta Communications Authority	PL	Poland	verified	2015-09-04	2015-12-04	57	8	24	0	2016-01-23	4	-
NL	Authority for Consumers & Markets	PT	Portugal	verified	2015-03-26	2015-09-25	20	7	14	0	2016-08-21	4	tslExpiry
NO	NASJONAL KOMMUNIKASJONSMYNDIGHET	RO	Romania	verified	2015-04-22	2015-10-22	9	5	37	0	2015-08-21	4	tslCertExpiry(expired)
PL	National Bank of Poland	SE	Sweden	verified	2015-06-23	2015-12-18	12	1	2	0	2017-02-03	4	-
PT	National Security Cabinet of Portugal	SI	Slovenia	verified	2015-05-08	2015-10-09	15	5	19	0	2016-12-08	4	-
RO	MINISTRY FOR INFORMATION SOCIETY	SK	Slovakia	verified	2015-03-24	2015-09-24	19	5	33	0	2016-09-06	4	tslExpiry
SE	Swedish Post and Telecom Agency (PTS)	UK	United Kingdom	verified	2015-08-06	2015-12-16	7	0	0	0	2017-02-20	4	-
SI	Republic of Slovenia, Ministry of Education, Science and Sport												
SK	NATIONAL SECURITY AUTHORITY												
UK	(Scheme Limited												

Terminology
 Territory Two letter ISO 3166 country code
 SigStatus Status of the TSL signature ("verified" = Signature is verified, "unverifiable" = The TSL is signed but the signature certificate is not published on the EU TSL, "absent" = The TSL is not signed, "syntax" = The signature validation process could not parse this signature, "invalid" = The signature certificate is invalid or the signature does not match the TSL content)

Dzt.: rund 210 Vertrauensdiensteanbieter aus 31 nationalen Listen

– Tool: <http://tlbrowser.tsl.website/tools/>

„EU-Vertrauensliste“ – Trust list browser

CEF Digital
Connecting Europe

Trusted List Browser

Tool to browse the national Trusted Lists and the European List of Trusted Lists (LOTL).

European Commission > CEF Digital > eSignature > Trusted List Browser

Search a trust service by

- Type of service**
Search by type of trust service (e.g. time-stamping, certificate for e-signature) and country
- Name of trust service**
Search based on the name of a trust service
- Signed file**
Find the trust service that issued the signing certificate(s) contained in a file

Austria Issue date 2019-01-23	Belgium Issue date 2019-02-01	Bulgaria Issue date 2019-02-05
Croatia Issue date 2019-02-08	Cyprus Issue date 2019-02-08	Czech Republic Issue date 2019-01-24
Denmark Issue date 2019-02-06	Estonia Issue date 2018-11-09	Finland Issue date 2019-02-19
France Issue date 2019-02-27	Germany Issue date 2019-02-26	Greece Issue date 2019-02-11
Hungary Issue date 2019-01-25	Iceland Issue date 2019-01-21	Ireland Issue date 2019-01-25
Italy Issue date 2019-02-26	Latvia Issue date 2018-12-06	Liechtenstein Issue date 2019-02-13

- URL: <https://webgate.ec.europa.eu/tl-browser/#/>

Art. 23 eIDAS-VO – EU-Vertrauenssiegel für qualifizierte Vertrauensdiensteanbieter

- (1)** Nachdem der Qualifikationsstatus in der Vertrauensliste ausgewiesen wurde, können qualif. VDA das EU-Vertrauenssiegel verwenden, um in einfacher, wiedererkennbarer und klarer Weise die von ihnen erbrachten qualifizierten Vertrauensdienste zu kennzeichnen.
- (3)** Durchführungsrechtsakt für Spezifikationen zur Form und Aufmachung, Zusammensetzung, Größe und Gestaltung des EU-Vertrauenssiegels.

Durchführungsverordnung (EU) 2015/806, ABI. Nr. L 128 vom 23.5.2015



Art. 20 eIDAS-VO – Beaufsichtigung qualifizierter Vertrauensdiensteanbieter

- (1)** Mind. alle 2 Jahre Prüfung durch Konformitätsbewertungsstelle und Vorlage an Aufsichtsstelle
- (2)** Jederzeitige Prüfung durch Aufsichtsstelle

„Konformitätsbewertungsstelle“

- Verordnung (EG) Nr. 765/2008 über die Vorschriften für die Akkreditierung von Konformitätsbewertungsstellen und Marktüberwachung von Produkten
- Bundesgesetz über die Akkreditierung von Konformitätsbewertungsstellen (Akkreditierungsgesetz 2012 – AkkG 2012), BGBl. I Nr. 28/2012 - „Akkreditierung Austria“, strenge Akkreditierungsverfahren
- CABS: <https://www.bmdw.gv.at/TechnikUndVermessung/Akkreditierung/Seiten/AkkreditiertePIZ-Stellen.aspx>
- EU: <https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation>

Art. 17 eIDAS-VO – Aufsichtsstelle

(1) MS benennen eine Aufsichtsstelle.

... Nähere Regelungen über die Aufsichtstätigkeiten/ Prüfungen/Zusammenarbeit mit anderen Aufsichtsstellen, Berichtspflichten...

Ex-ante- und Ex-post-Aufsichtstätigkeiten

§ 12 SVG – Aufsichtsstelle

- (1) Aufsichtsstelle gemäß Art. 17 eIDAS-VO ist die **Telekom-Control-Kommission** (§ 116 TKG 2003).
- (3) Die Aufsichtsstelle kann sich zur Beratung geeigneter Personen oder Einrichtungen wie etwa einer Bestätigungsstelle bedienen. Die Wahrnehmung ihrer Aufgaben in technischen Belangen hat in Abstimmung mit einer Bestätigungsstelle (§ 7) oder einer in einem anderen Mitgliedstaat der Europäischen Union gemäß Art. 30 Abs. 1 eIDAS-VO benannten Stelle zu erfolgen.

§ 12 SVG – Aufsichtsstelle

(4) Die Mitglieder der Aufsichtsstelle sind gemäß Art. 20 Abs. 2 B-VG bei Ausübung ihres Amtes an keine Weisungen gebunden.

§ 13 SVG: Die Aufsichtsstelle kann sich bei der Durchführung der Aufsicht der **RTR-GmbH** (§ 16 KOG) bedienen.

§ 15 SVG – Durchführung der Aufsicht

- (1) Die VDA haben das Betreten der Geschäfts- und Betriebsräume zu gestatten, Aufzeichnungen oder Unterlagen vorzulegen.
- (2) Die Organe des öffentlichen Sicherheitsdienstes haben der Aufsichtsstelle zur Durchführung der Aufsicht im Rahmen ihres gesetzmäßigen Wirkungsbereichs Hilfe zu leisten.
- (3) ...unter möglicher Schonung der Betroffenen und ohne unnötiges Aufsehen so durchzuführen, dass dadurch die Sicherheit der Vertrauensdienste nicht verletzt wird.

§ 10 SVG – Zugangsrechte (1/2)

- (1) Auf Ersuchen von Gerichten oder anderen Behörden hat ein qualifizierter VDA **Zugang zur Dokumentation** nach Art. 24 Abs. 2 lit. h eIDAS-VO und seiner Zertifikatsdatenbank zu gewähren.
- (2) Bei Verwendung eines **Pseudonyms** in einem Zertifikat hat der VDA die Daten über die Identität des Signators an einen Dritten zu übermitteln, sofern von diesem an der Feststellung der Identität ein **überwiegendes berechtigtes Interesse** glaubhaft gemacht wird. Die Übermittlung ist zu dokumentieren.

§ 10 SVG – Zugangsrechte (2/2)

(3) Die **Dokumentation** ist vom qualifizierten VDA **30 Jahre**, gerechnet ab dem im qualifizierten Zertifikat eingetragenen Ende der Gültigkeit oder, mangels eines solchen, 30 Jahre ab dem Zeitpunkt des Anfallens von einschlägigen Informationen über die von dem qualifizierten VDA im Rahmen seiner Tätigkeit ausgegebenen und empfangenen Daten, **aufzubewahren**.

Art. 3 eIDAS-VO – Begriffsbestimmungen...

40. „**Validierungsdaten**“ sind Daten, die zur Validierung einer elektronischen Signatur oder eines elektronischen Siegels verwendet werden.

41. „**Validierung**“ ist der Prozess der Überprüfung und Bestätigung der Gültigkeit einer elektronischen Signatur oder eines elektronischen Siegels.

Art. 32 eIDAS-VO – Anforderungen an die Validierung qualifizierter elektronischer Signaturen (1/3)

- (1) Mit dem Verfahren für die Validierung einer qualifizierten elektronischen Signatur wird die Gültigkeit einer qualifizierten elektronischen Signatur bestätigt, wenn
- a) das der Signatur zugrunde liegende Zertifikat **zum Zeitpunkt des Signierens** ein qualifiziertes Zertifikat für elektronische Signaturen war, das die Anforderungen des Anhangs I erfüllt,

Art. 32 eIDAS-VO – Anforderungen an die Validierung qualifizierter elektronischer Signaturen (2/3)

- b) das qualifizierte Zertifikat von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wurde und **zum Zeitpunkt des Signierens gültig** war,
- c) die **Signaturvalidierungsdaten** den Daten entsprechen, die dem vertrauenden Beteiligten bereitgestellt werden,
- d) der eindeutige Datensatz, der den **Unterzeichner** im Zertifikat repräsentiert, dem vertrauenden Beteiligten korrekt bereitgestellt wird,
- e) die etwaige Benutzung eines **Pseudonyms** dem vertrauenden Beteiligten eindeutig angegeben wird,

Art. 32 eIDAS-VO – Anforderungen an die Validierung qualifizierter elektronischer Signaturen (3/3)

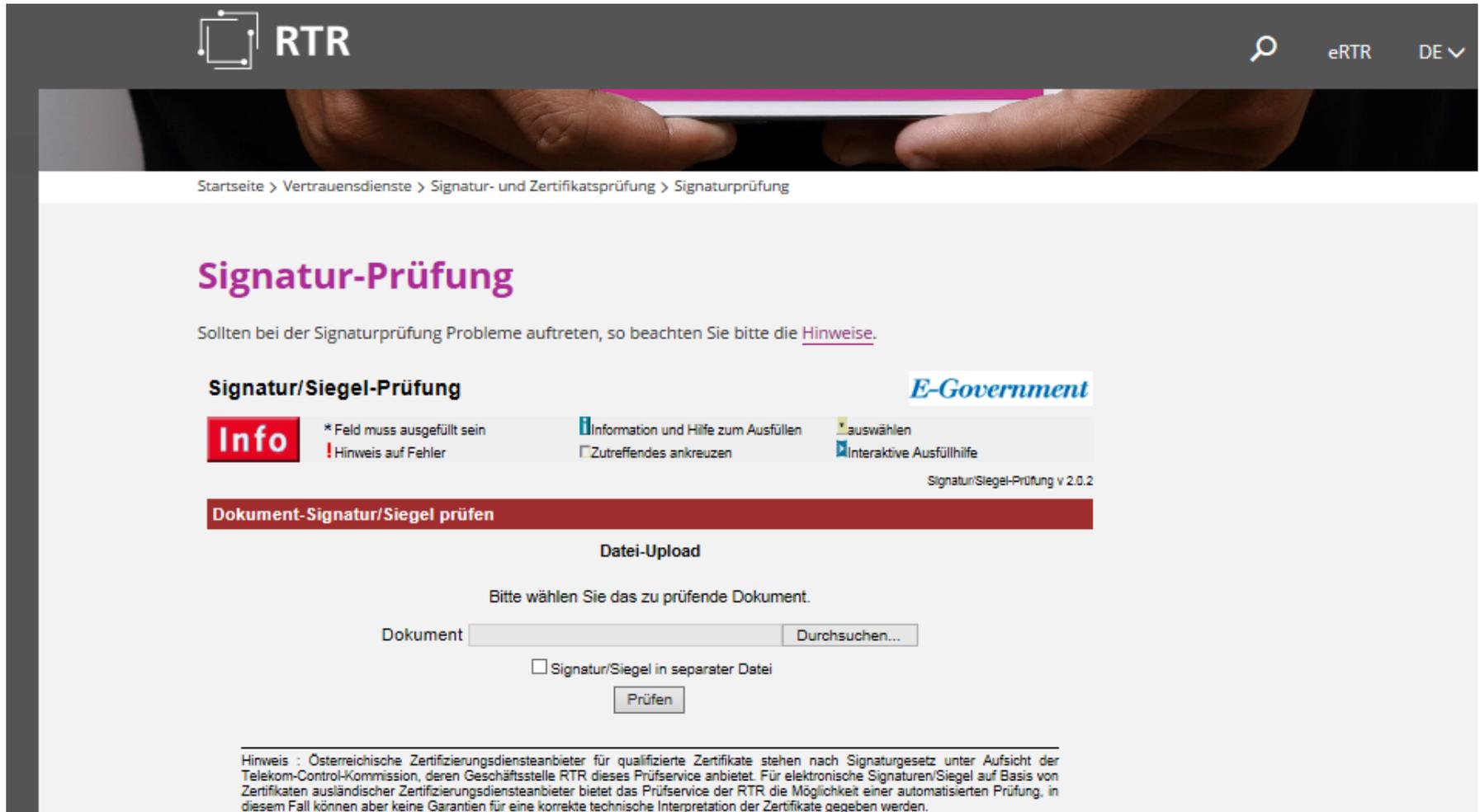
- f) die elektronische Signatur von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde,
- g) die Unversehrtheit der unterzeichneten Daten nicht beeinträchtigt ist,
- h) die Anforderungen des Artikels 26 zum Zeitpunkt des Signierens erfüllt waren.

Art. 33 eIDAS-VO – Qualifizierter Validierungsdienst für qualifizierte elektronische Signaturen (3/3)

- (1) Qualif. Validierungsdienste für können nur von qualifizierten VDA erbracht werden, die
- a) eine Validierung gemäß Art. 32 Abs 1 durchführen und
 - b) es vertrauenden Beteiligten ermöglichen, das Ergebnis automatisch in zuverlässiger und effizienter Weise mit Bestätigung durch die fortgeschrittene elektronische Signatur oder das fortgeschrittene elektronische Siegel des Anbieters des qualif. VDA zu erhalten.

§ 14 SVG - Validierungsservice

- (2) Die RTR-GmbH hat für die Aufsichtsstelle **im öffentlichen Interesse kostenfrei** im Internet ein **technisches Service** zur Verfügung zu stellen, **mit dem qualifizierte elektronische Signaturen oder qualifizierte elektronische Siegel validiert werden können**. Nach Maßgabe der technischen Möglichkeiten ist eine Schnittstelle für die automatische Verarbeitung anzubieten.
...Das Service hat ...die Anforderungen des Art. 32 Abs. 1 eIDAS-VO zu erfüllen.



The screenshot shows the RTR website interface for signature verification. At the top, there is a navigation bar with the RTR logo, a search icon, and language options for 'eRTR' and 'DE'. Below the navigation bar, a breadcrumb trail reads: 'Startseite > Vertrauensdienste > Signatur- und Zertifikatsprüfung > Signaturprüfung'. The main heading is 'Signatur-Prüfung' in purple. A sub-heading reads: 'Sollten bei der Signaturprüfung Probleme auftreten, so beachten Sie bitte die [Hinweise](#).' Below this, there is a section for 'Signatur/Siegel-Prüfung' with an 'E-Government' logo. An 'Info' box contains the following information: '* Feld muss ausgefüllt sein', '! Hinweis auf Fehler', 'Information und Hilfe zum Ausfüllen', 'Zutreffendes ankreuzen', 'auswählen', and 'Interaktive Ausfüllhilfe'. The version 'Signatur/Siegel-Prüfung v 2.0.2' is noted. A red bar highlights the 'Dokument-Signatur/Siegel prüfen' section. Under 'Datei-Upload', the instruction 'Bitte wählen Sie das zu prüfende Dokument.' is followed by a 'Dokument' input field and a 'Durchsuchen...' button. A checkbox for 'Signatur/Siegel in separater Datei' is also present, along with a 'Prüfen' button. A disclaimer at the bottom states: 'Hinweis : Österreichische Zertifizierungsdiensteanbieter für qualifizierte Zertifikate stehen nach Signaturgesetz unter Aufsicht der Telekom-Control-Kommission, deren Geschäftsstelle RTR dieses Prüfservice anbietet. Für elektronische Signaturen/Siegel auf Basis von Zertifikaten ausländischer Zertifizierungsdiensteanbieter bietet das Prüfservice der RTR die Möglichkeit einer automatisierten Prüfung, in diesem Fall können aber keine Garantien für eine korrekte technische Interpretation der Zertifikate gegeben werden.'

Ist somit die RTR-GmbH ein qualifizierter VDA (der sich selbst beaufsichtigt)?

Nein – siehe oben: Art. 3 eIDAS-VO –
Begriffsbestimmungen...

16. „**Vertrauensdienst**“ ist ein elektronischer Dienst, der **in der Regel gegen Entgelt** erbracht wird und

Art. 24 eIDAS-VO – Ausstellung qual. Zert. (1/3)

(1) Bei der Ausstellung eines qualifizierten Zertifikats **überprüft** der qualif. VDA **anhand geeigneter Mittel und im Einklang mit dem jeweiligen nationalen Recht** die **Identität** und gegebenenfalls die spezifischen **Attribute** der natürlichen oder juristischen Person, der das qualifizierte Zertifikat ausgestellt wird.

Die Informationen nach Unterabsatz 1 werden vom qualifizierten VDA **im Einklang mit dem nationalen Recht** entweder unmittelbar oder unter Rückgriff auf einen Dritten wie folgt überprüft:

Art. 24 eIDAS-VO – Ausstellung qual. Zert. (2/3)

- a) durch **persönliche Anwesenheit** der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person **oder**
- b) **aus der Ferne** mittels elektronischer Identifizierungsmittel, für die vor der Ausstellung des qualifizierten Zertifikats eine persönliche Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person gewährleistet war und die die Anforderungen gemäß Artikel 8 hinsichtlich der Sicherheitsniveaus „substanziell“ oder „hoch“ erfüllen, **oder**

Art. 24 eIDAS-VO – Ausstellung qual. Zert. (3/3)

- c) durch ein **Zertifikat einer qualifizierten elektronischen Signatur** oder eines qualifizierten elektronischen Siegels, das gemäß Buchstabe a oder b ausgestellt wurde, **oder**
- d) durch **sonstige Identifizierungsmethoden**, die auf **nationaler Ebene anerkannt** sind und **gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit** bieten. Die gleichwertige Sicherheit muss von einer **Konformitätsbewertungsstelle** bestätigt werden.

§ 8 SVG – Ausstellung qual. Zert. (1/2)

- 1) Ein qualifizierter VDA oder eine in seinem Auftrag tätige Stelle hat die Identität von **persönlich anwesenden** natürlichen Personen oder Vertretern einer juristischen Person, denen ein qualifiziertes Zertifikat ausgestellt werden soll, anhand eines **amtlichen Lichtbildausweises oder durch einen anderen in seiner Zuverlässigkeit gleichwertigen, dokumentierten oder zu dokumentierenden Nachweis festzustellen** (Art. 24 Abs. 1 lit. a eIDAS-VO). Vertreter von juristischen Personen haben darüber hinaus einen Nachweis über das Bestehen der Vertretungsbefugnis vorzulegen.

§ 3 SVV - Konkretisierung

Zur Feststellung der Identität von **persönlich anwesenden** natürlichen Personen oder Vertretern einer juristischen Person, denen ein qualifiziertes Zertifikat ausgestellt werden soll (§ 8 Abs. 1 SVG), geeignet sind ein

1. amtlicher Lichtbildausweis oder
2. ein Nachweis, der bescheinigt, dass die Identität zumindest mit jener Verlässlichkeit geprüft wurde, wie sie bei der Zustellung zu eigenen Händen (§ 21 ZustG) einzuhalten ist.

Die Daten des Lichtbildausweises oder des anderen Nachweises (§ 8 Abs. 1 erster Satz SVG) sind zu erfassen und mit dem Antrag zu dokumentieren, sofern sie nicht schon dokumentiert wurden. Die Erfassung und Dokumentation kann auch in ausschließlich elektronischer Form erfolgen.

§ 8 SVG – Ausstellung qual. Zert. (2/2)

- 2) Erfolgt die Ausstellung **nicht in persönlicher Anwesenheit**, können auch **sonstige Identifizierungsmethoden**, die eine gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten, angewendet werden (**Art. 24 Abs. 1 lit. d eIDAS-VO**). Dabei ist insbesondere **auf eine erfolgte Identifizierung anhand eines Nachweises iSd Abs. 1, die von einer vertrauenswürdigen Stelle durchgeführt wurde, zurückzugreifen.**

§ 5 SVG – Pflichten der Signatoren

Signatoren haben ihre elektronischen **Signaturerstellungsdaten sorgfältig zu verwahren**, soweit zumutbar **Zugriffe** von Dritten auf ihre elektronischen Signaturerstellungsdaten **zu verhindern** und deren Weitergabe an Dritte zu unterlassen... Signatoren haben den **Widerruf** des qualifizierten Zertifikats **zu verlangen**, wenn die elektronischen Signaturerstellungsdaten **abhandenkommen**, wenn Anhaltspunkte für deren **Kompromittierung** bestehen oder wenn **sich die im qualifizierten Zertifikat bescheinigten Umstände geändert** haben.

Art. 24 eIDAS-VO – Widerruf

- (3) Bei Widerruf: VDA **registriert den Widerruf in seiner Zertifikatsdatenbank** und veröffentlicht den Widerrufsstatus des Zertifikats zeitnah und in jedem Fall innerhalb von 24 Stunden nach Erhalt des Ersuchens. Der Widerruf wird sofort nach seiner Veröffentlichung wirksam.
- (4) ...Informationen über den Gültigkeits- oder **Widerrufsstatus** der ausgestellten qualifizierten Zertifikate. ... **jederzeit und über die Gültigkeitsdauer des Zertifikats hinaus automatisch**, zuverlässig, kostenlos..

Art. 28 eIDAS-VO – Aussetzung

- (5) MS können vorbehaltlich der folgenden Bedingungen **nationale Vorschriften zur vorläufigen Aussetzung** eines qual. Zertifikats für eine elektronische Signatur erlassen:
- a) Ist ein qualifiziertes Zertifikat für elektronische Signaturen vorläufig ausgesetzt worden, so **verliert dieses Zertifikat für die Dauer der Aussetzung seine Gültigkeit.**
 - b) Die Dauer der Aussetzung wird in der Zertifikatsdatenbank deutlich angegeben und der Status der Aussetzung ist während der Dauer der Aussetzung ersichtlich.

§ 6 SVG – Aussetzung (1/3)

(1) Sofern ein qual. VDA ein qual. Zertifikat nicht widerruft, hat er dieses vorläufig auszusetzen, wenn

- 1. der Signator, der Siegelersteller oder ein sonstiger dazu Berechtigter dies verlangt,**
- 2. die Aufsichtsstelle (§ 12) die Aussetzung des Zertifikats anordnet,**
- 3. der qualifizierte VDA Kenntnis vom Ableben des Signators, der Beendigung des Bestehens des Siegelerstellers oder sonst von der Änderung im Zertifikat bescheinigter Umstände erlangt,**

§ 6 SVG – Aussetzung (2/3)

4. das Zertifikat auf Grund **unrichtiger Angaben** erwirkt wurde oder
 5. die **Gefahr einer missbräuchlichen Verwendung** des Zertifikats besteht.
- (2) Ein qualifizierter VDA hat bei Vorliegen der in Abs. 1 genannten Umstände die Aussetzung zeitnah und in jedem Fall innerhalb von 24 Stunden nach Erhalt des Ersuchens vorzunehmen.

§ 6 SVG – Aussetzung (3/3)

- (3) Ist ein qualifiziertes Zertifikat für elektronische Signaturen oder elektronische Siegel vorläufig ausgesetzt worden, so **verliert dieses Zertifikat, solange der Status der Aussetzung gemäß Abs. 4 veröffentlicht ist, seine Gültigkeit**. Dieser Zeitraum **darf zwei Wochen nicht überschreiten**.
- (4) Ein qual. VDA hat die Dauer der Aussetzung in seiner Zertifikatsdatenbank zu registrieren und den Status der Aussetzung **während der Dauer der Aussetzung** elektronisch jederzeit allgemein zugänglich zu veröffentlichen.

§ 5 SVV – Aussetzung

- (7) Im Fall einer Aussetzung eines qualifizierten Zertifikats **ist der Signator oder der Siegelersteller unverzüglich zu verständigen. Die Aussetzung kann aufgehoben werden. Eine aufgehobene Aussetzung hat auf die Gültigkeit des Zertifikats keinen Einfluss. Wird eine Aussetzung nicht aufgehoben, so ist das Zertifikat zu widerrufen. Erfolgt auf Grund einer Aussetzung der Widerruf eines Zertifikats, so gilt bereits die Aussetzung als Widerruf.**

Art. 13 eIDAS-VO – Haftung des VDA (1/2)

(1) Unbeschadet des Absatzes 2 haften VDA für alle natürlichen oder juristischen Personen **vorsätzlich oder fahrlässig** zugefügten Schäden, die auf eine Verletzung der in dieser Verordnung festgelegten Pflichten zurückzuführen sind.

Die **Beweislast** für den Nachweis des Vorsatzes oder der Fahrlässigkeit seitens eines **nichtqualifizierten VDA** liegt **bei** der natürlichen oder juristischen **Person**, die den in Unterabsatz 1 genannten **Schaden geltend macht**.

Art. 13 eIDAS-VO – Haftung des VDA (2/2)

Bei einem **qualifizierten VDA wird von Vorsatz oder Fahrlässigkeit ausgegangen, es sei denn, der qualifizierte VDA weist nach**, dass der in Unterabsatz 1 genannte Schaden entstanden ist, ohne dass er vorsätzlich oder fahrlässig gehandelt hat.

- (2) Beschränkungen möglich, wenn informiert und ersichtlich – Haftung nicht bei einer über diese Beschränkungen hinausgehenden Verwendung
- (3) Anwendung „im Einklang mit den nationalen Vorschriften über die Haftung“

§ 11 SVG - Haftung

- (1) Abgesehen von Art. 13 Abs. 2 eIDAS-VO kann die Haftung eines VDA nach Art. 13 Abs. 1 eIDAS-VO im Vorhinein weder ausgeschlossen noch beschränkt werden.
- (2) Umfang und Ausmaß des nach Art. 13 eIDAS-VO zu ersetzenden Schadens sowie allfällige Rückgriffsrechte gegenüber anderen Personen richten sich nach den auf den Schadensfall sonst anwendbaren Bestimmungen.
- (3) Ersatzansprüche gegenüber anderen Personen oder aus einem anderen Rechtsgrund bleiben unberührt

Art. 24 eIDAS-VO - Beendigungsplan

(2) lit. i) VDA verfügen über einen fortlaufend aktualisierten **Beendigungsplan**, um die **Dienstleistungskontinuität** nach den von der Aufsichtsstelle gemäß Artikel 17 Absatz 4 Buchstabe i geprüften Vorgaben sicherzustellen

Dort ist als **Aufsichtsaufgabe** vorgesehen: Überprüfung des Vorliegens und der ordnungsgemäßen Anwendung von Vorschriften über Beendigungspläne für den Fall, dass der Vertrauensdiensteanbieter seine Tätigkeit einstellt, wobei auch die Frage, wie die Informationen (Dokumentationen...) weiter zugänglich gehalten werden, geprüft wird;

§ 9 SVG - Beendigungsplan und Vertrauensinfrastruktur (1/2)

- (1) Ein qualifizierter VDA hat der Aufsichtsstelle zumindest drei Wochen im Vorhinein die geplante Einstellung seiner Tätigkeit anzuzeigen.
- (2) Widerruf der gültigen qualifizierten Zertifikate oder dafür Sorge zu tragen, dass zumindest seine Zertifikatsdatenbank von einem anderen qualifizierten VDA übernommen wird. Auch im Fall des Widerrufs der qualifizierten Zertifikate hat der qualifizierte VDA sicherzustellen, dass die Zertifikatsdatenbank weitergeführt wird;

§ 9 SVG - Beendigungsplan und Vertrauensinfrastruktur (2/2)

- (2) kommt er dieser Verpflichtung nicht nach, so hat die **Aufsichtsstelle** als Teil ihrer Vertrauensinfrastruktur für die **Weiterführung der Zertifikatsdatenbank** auf Kosten des qualifizierten VDA Sorge zu tragen.
- (3) Ein **Widerruf** der gültigen qualifizierten Zertifikate gemäß Abs. 2 ist nur dann zulässig, **wenn** die Aufsichtsstelle auf Antrag des BMDW feststellt, dass deren **Weiterführung nicht im öffentlichen Interesse gelegen** ist. Ist der Widerruf unzulässig, hat der Bund für deren Weiterführung Sorge zu tragen.

Art. 27 eIDAS-VO - Elektronische Signaturen in öffentlichen Diensten (1/3)

- (1) Verlangt ein Mitgliedstaat für die Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle oder im Namen einer öffentlichen Stelle angeboten wird, eine **fortgeschrittene** elektronische Signatur, so erkennt dieser Mitgliedstaat fortgeschrittene elektronische Signaturen, fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat für elektronische Signaturen beruhen, und qualifizierte elektronische Signaturen zumindest in den **Formaten** oder unter Verwendung der Verfahren an, die in den Durchführungsrechtsakten nach Absatz 5 festgelegt sind.

Art. 27 eIDAS-VO - Elektronische Signaturen in öffentlichen Diensten (2/3)

(2) Verlangt ein Mitgliedstaat für die Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle oder im Namen einer öffentlichen Stelle angeboten wird, eine **fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht**, so erkennt dieser Mitgliedstaat fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen, und qualifizierte elektronische Signaturen zumindest in den **Formaten** oder unter Verwendung der Verfahren an, die in den Durchführungsrechtsakten nach Absatz 5 festgelegt sind.

Art. 27 eIDAS-VO - Elektronische Signaturen in öffentlichen Diensten (3/3)

- (3) Die Mitgliedstaaten **verlangen** für die grenzüberschreitende Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle angeboten wird, **keine elektronische Signatur mit einem höheren Sicherheitsniveau als dem der qualifizierten elektronischen Signatur.**
- (4) und (5)...Komitologiebeschlüsse für Normen und Referenzformate...

„**Signaturformate**“

Siehe den **Durchführungsbeschluss (EU) 2015/1506** zur Festlegung von Spezifikationen für Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener Siegel, die von öffentlichen Stellen gemäß Artikel 27 Absatz 5 und Artikel 37 Absatz 5 der Verordnung (EU) Nr. 910/2014.

- MS erkennen fortgeschrittene elektronische **XML-, CMS- und PDF-Signaturen** der Konformitätsstufen **B, T oder LT** und Signaturen mit zugehörigen Containern an, wenn diese Signaturen die technischen Spezifikationen des Anhangs erfüllen...
- Bei **anderen Formaten: Validierungsservice** muss angeboten werden (kostenlos, online, verständlich...)

Elektronisches Siegel

- „Signatur“ der **juristischen** Person
- Art. 3 Z 25 eIDAS-VO: „Elektronisches Siegel“ sind Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt oder logisch mit ihnen verbunden werden, **um deren Ursprung und Unversehrtheit sicherzustellen.**
- Begrifflichkeiten angepasst:
 - Signator – Siegelersteller
 - Signaturerstellungsdaten – Siegelerstellungsdaten
 - Signaturerstellungseinheit – Siegelerstellungseinheit

Art. 35 eIDAS-VO – Rechtswirkungen el. Siegel

- (1) Einem elektronischen Siegel darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in einer elektronischen Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Siegel erfüllt.
- (2) Für ein **qualifiziertes elektronisches Siegel** gilt die **Vermutung der Unversehrtheit der Daten** und der **Richtigkeit der Herkunftsangabe** der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist.
- (3) Ein qualifiziertes elektronisches Siegel, das auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruht, wird in allen anderen Mitgliedstaaten als qualifiziertes elektronisches Siegel anerkannt.

Art. 14 eIDAS-VO – Internationale Aspekte

- (1) Vertrauensdienste, die von in einem Drittland niedergelassenen Vertrauensdiensteanbietern bereitgestellt werden, werden als rechtlich gleichwertig mit den Vertrauensdiensten anerkannt, die von in der Union niedergelassenen qualifizierten Vertrauensdiensteanbietern bereitgestellt werden, sofern die Vertrauensdienste aus dem Drittland im Rahmen einer gemäß Artikel 218 AEUV geschlossenen **Vereinbarung zwischen der Union und dem betreffenden Drittland oder einer internationalen Organisation** anerkannt sind.
- (2) Regelt nähere Voraussetzungen

Zusammenfassung

1. „Unterschrift“ - „Elektronische Unterschrift“
2. Praktische Demonstration
3. Technischer Hintergrund
4. Detaillierte Darstellung des Rechtsrahmens:
EU (eIDAS-VO) und national (SVG)

Überblick

- E-Kommunikation birgt Risiken in sich
 - Wer ist mein Gegenüber?
 - Wurde etwas verändert?
- Lösung dazu elektronische Signatur/Siegel
 - Elektronisch signierte Texte können nicht unbemerkt verändert werden (weder am Übertragungsweg noch vom Empfänger)
 - Absender kann Text nicht abstreiten (z.B. verbindliches Angebot)
- Elektronische Signaturen/Siegel gibt es in unterschiedlichen Qualitäten
 - Einfache Signaturen/Siegel (geringere technische und organisatorische Anforderungen)
 - Qualifizierte Signatur/Siegel (hohe technische und organisatorische Anforderungen)

Elektronische Signatur

▪ „Einfache“ elektronische Signatur

- Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet

▪ „fortgeschrittene“ elektronische Signatur

- elektronische Signatur, die die Anforderungen des Artikels 26 der eIDAS-VO erfüllt:
 - a) ist eindeutig dem Unterzeichner zugeordnet.
 - b) ermöglicht die Identifizierung des Unterzeichners.
 - c) wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.
 - d) ist so mit den unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

▪ „qualifizierte“ elektronische Signatur

- Ist eine fortgeschrittene Signatur
- beruht auf einem qualifizierten Zertifikat
- mit einer qualifizierten Signaturerstellungseinheit (QSCD) erzeugt.

Rechtswirkung

- „Einfache“ & „fortgeschrittene“ Signatur
 - müssen als Beweismittel zugelassen werden
 - unterliegen der richterlichen Beweiswürdigung
 - Grundsatz der Nichtdiskriminierung
- **„Qualifizierte“ Signatur**
 - der handschriftlichen Unterschrift gleichgestellt (Art. 25 Abs. 2 eIDAS-VO iVm § 4 Abs. 1 SVG (-Erfordernis der Schriftlichkeit nach §886 ABGB))
 - Ausnahmen:
 - Letztwillige Verfügungen
 - bei Schriftformerfordernis im Familien- & Erbrecht*
 - Bürgschaftserklärungen (außer Geschäftsverkehr)*

* Diese Willenserklärungen können in elektr. Form abgefasst werden, wenn Signator von Rechtsanwalt/Notar über Rechtsfolgen der Signatur aufgeklärt wurde.

Qual. Signatur – qual. Siegel

- Qualifizierte elektronische Signatur – nat. Person
 - Rechtswirkungen (Art. 25 eIDAS-VO): „der handschriftlichen Unterschrift gleichgestellt“
- Elektronische Siegel – jur. Person (weiter Begriff)
 - Rechtswirkung qual. elektronischer Siegel (Art. 35 Abs. 2 eIDAS): „Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist.“

Berücksichtigung innovativer Möglichkeiten
(server/remote signing; HSM etc.)

Qualifiziertes Zertifikat

- Basis für qualifizierte elektronische Signatur (Anhang I eIDAS-VO):
 - Hinweis, dass es sich um ein qualifiziertes Zertifikat handelt
 - den unverwechselbaren Namen des qu. Vertrauensdiensteanbieters (VDA) und den Staat seiner Niederlassung
 - Namen des Signators
 - Signaturvalidierungsdaten
 - Gültigkeitsdauer des Zertifikats
 - eindeutige Kennung des Zertifikats
 - Signatur/Siegel des qu. VDA

Vertrauensdiensteanbieter (VDA)

- VDA (Art. 3 Z 19 eIDAS-VO) = natürliche od. juristische Person, die einen oder mehrere Vertrauensdienste erbringt
- Spezielle Anforderungen an qualifizierte VDA in Art. 24 eIDAS-VO
- Zulassung durch die Aufsichtsbehörde (Telekom-Control-Kommission bzw. RTR) – konstitutive Liste
- Vor Zulassung als qualifizierter Vertrauensdienste ist vom VDA ein Konformitätsbewertungsbericht vorzulegen (Art. 21 eIDAS-VO)

Ausstellung eines qualifizierten Zertifikats

Qu. VDA (od. in seinem Auftrag tätige Stelle) hat gem. Art. 24 Abs. 1 eIDAS-VO iVm § 8 Abs. 1 SVG die Identität **von persönlich anwesenden Personen** anhand:

- eines amtlichen Lichtbildausweises oder
- durch einen anderen in seiner Zuverlässigkeit gleichwertigen, dokumentierten oder zu dokumentierenden Nachweis festzustellen

Bei **nicht persönlich anwesenden Personen**, können auch gem. § 8 Abs. 2 SVG auch sonstige Identifizierungsmethoden, die eine gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten, angewendet werden.

- Rückgriff auf bereits erfolgte Identifizierung anhand eines Nachweises gem. Abs. 1 durch vertrauenswürdige Stelle

Qualifizierte Signaturerstellungseinheit

- Verarbeitung der Signaturerstellungsdaten
 - Chipkarte/ HSM



- Nicht: Systemumgebung/ Kartenleser/ Signatursoftware/...
- Erfüllung der Sicherheitsanforderungen muss von einer Bestätigungsstelle gem. § 7 SVG (in Ö: A-Sit) bescheinigt sein (Art. 30 Abs. 1 eIDAS-VO)

Berufsspezifische Ausprägungen der elektronischen Signaturen

- Für Berufsgruppen
 - Elektronische Beurkundungssignatur der Notare
 - El. Notarsignatur
 - El. Anwaltssignatur
 - El. Beurkundungssignatur der Ziviltechniker
 - El. Ziviltechnikersignatur
- Für Behörden
 - Elektronische Signatur der Justiz
 - Amtssignatur

**Seit 1.7.2016:
„Siegel“!**

Elektronisches Siegel

- Für juristische Personen
- „digitaler Stempel“
- Für qu. elektr. Siegel gelten ähnliche Anforderungen wie für qu. elektr. Signaturen
- **Nicht** dieselben Rechtswirkungen einer qu. Elektronischen Signatur!
- Mit elektronischen Siegeln werden der Ursprung und die Unversehrtheit von Daten sichergestellt (Art. 3 Z 25 iVm. Art. 35ff eIDAS-VO).

Danke

für Ihre Aufmerksamkeit!

Peter Kustor

Bundesministerium für Digitalisierung und Wirtschaftsstandort

Leiter der Abteilung III/4 –

Digitales und E-Government – Recht, Strategie und Internationales

Peter.Kustor@bmdw.gv.at

 @PeterKustor



Links

- **Digitales Österreich**, www.digitales.oesterreich.gv.at
- **Das E-Government-ABC**: www.digitales.oesterreich.gv.at/abc
- **Reference-Server**
Auf diesem Server werden die gemeinsam von Bund, Ländern und Gemeinden erarbeiteten Vorschläge und Empfehlungen publiziert.
<http://reference.e-government.gv.at/>
- **HELP.gv.at**: <http://www.help.gv.at/>
- **Unternehmensserviceportal**: www.usp.gv.at
- **IKT-Sicherheitsportal**: <https://www.onlinesicherheit.gv.at/>
- **Datenschutz**
offizielle Website der österreichischen Datenschutzbehörde
<http://www.dsb.gv.at/>

Links

- Konzept Bürgerkarte: <http://www.buergerkarte.at/>
- Handy-Signatur: <http://www.handy-signatur.at/>
- Monitoring Handy-Signatur: <https://www.a-trust.at/handystat/>
- Monitoring E-Government Systeme: <http://pubmon.egiz.gv.at/>
- Zentrum für sichere Informationstechnologie - Austria (A-SIT)
<http://www.a-sit.at/>