Selected Topics IT-Security 1

Electronic Signatures

Andreas Abraham
andreas.abraham@iaik.tugraz.at
Graz, 09.10.2019

EGIZ
E-Government Innovationszentrum

Das E-Government Innovationszentrum ist eine
gemeinsame Einrichtung des BMDW und der TU Graz

TU Graz

Overview

- Electronic Signatures
- Legal Framework
- Signature Formats
- Official Signature
- Signature Verification
- Research
- Conclusion

Overview

- Electronic Signatures
- Legal Framework
- Signature Formats
- Official Signature
- Signature Verification
- Research
- Conclusion

Electronic Signatures | Why do we need Signatures?

- Once upon a time… a Seal
  - Securing of documents
- Stamp and Signature vs.
- Electronic Signature Block

BPOLDION WIEN STRAFREGISTERAMT

WASAG.22
1090 WIEN

BEZUG: III-STRB-384-STRA/2005 (ANFRNR. 0002604) SB

STRAFREGISTERBESCHEINIGUNG

Familienname(n):	LEITOLD
Geschlecht:	MAENNLICH
Vorname(n):	HERBERT
Akad. Grad:	DI
Geboren am:	[redacted]
Geburtsort:	GRAZ STMK

Im Strafregister der Republik Österreich - geführt von der Bundespolizeidirektion Wien - scheint keine Verurteilung auf.

DVR: 0003506

Tagesdatum 23.09.2005
Uhrzeit 13.24.24

Gebühr entrichtet

Landespolizeidirektion Wien
Strafregisteramt

Wasagasse 22
1090 Wien

Zur Vorlage bei:
E-Government Innovationszentrum

Inffeldgasse 16a

8010 Graz

BEZUG: SRB2013092713350082 SB
(REFERENCE NUMBER)

STRAFREGISTERBESCHEINIGUNG
(CRIMINAL RECORD CERTIFICATE)

Familienname(n): (Family Name)	STRANACHER
Geschlecht: (Gender:	MAENNLICH MALE)
Vorname(n): (First Name)	KLAUS
Akad. Grad: (Academic Degree)	DIPL.-ING.
Geboren am: (Date of Birth:	[redacted] DD.MM.YYYY)
Geburtsort: (Place of Birth)	KLAGENFURT
Staatsang.: (Nationality)	Österreich

Im Strafregister der Republik Österreich - geführt von der Landespolizeidirektion Wien - scheint keine Verurteilung auf.

(No convictions are listed in the criminal records database of the Republic of Austria, kept by the Federal Police Directorate of Vienna.)

DVR: 0003506

Tagesdatum (Date): 27.09.2013
Uhrzeit (Time): 13.49.32

Signaturwert	U3ABlQ+4VPo4L/TWuyrt1HIN27mMPa4D618yBAJ3xXpjHhVmo7ynEslAzc36DVlfYAKByADHa6/fublEtylooi/DGoI3p93T+Blr0tGnVc4AQIh+JSoo3VbQGK/eygtQgU4gOJzzVys6qMkRHTnhV1EJBqX11eKkiN3xR8qhPJghuv/KXJZxP/61XStHfb9ym/W6DpVg6Fwy9s2NTLsIqQ6UKk26t9VOXbaPiHr5Uhh1KiNIMUt+Up7UGnosyOG6NxX81vPTBveWSAVYWZj1+IFe2OCXT4JrvnrE191eHF7IY4M6BPdRNpXpcS1YmabgAOJH+tkMCX+Y63PDK36jpw==	
	Datum/Zeit-UTC	2013-09-27T13:49:35+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	465297
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	etsi-bka-moa-1.0
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

Electronic Signatures | Features

- Authenticity of originator and data
  - Mapping data to signatory
- Data integrity
- Protection against:
  - Repudiation
  - Forgery
  - Data manipulation

Electronic Signatures | Basic Principle

- Public Key Cryptography
  - Key pair (public/private)
  - Public certificate:
    - Public key is assigned to exactly one person (signatory)
    - Verification of the signatory's identity on different levels of assurance
    - → Quality of the authenticity depends on this identification
    - Issuance and identification by the trust service provider (TSP)

Electronic Signatures | Basic Principle

- Signature creation
  - Creating the document
  - Calculating the hash value
  - Signing the hash value with private key
  - Distributing the signed message

    (including the public key/certificate)

Electronic Signatures | Basic Principle

- Signature Verification
  - The hash value of the received document is calculated
  - The signature is verified using the signatory's public key and the original hash value
  - Comparison of the hash values
  - Matching hash values → message not altered
  - Authenticity of the signatory ensured by the private/public key binding

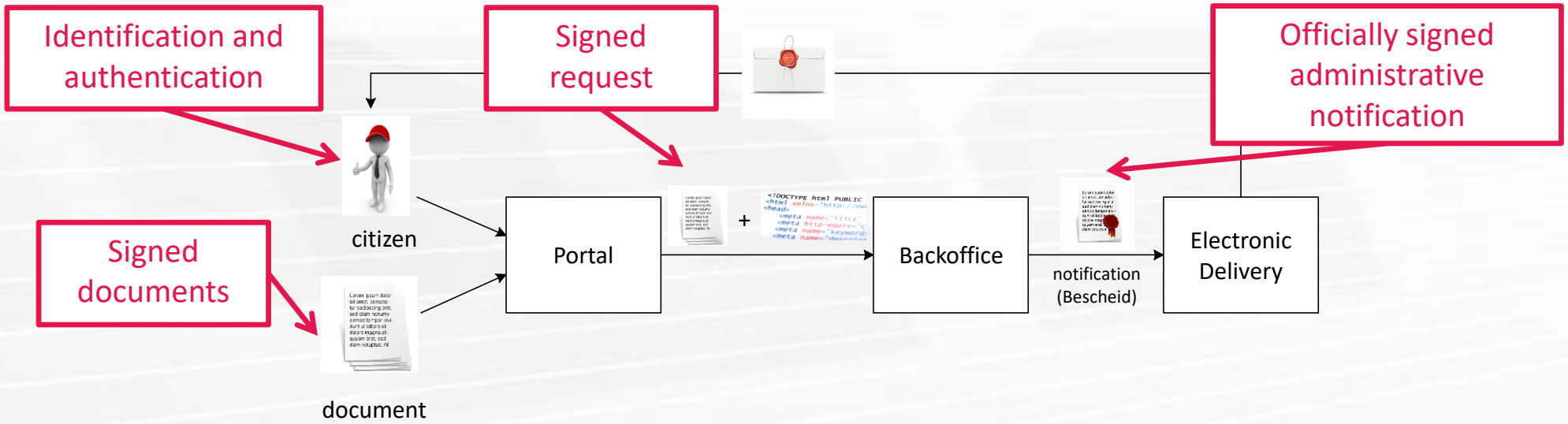
Certificate validation is also necessary!
Coming later.

Electronic Signatures | Identification vs. Authentication

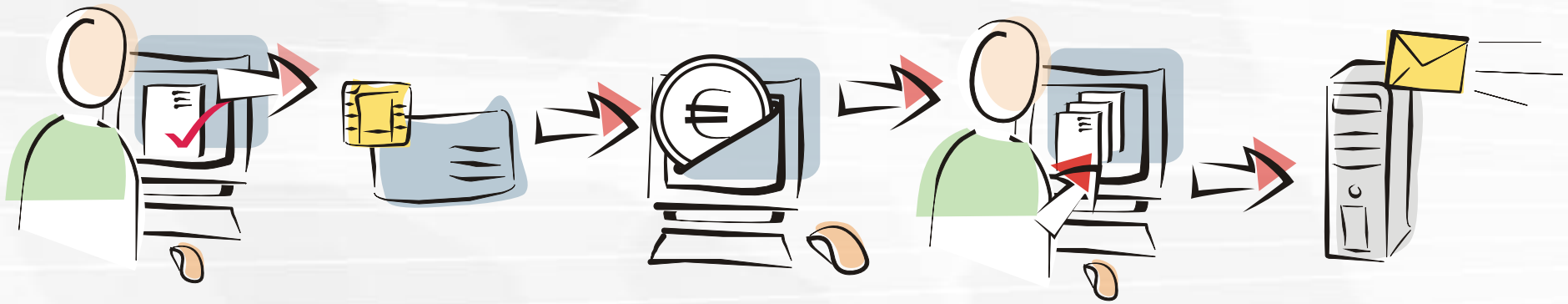
- Identification
  - Identification is the association of a personal identifier with an individual presenting attributes [clarke]
  - e.g. “I am Alice Doe”
- Authentication
  - Authentication is the proof of attributes [clarke]
  - e.g. Proof by verifying attributes by using a passport

Electronic Signatures | eGovernment

- Where are signatures used?
- → Generic E-Government Process



Example: Criminal Record Certificate



Login to fill in a form

Sign the request

Payment

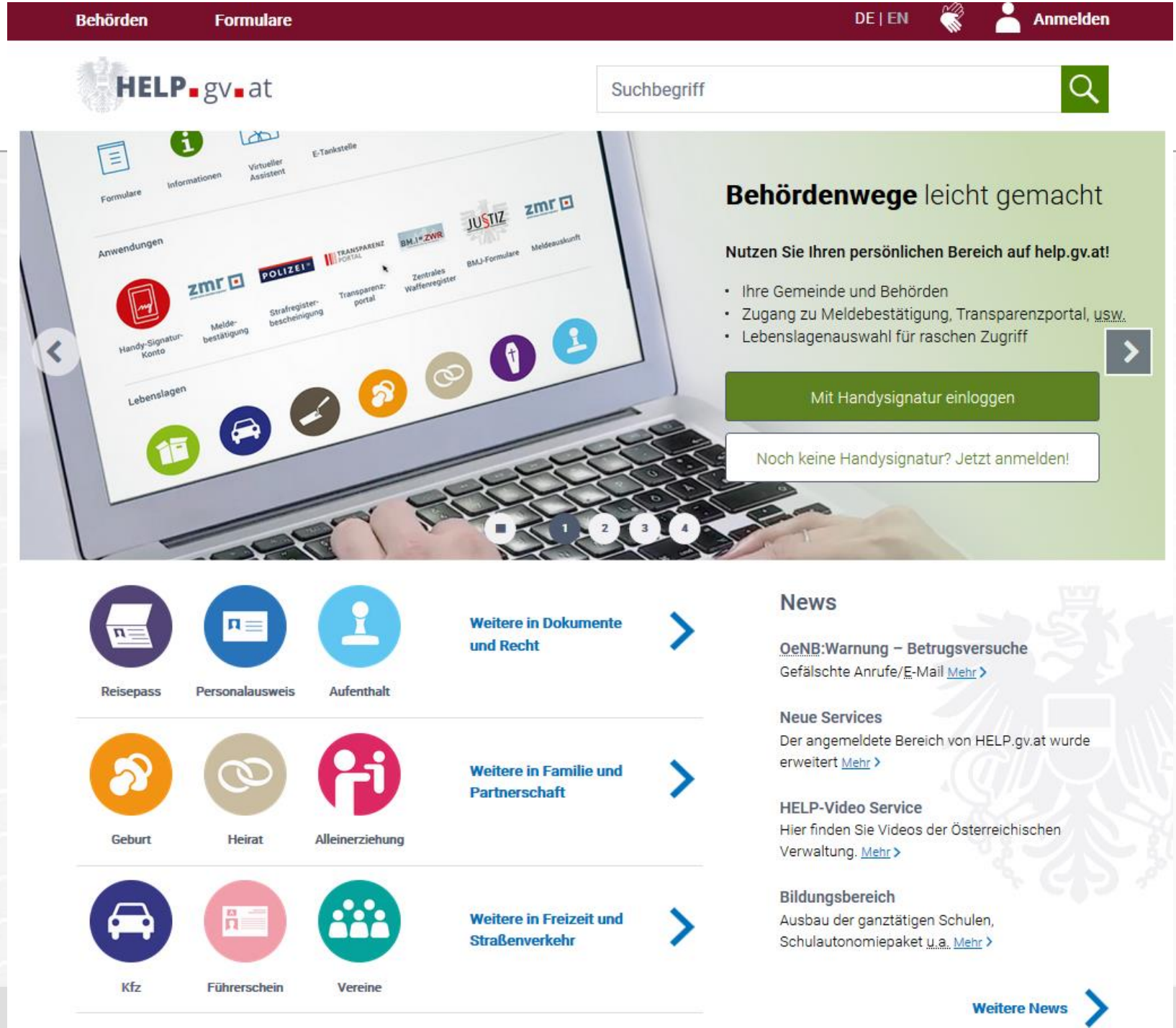
Back office processing (ELAK)

Electronic delivery

www.help.gv.at

www.meinbrief.at

1| Help.gv.at


Behörden
Formulare
DE | EN
Anmelden
HELP.gv.at
Suchbegriff
Behördenwege leicht gemacht
Nutzen Sie Ihren persönlichen Bereich auf help.gv.at!
Ihre Gemeinde und Behörden
Zugang zu Meldebestätigung, Transparenzportal, usw.
Lebenslagenauswahl für raschen Zugriff
Mit Handysignatur einloggen
Noch keine Handysignatur? Jetzt anmelden!
Reisepass
Personalausweis
Aufenthalt
Weitere in Dokumente und Recht
Geburt
Heirat
Alleinerziehung
Weitere in Familie und Partnerschaft
Kfz
Führerschein
Vereine
Weitere in Freizeit und Straßenverkehr
News
OeNB:Warnung – Betrugsversuche
Gefälschte Anrufe/E-Mail Mehr
Neue Services
Der angemeldete Bereich von HELP.gv.at wurde erweitert Mehr
HELP-Video Service
Hier finden Sie Videos der Österreichischen Verwaltung. Mehr
Bildungsbereich
Ausbau der ganztätigen Schulen, Schulautonomiepaket u.a. Mehr
Weitere News

2| Forwarded to the Police Department

REPUBLIK ÖSTERREICH

.LPD REPUBLIK ÖSTERREICH
LANDESPOLIZEIDIREKTION WIEN

Zeichenerklärung

* Feld muss aufgefüllt sein. Hinweis auf Fehler. Information und Hilfe zum Ausfüllen. Zutreffendes ankreuzen oder auswählen.

Information zur Strafregisterbescheinigung

Mit diesem Online-Formular können Sie die Ausstellung einer Strafregisterbescheinigung beantragen.

Das Strafregister ist ein zentral geführtes Register über rechtskräftige Verurteilungen durch inländische Strafgerichte sowie aller rechtskräftigen Verurteilungen österreichischer Staatsbürger und von Personen, die in Österreich ihren Wohnsitz oder gewöhnlichen Aufenthalt haben, durch ausländische Strafgerichte, sofern der Tatbestand auch nach österreichischen strafrechtlichen Bestimmungen gerichtlich strafbar ist. Für die Führung des Strafregisters ist die Landespolizeidirektion Wien (Strafregisteramt) zuständig.

Die Strafregisterbescheinigung (Bescheinigung gemäß § 10 des Strafregistergesetzes; früher: Leumunds-, Führungs- oder Sittenzeugnis) gibt Auskunft über die im Strafregister eingetragenen Verurteilungen einer Person bzw. darüber, dass das Strafregister keine solche Verurteilung enthält.

Für viele Tätigkeiten und Berufe (z.B. Ausstellung eines Gewerbescheins, Aufnahme in ein Sicherheits- oder Bewachungsunternehmen) ist die Vorlage einer aktuellen Strafregisterbescheinigung, die keine Verurteilungen enthält, erforderlich. Die Gültigkeitsdauer einer Strafregisterbescheinigung ist gesetzlich nicht geregelt. Im Regelfall wird die Vorlage eines Dokumentes, dessen Ausstellungsdatum nicht länger als 3 Monate zurückliegt, verlangt.

Gebühren:

- Bei Verwendung als Zeugnis EUR 22,90 plus EUR 2,10 Verwaltungsabgabe
- Zur Vorlage ausschließlich bei einer exakt zu bezeichnenden Stelle (z.B. Behörde, Versicherung, Bank, Unternehmen, Verein, vom Antragsteller verschiedene natürliche Person odgl.) EUR 8,60 plus EUR 2,10 Verwaltungsabgabe.

Achtung:

Für die Ausstellung der Strafregisterbescheinigung auf elektronischem Wege werden die im Zentralen Melderegister gespeicherten Personen- und Wohnsitzdaten herangezogen. Ein allenfalls verliehener akademischer Grad, der nicht im Zentralen Melderegister gespeichert ist, scheint daher in der Strafregisterbescheinigung nicht auf. Sollten Sie dennoch auf die Eintragung Ihres akademischen Grades in der Strafregisterbescheinigung Wert legen, der nicht im Zentralen Melderegister gespeichert ist, müssten Sie auch in diesem Falle den Antrag auf konventionellem Weg einbringen. Die örtlich und sachlich zuständige Behörde wäre in diesem Fall, je nach Ihrem momentanen Aufenthalt,

- innerhalb Österreichs: das Gemeindeamt bzw. die Landespolizeidirektion (in Wien das nächste Polizeikommissariat)
- im Ausland: die nächstgelegene österreichische Vertretungsbehörde (Botschaft, Konsulat)

Voraussetzungen

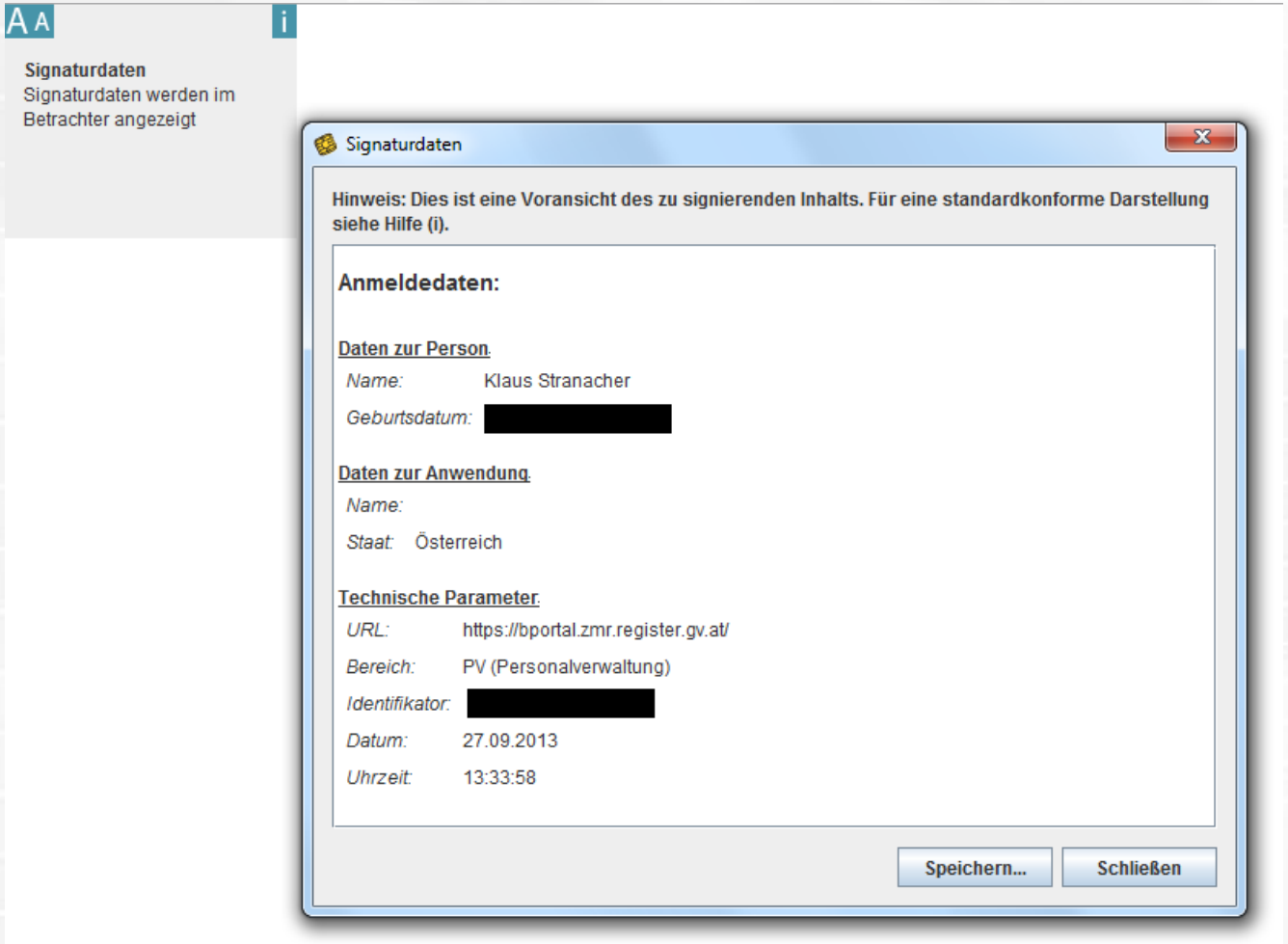
1. Eine Bürgerkarte (Chipkarte laut Konzept Bürgerkarte oder Handysignatur)
2. Eine Möglichkeit der elektronischen Bezahlung (mit einer Kreditkarte oder durch eps-Online-Überweisung via Raiffeisen-Bank, BA-CA, Erste Bank, BAWAG/P.S.K., Hypo Oberösterreich, Hypo Salzburg, Hypo Steiermark, Hypo Niederösterreich, Hypo Tirol, Hypo Vorarlberg oder Volksbanken)
3. Wenn Sie die elektronische Zustellung wünschen, müssen Sie bei einem elektronischen Zustelldienst registriert sein (für eine Liste der registrierten Zustelldienste siehe www.bka.gv.at/zustelldienste)

Verfahrensschritte

1. Auswahl der Bürgerkarte
2. Ausfüllen des Formulars
3. Signieren des Antrages
4. Bezahlung der anfallenden Gebühr(en) mittels elektronischer Bezahlung

3| Log in using the Citizen Card

4| Display and Signing of Login Data



5| Completion of Form

REPUBLIK ÖSTERREICH

.LPD REPUBLIK ÖSTERREICH
LANDESPOLIZEIDIREKTION WIEN

Zeichenerklärung

* Feld muss aufgefüllt sein. Hinweis auf Fehler. Information und Hilfe zum Ausfüllen. Zutreffendes ankreuzen oder auswählen.

Antrag auf Ausstellung einer Strafregisterbescheinigung

Absender/in

Akad. Grad: Dipl.-Ing.
Familienname: Stranacher
Vorname: Klaus
E-Mail Adresse: *

Zur Anfrage im Register benötigte Personenmerkmale

Geschlecht: männlich
Frühere Familiennamen:
Weitere frühere Familiennamen:
Geburtsdatum: [redacted]
Geburtsort: [redacted]
Vorname des Vaters: *
"unbekannt" eintragen, falls Name nicht bekannt
Vornamen der Mutter: *
"unbekannt" eintragen, falls Name nicht bekannt

Verwendungszweck

* Zur Vorlage ausschließlich bei einer exakt zu bezeichnenden Stelle (z.B. Behörde, Versicherung, Bank, Unternehmen, Verein, vom Antragsteller verschiedenen natürlichen Person odgl.) (Gebühr EUR 16,40)

Name: *
Strasse Hausnr.: *
PLZ Ortschaft: *
Staat:

* Als Zeugnis (gültig gegenüber jedermann; Gebühr 30,70)

Art der Zustellung

Elektronische Zustellung: Ich bin bei einem elektronischen Zustellservice registriert und ersuche nach Möglichkeit um Zustellung über dieses.
(Strafregisterbescheinigungen können dzt. dann elektronisch zugestellt werden,

Art der Zustellung

Elektronische Zustellung ☑ Ich bin bei einem elektronischen Zustellservice registriert und ersuche nach Möglichkeit um Zustellung über dieses.
(Strafregisterbescheinigungen können dzt. dann elektronisch zugestellt werden, wenn auf Grund der Personendaten eindeutig festgestellt werden kann, ob über Sie Strafen registriert sind und Sie nicht gefahndet werden.)

Für den Fall, dass Sie die elektronische Zustellung nicht wünschen oder diese nicht möglich ist, geben Sie bitte bekannt, auf welchem (konventionellen) Weg die Strafregisterbescheinigung zugestellt werden soll.

Brief-Qualität
- ○ Normal-Brief
- ◉ RSa-Brief

Auswahl der Zustelladresse (Hauptwohnsitz laut ZMR ODER andere Adresse)

Auswahl
- ◉ * Hauptwohnsitz laut ZMR
- ○ * andere Adresse

Postalische Zustelladresse (Hauptwohnsitz laut ZMR)

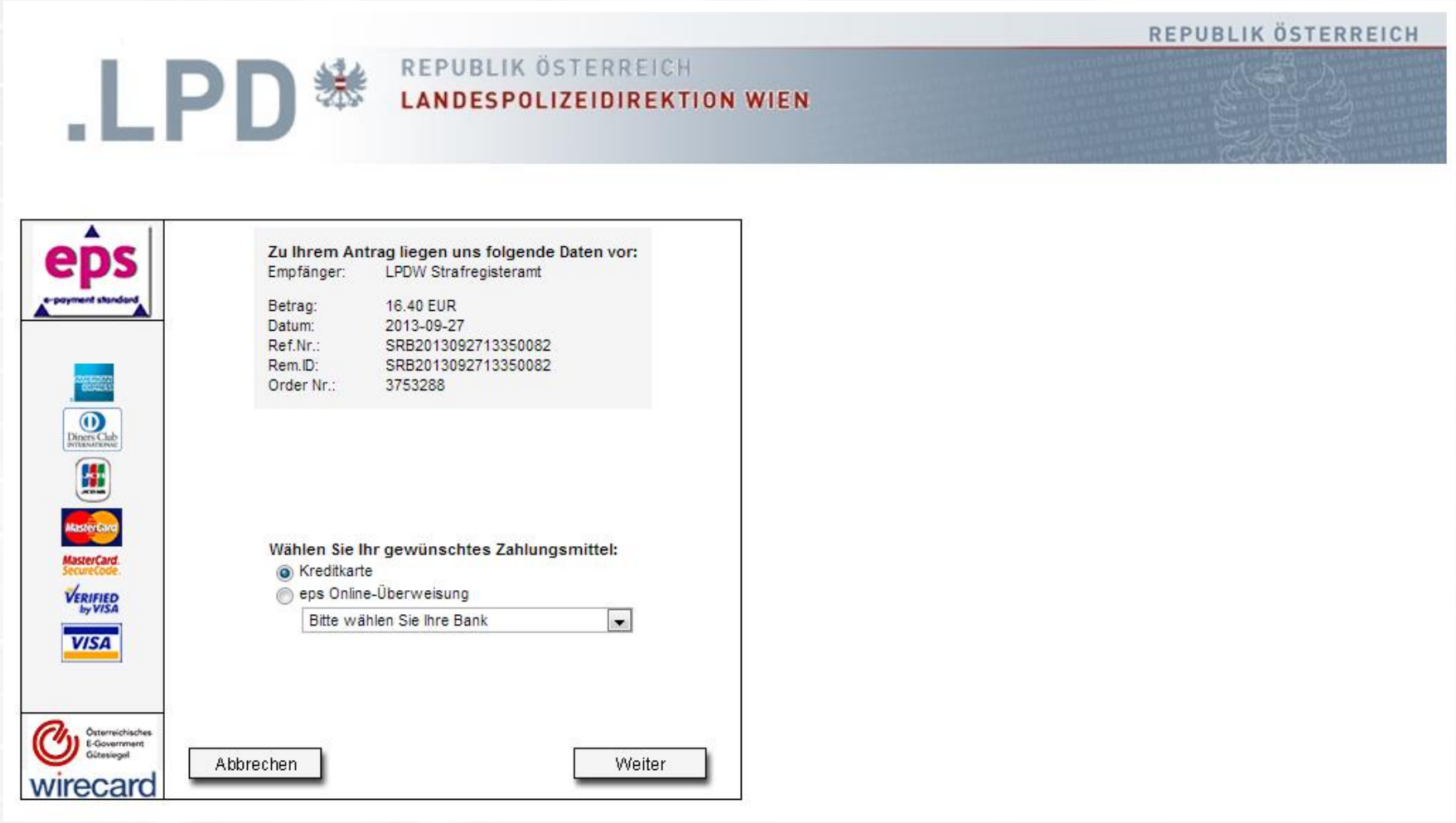
Strasse	[redacted]
Hausnummer	[redacted]
Stiege	
Tür	
Postleitzahl	[redacted]
Ort	[redacted]
Staat	

Antrag signieren

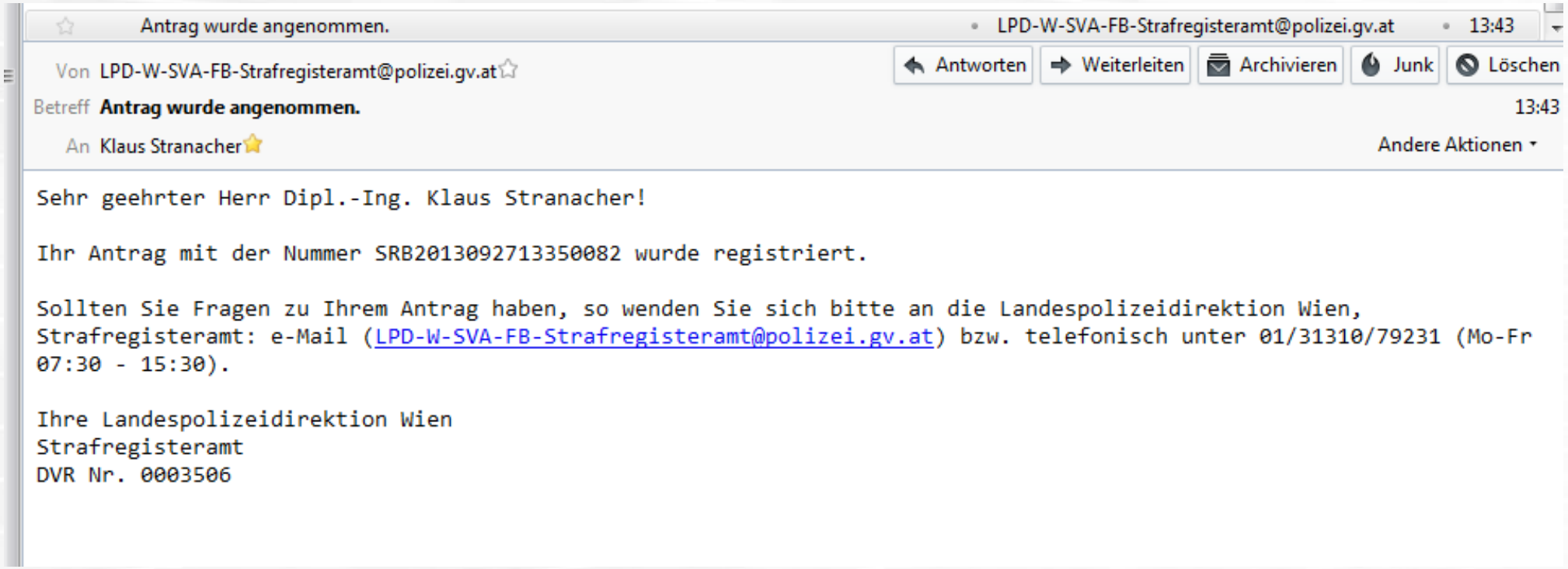
6| Signing of Request using Citizen Card

7| Display and Signing of Request

8| Payment using Electronic Payment System (EPS)



9| Request Confirmation via email



Antrag wurde angenommen. • LPD-W-SVA-FB-Strafregisteramt@polizei.gv.at • 13:43

Antworten | Weiterleiten | Archivieren | Junk | Löschen

Von LPD-W-SVA-FB-Strafregisteramt@polizei.gv.at

Betreff **Antrag wurde angenommen.** 13:43

An Klaus Stranacher Andere Aktionen

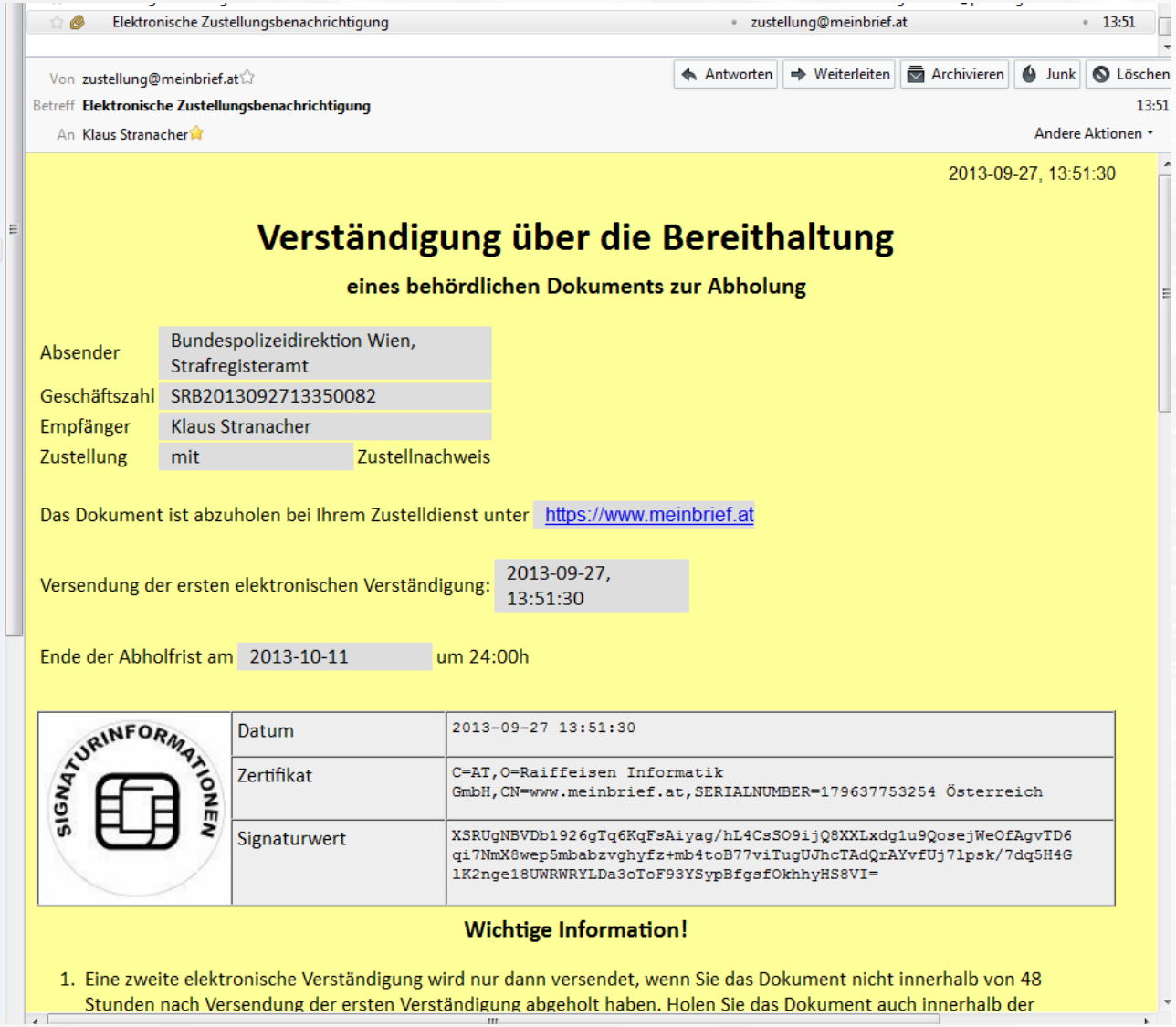
Sehr geehrter Herr Dipl.-Ing. Klaus Stranacher!

Ihr Antrag mit der Nummer SRB2013092713350082 wurde registriert.

Sollten Sie Fragen zu Ihrem Antrag haben, so wenden Sie sich bitte an die Landespolizeidirektion Wien, Strafregisteramt: e-Mail (LPD-W-SVA-FB-Strafregisteramt@polizei.gv.at) bzw. telefonisch unter 01/31310/79231 (Mo-Fr 07:30 - 15:30).

Ihre Landespolizeidirektion Wien
Strafregisteramt
DVR Nr. 0003506

10| Notification by the Delivery Service



Elektronische Zustellungsbenachrichtigung • zustellung@meinbrief.at • 13:51

Von zustellung@meinbrief.at
Betreff **Elektronische Zustellungsbenachrichtigung**
An Klaus Stranacher

Antworten | Weiterleiten | Archivieren | Junk | Löschen
13:51
Andere Aktionen

2013-09-27, 13:51:30

Verständigung über die Bereithaltung

eines behördlichen Dokuments zur Abholung

Absender	Bundespolizeidirektion Wien, Strafregisteramt	
Geschäftszahl	SRB2013092713350082	
Empfänger	Klaus Stranacher	
Zustellung	mit	Zustellnachweis

Das Dokument ist abzuholen bei Ihrem Zustelldienst unter https://www.meinbrief.at

Versendung der ersten elektronischen Verständigung: 2013-09-27, 13:51:30

Ende der Abholfrist am 2013-10-11 um 24:00h

SIGNATURINFORMATIONEN

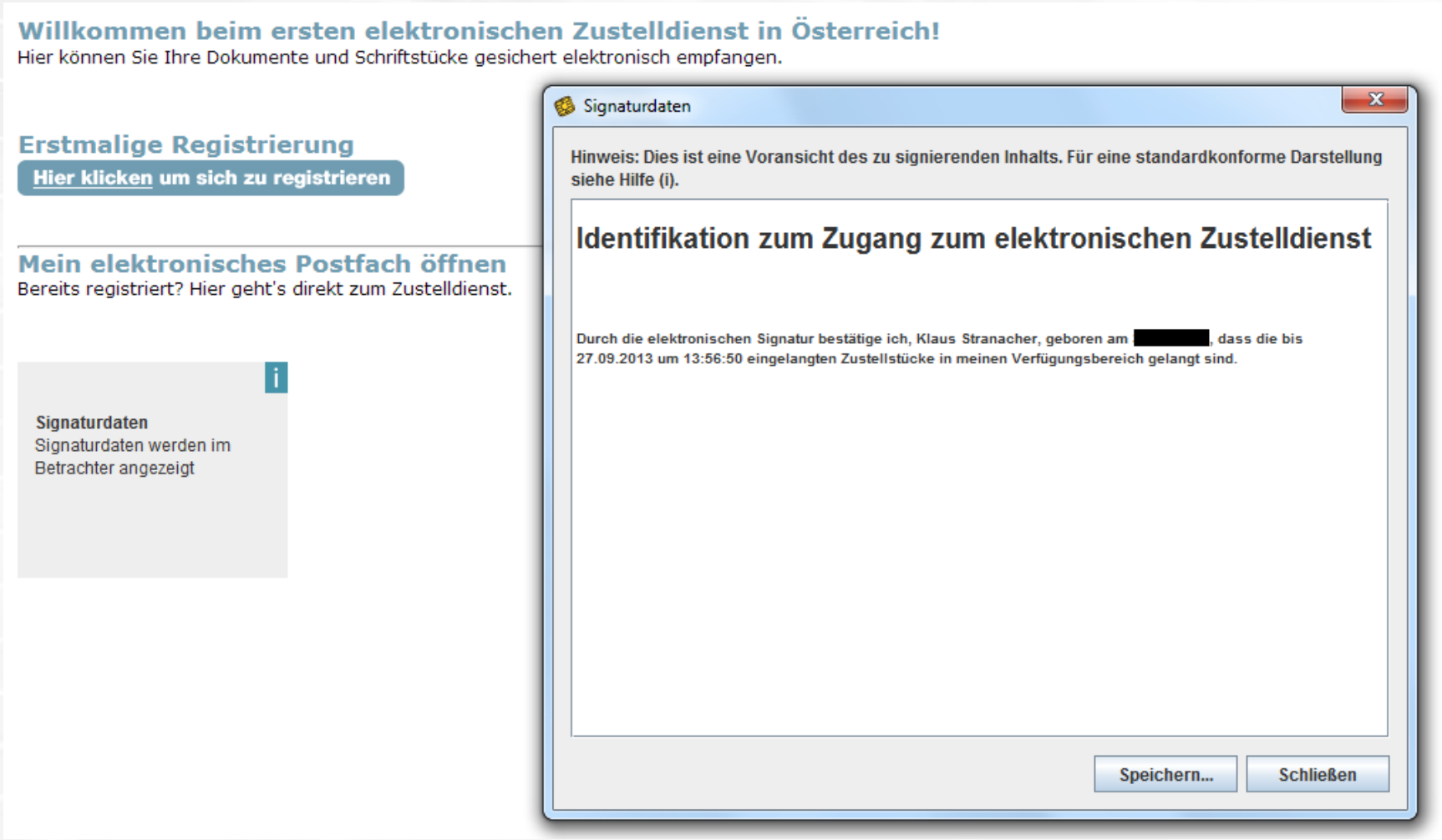
Datum	2013-09-27 13:51:30
Zertifikat	C=AT,O=Raiffeisen Informatik GmbH,CN=www.meinbrief.at,SERIALNUMBER=179637753254 Österreich
Signaturwert	XSRUgNBVDb1926gTq6KqFsAiyag/hL4CsSO9ijQ8XXLxdg1u9QosejWeOfAgvTD6 qi7NmX8wep5mbabzvghyfz+mb4toB77viTugUJhcTAdQrAYvfUj7lpsk/7dq5H4G lK2nge18UWRWRYLDa3oToF93YSypBfgsfOkhhyHS8VI=

Wichtige Information!

1. Eine zweite elektronische Verständigung wird nur dann versendet, wenn Sie das Dokument nicht innerhalb von 48 Stunden nach Versendung der ersten Verständigung abgeholt haben. Holen Sie das Dokument auch innerhalb der

11| Log into E-Delivery Service

12| Display and Signing of Login Data



13| Post-Office Box at meinbrief.at

Mein Brief.at

Das sichere elektronische Postfach.

Briefkasten **Papierkorb** **Abwesenheitsmeldung** **Einstellungen** **Logout**

Postfach von Klaus Stranacher

Status	Datum	Absender	Typ	Größe	Aktionen
	27.09.2013	§ Bundespolizeidirektion Wien, Strafregisteramt	RSa	270633 Byte	
	21.07.2012	§ Finanzamt Graz-Stadt	RSa	386039 Byte	
	21.07.2012	§ Finanzamt Graz-Stadt	RSa	74443 Byte	
	21.07.2012	§ Finanzamt Graz-Stadt	RSa	65395 Byte	
	21.10.2009	§ BMI IV/SU-ZMR	normal	31309 Byte	

14| Officially signed Criminal Record Certificate

Landespolizeidirektion Wien
Strafregisteramt

Wasagasse 22
1090 Wien

Zur Vorlage bei:
E-Government Innovationszentrum

Inffeldgasse 16a

8010 Graz

BEZUG: SRB2013092713350082 SB
(REFERENCE NUMBER)

S T R A F R E G I S T E R B E S C H E I N I G U N G
(C R I M I N A L R E C O R D C E R T I F I C A T E)

Familienname(n): (Family Name)	STRANACHER
Geschlecht: (Gender:	MAENNLICH MALE)
Vorname(n): (First Name)	KLAUS
Akad. Grad: (Academic Degree)	DIPL.-ING.
Geboren am: (Date of Birth:	[redacted] DD.MM.YYYY)
Geburtsort: (Place of Birth)	KLAGENFURT
Staatsang.: (Nationality)	Österreich

Im Strafregister der Republik Österreich - geführt von der Landespolizeidirektion Wien - scheint keine Verurteilung auf.

(No convictions are listed in the criminal records database of the Republic of Austria, kept by the Federal Police Directorate of Vienna.)

DVR: 0003506

Tagesdatum (Date): 27.09.2013
Uhrzeit (Time): 13.49.32

Signaturwert	U3ABlQ+4VFo4L/TWuyrtiHIN27mMPa4D618yBAJ3xXpjHhVmo7ynEslAzc36DVlfYAKByADHa6/fublEtylo oi/DGoI3p93T+Blr0tGnVc4AQIh+JSoo3VbqGK/eygtQgU4gOJzzVys6qMkEHTnhV1EJBqX11eKKiN3xR8qh PJghuv/KXJZxP/61XStHfD9ym/W6DpVg6Fwy9s2NTLsIqQ6UKk26t9VOXbaP1Hr5Uhh1KiNIMUt+Up7UGnos yOG6NxX81vPTBveWSAVYWZj1+IPe2OCXT4JrvnrE191eBP7IY4M6BPdRNpXpcSlYmabqAOJH+tkMCX+Y63PD k36jpw==	
	Datum/Zeit-UTC	2013-09-27T13:49:35+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	465297
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	etsi-bka-moa-1.0
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

Overview

- Electronic Signatures
- Legal Framework
- Signature Formats
- Official Signature
- Signature Verification
- Research
- Conclusion

Legal Framework

- European Framework given by the EU Signature Directive
  - Implementation of the directive by the national laws
  - Since 1. July 2016
    - eIDAS regulation
    - Signature act SVG (Signatur- und Vertrauensdienstegesetz)

- Different classes of signatures:
  - Electronic signature
  - Advanced electronic signature
  - Qualified electronic signature

Legal Framework

« Electronic Signature

eIDAS Regulation Article 3 (10) [eIDAS]:

'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

« Advanced Electronic Signature

eIDAS Regulation Article 26 [eIDAS]:

An advanced electronic signature shall meet the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Legal Framework

« Advanced Electronic Signature

eIDAS Regulation Article 26 [eIDAS]:

An advanced electronic signature shall meet the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

« Signature-creation data (e.g. private key) and the complementary signature-verification data (e.g. public key) must NOT occur more than once

Legal Framework

« Advanced Electronic Signature

eIDAS Regulation Article 26 [eIDAS]:

An advanced electronic signature shall meet the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

- « Practically impossible to create the same key pair twice
- « It is ensured that a signature, verified with a public key, can only have been created using the corresponding private key
- « Practically impossible that the private key is calculated or derived from the public key

Legal Framework

« Advanced Electronic Signature

eIDAS Regulation Article 26 [eIDAS]:

An advanced electronic signature shall meet the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

- « Creation by an authorized person only
- « Binding by possession and knowledge

Legal Framework

« Advanced Electronic Signature

eIDAS Regulation Article 26 [eIDAS]:

An advanced electronic signature shall meet the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

« It is practically impossible that

- « Different electronic data leads to the same hash value (collision resistance)
- « Any electronic data lead to a given hash value (preimage resistance)

Legal Framework

« Qualified Electronic signature

eIDAS Regulation Article 3 (12) [eIDAS]:

'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

« Legal Effects

eIDAS Regulation Article 25 [eIDAS]:

1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.
2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.
3. A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognized as a qualified electronic signature in all other Member States.

« Equivalent to handwritten signatures – except a few cases (e.g. family law)

Legal Framework

- Qualified Certificate (QC)
  - Must meet requirements according to eIDAS Regulation Annex I
  - Issued by the qualified trust service provider (QTSP)
  - List of Austrian QTSPs[1]
- Requirements for Qualified Certificates for Elektronic Signatures
  - Indication that the certificate is qualified
  - The unique name of the TSP and the country where it operates
  - The signatory's name
  - Signature validation data
  - Validity period of the certificate
  - Signature of the issuing qualified trust service provider

[1] https://www.signatur.rtr.at/en/vd/Anbieter.html

Legal Framework

- qualified trust service provider requirements according eIDAS Regulation
  - Necessary reliability
  - Directory and revocation service
  - Qualified time
  - Identification of the potential signatories
  - Reliable personnel
  - Appropriate financial means and third party insurance
  - Record keeping
  - Safety measures
  - Supervision by the supervisory authority (RTR-Rundfunk und Telekom Regulierungs-GmbH) [RTR]

Legal Framework

Secure Signature Creation Device (SSCD)

eIDAS Regulation Article 3 [eIDAS]:

(22) 'electronic signature creation device' means configured software or hardware used to create an electronic signature;
(23) 'qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II;

- SSCD shall create signatures using currently available technologies
- SSCD shall not alter signed data when creating the signature
- Applies to the processing of the signature creation data
  - Smart card and hardware security module (HSM)
- Compliance of the security requirements must be confirmed by the confirmation party (A-SIT)
  - http://www.a-sit.at/de/bestaetigungsstelle/bescheinigungen_sigg/veroeffentlichungen.php

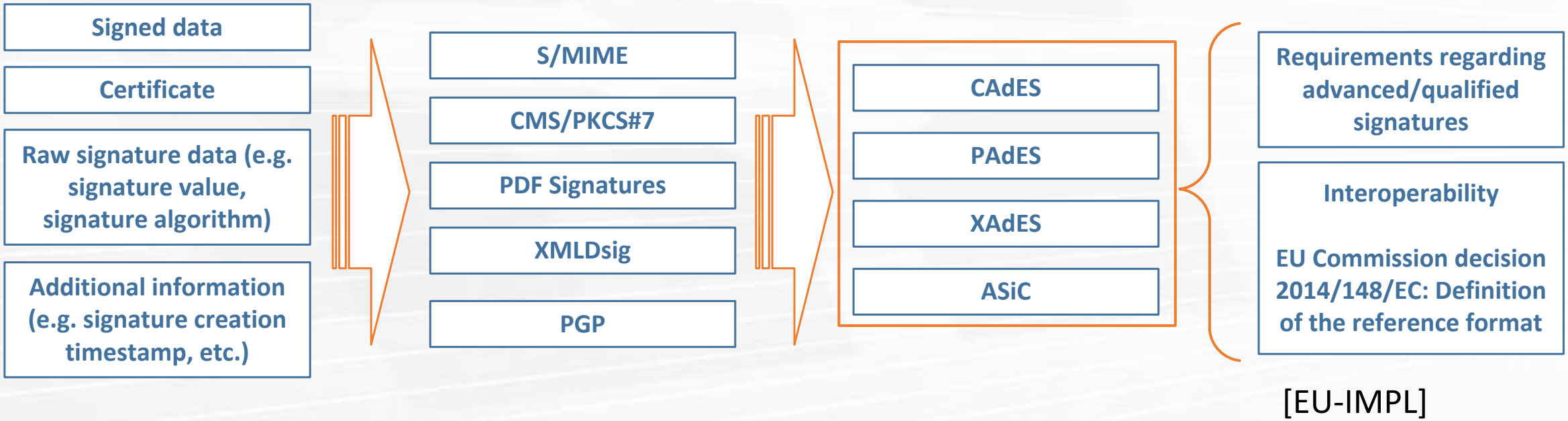
Control Questions

1. Explain an example E-Government process
2. List the features of electronic signatures
3. Explain the signature creation process

Overview

- Electronic Signatures
- Legal Framework
- Signature Formats
- Official Signature
- Signature Verification
- Research
- Conclusion

Signature Formats



[EU-IMPL]

- *AdES (Advanced Electronic Signature)
- ASiC (Associated Signature Container)

Signature Formats | XAdES

- XAdES (XML AdES) defines a standard for advanced XML signatures
- Specified by European Telecommunication Standards Institute (ETSI TS 103 171)
- Based on XMLDSig
- Suitable for advanced electronic signatures
  according to EU signature Directive
- http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf

Signature Formats | CAdES

- CAdES defines a standard for advanced CMS
- Specified by ETSI (ETSI TS 103 173)
- Based on Cryptographic Message Syntax (CMS)
- Suitable for advanced electronic signatures according to EU signature directive
- http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf

Signature Formats | PAdES

- PAdES defines a standard for advanced PDF signatures
- Specified by ETSI (ETSI TS 103 172)
- Based on CAdES
- Suitable for advanced electronic signatures according to EU signature Directive
- http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

Signature Formats | ASiC

- ASiC – Associated Signature Container
- Can hold a group of file objects and their associated signatures
- Structure:
  - Root folder: contains the file objects
  - META-INF folder: contains the metadata such as the associated signatures or time assertion files
- Based on CAdES or XAdES
- Specified by ETSI (ETSI TS 103 174)
- Suitable for advanced electronic signatures according to EU signature Directive
- http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

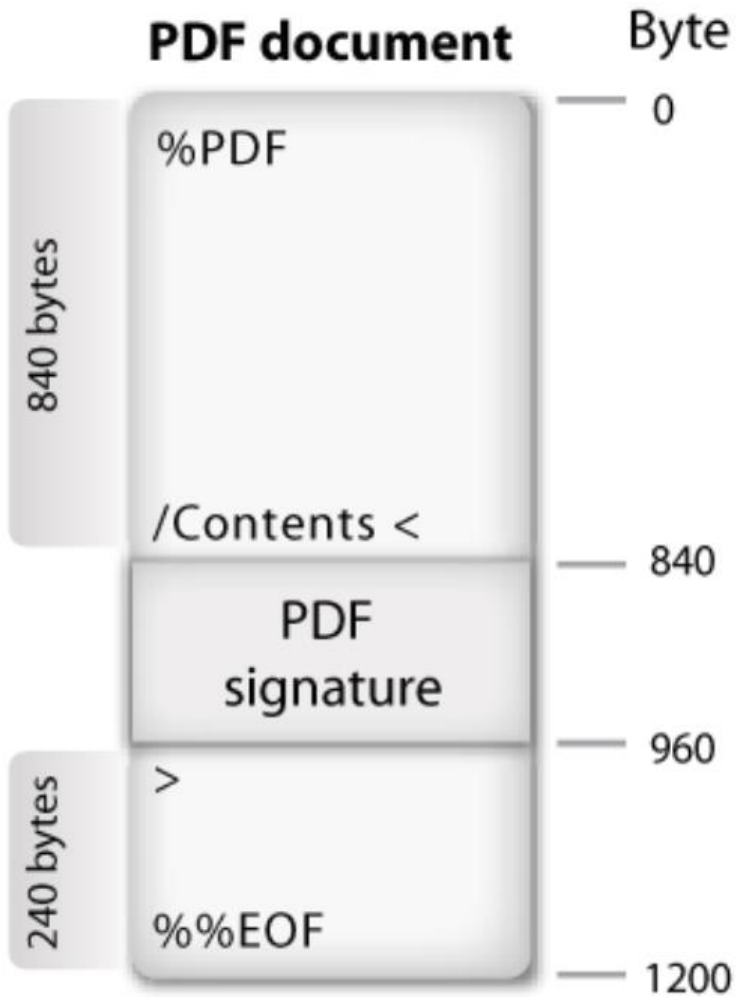
Signature Formats | PAdES types

- PAdES-BES (Basic Electronic Signature)
  - PAdES Basic Profile based on ISO 32000-1
- PAdES-EPES (Explicit Policy based Electronic Signature)
  - Additionally: Declaration of a signature policy
- PAdES-LTV (Long Term Validation Profile)
  - Used for long term validation
- PAdES for XML Content
  - Used for PDFs with XML content

Signature Formats | PAdES Example

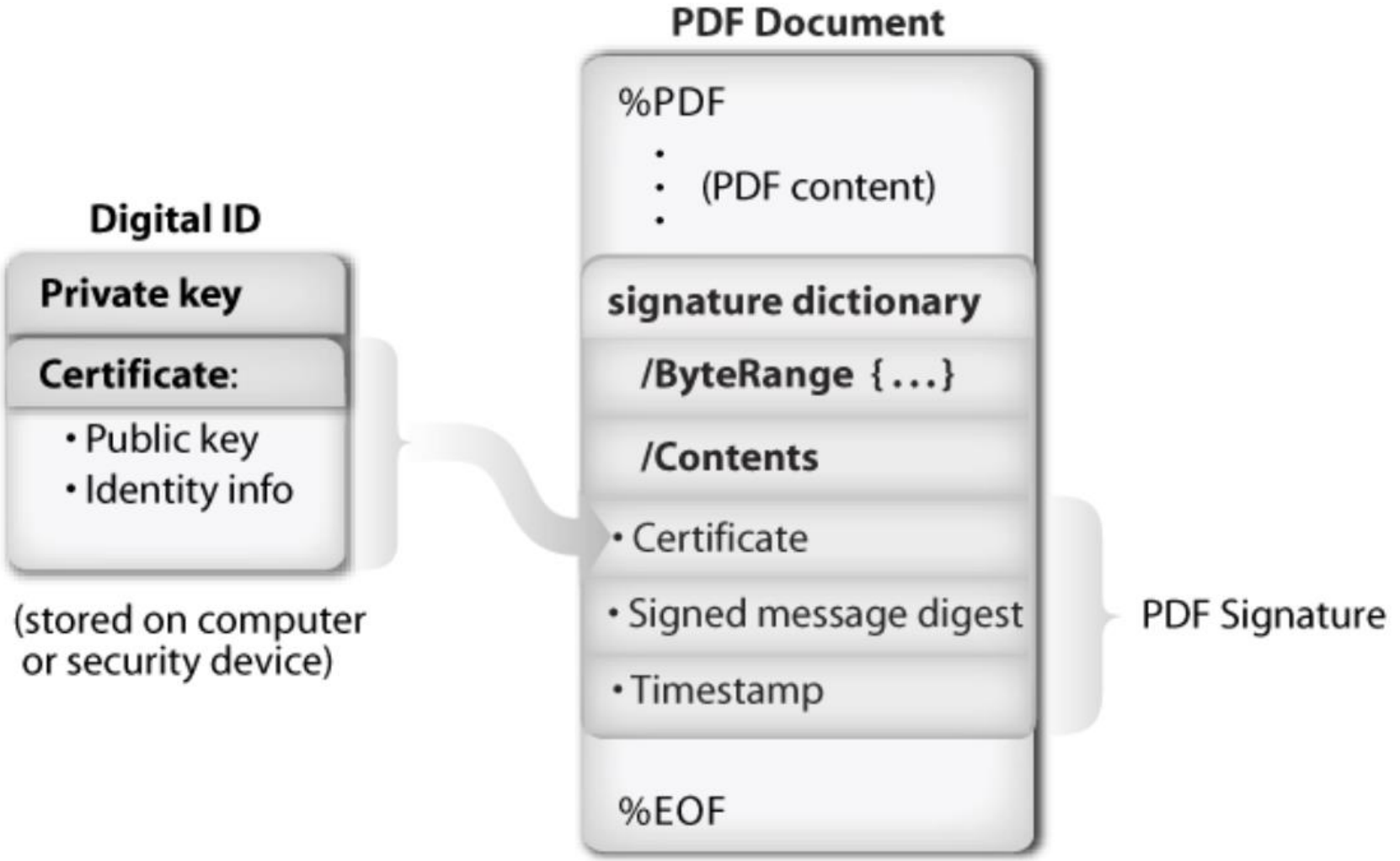
- Example: PAdES signature
- Signature block is included in the signed data
- Actual signature value is **not** included in the signed data
- Byte Range shows the signed content

Example:



Signature Formats | PAdES Example

- Actual signature content within the PDF document
- Byte Range used for signature validation



Signature Formats | PAdES Example

```
63 0 obj
<<
/Type /Sig
/Filter /Adobe.PPKLite
/SubFilter /ETSI.CAdES.detached
/Name (Andreas Abraham)
/M (D:20160225100113+01'00')
/Reason (Signaturpruefung unter http://www.signaturpruefung.gv.at)
/Contents
<3082077106092A864886F70D010702A08207623082075E020101310F300D06096086480165030402010500300B06092A864886F70D01070
0202030EFB9D300D06092A864886F70D0101050500308 19D310B3009060355040613024154314830460603550 40A0C3F412D547275737420
97473737974656D6520696D20656C656000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000>
/ByteRange [0 116539 124733 21637]
>>
endobj
```

Signature Formats | Available Tools

- Citizen card environment (CCE): Signature creation utilizing the citizen card
- MOA-SPSS: Modules for (server-side) signature creation and verification: https://www.egiz.gv.at/en/schwerpunkte/13-moaspssid
- PDF-Over: Client application for creation of PAdES signatures using the mobile phone signature (Handysignatur)
- Prime Sign: Web application - https://www.prime-sign.com
- Online signature verification: https://pruefung.signatur.rtr.at
- Online signature creation and verification: http://www.buergerkarte.at

Overview

- Electronic Signatures
- Legal Framework
- Signature Formats
- Official Signature
- Signature Verification
- Research
- Conclusion

Official Signature (Amtssignatur)

« Official Documents

BPOLDION WIEN STRAFREGISTERAMT

WASAG.22
1090 WIEN

BEZUG: III-STRB-384-STRA/2005 (ANFRNR. 0002604) SB

STRAFREGISTERBESCHEINIGUNG

Familienname(n): LEITOLD
Geschlecht: MAENNLICH
Vorname(n): HERBERT
Akad. Grad: DI
Geboren am: [redacted]
Geburtsort: GRAZ STMK

Im Strafregister der Republik Österreich - geführt von der Bundespolizeidirektion Wien - scheint keine Verurteilung auf.

DVR: 0003506

Tagesdatum 23.09.2005
Uhrzeit 13.24.24

Gebühr entrichtet

How to recognize a document issued by a public authority ?

↓

Invention of the official signature

↙ ↘

Recognition of origin

Authenticity

Official Signature

- E-Government law defines the official signature to identify a document's origin
- Official signature is used for electronically signing issued documents
- The official signature is, except from the requirement to be an advanced electronic signature, more a regulation of the look rather than a technical requirement.

Signaturwert	KTyBXLlDjH4jtEWpzcI2xqHwZZXAVRCFWRl7vycFo+EDGu0bJLr3nmBWxAnGc4UC	
MARKTGEMEINDE KREMSMÜNSTER AMTSSIGNATUR	Unterzeichner	Franz Fellinger, Bürgermeister
	Datum/Zeit-UTC	2008-05-08T10:05:10Z
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	238730
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1210241110-14617390@734-26815-0-11788-24523
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur und zur Prüfung des Ausdrucks finden Sie unter: https://www.buergerkarte.at/signature-verification/	
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	

Official Signature

- Properties of the official signature
  - Figurative mark or logo
    - Obligation to publish the mark/logo securely
  - Hint that a document has been officially signed
    - On arbitrary position within the document
    - Signature certificate with administrative character

      (Signatory has to be an administrative authority)
  - Signature verification information

Official Signature

Landespolizeidirektion Wien
Strafregisteramt

Wasagasse 22
1090 Wien

Zur Vorlage bei:
E-Government Innovationszentrum

Inffeldgasse 16a

BEZUG: SRB2013092713350082 SB
(REFERENCE NUMBER)

S T R A F R E G I S T E R B E S C H E I N
(C R I M I N A L R E C O R D C E R T I F

Familienname(n): STRANACHER
(Family Name)

Geschlecht: MAENNLICH
(Gender: MALE)

Vorname(n): KLAUS
(First Name)

Akad. Grad: DIPL.-ING.
(Academic Degree)

Geboren am: [redacted]
(Date of Birth: DD.MM.YYYY)

Geburtsort: KLAGENFURT
(Place of Birth)

Staatsang.: Österreich
(Nationality)

Im Strafregister der Republik Österreich - geführt von
Landespolizeidirektion Wien - scheint keine Verurteilun

(No convictions are listed in the criminal records data
Republic of Austria, kept by the Federal Police Directo

DVR: 0003506

Tagesdatum (Date): 27.09.2013
Uhrzeit (Time): 13.49.32

Signaturwert	U3ABlQ+4VPo4L/TWuyrt1HIN27mMPa4D618yBAJ3xXpjHhVmo7ynEs1Azc36DV1fYAKByADHa6/fub1Etylo o1/DGoI3p93T+B1r0tGnVc4AQIh+JSoo3VbqGK/eygtQgU4gOJzzVys6qMkEBTnhV1EJBqX11eKk1N3xR8qh PJghuv/KXJZxP/61XStHfb9ym/W6DpVg6Pwy9s2NTLsIqQ6UKk26t9VOXbaP1Hr5Uhh1K1NIMUt+Up7UGnos yOG6NxX81vPTBveWSAVYWZj1+IPe2OCXT4JrvnrE191eBP7IY4M6BPdRNpXpcS1YmabqAOJH+tkMCX+Y63PD k36jpw==	
	Datum/Zeit-UTC	2013-09-27T13:49:35+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	465297
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	etsi-bka-moa-1.0
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

Signaturwert	U3ABlQ+4VPo4L/TWuyrt1HIN27mMPa4D618yBAJ3xXpjHhVmo7ynEs1 o1/DGoI3p93T+B1r0tGnVc4AQIh+JSoo3VbqGK/eygtQgU4gOJzzVys PJghuv/KXJZxP/61XStHfb9ym/W6DpVg6Pwy9s2NTLsIqQ6UKk26t9V yOG6NxX81vPTBveWSAVYWZj1+IPe2OCXT4JrvnrE191eBP7IY4M6BPd k36jpw==	
	Datum/Zeit-UTC	2013-09-27T13:49:35+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	465297
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	etsi-bka-moa-1.0
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

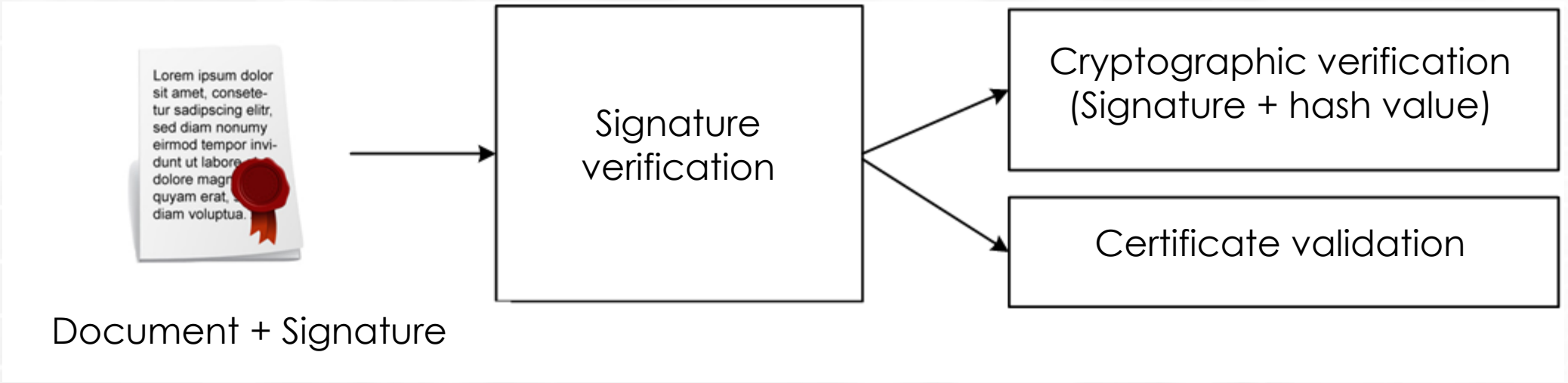
Control Questions

1. Explain the properties of the official signature
2. Explain the legal effects of a qualified electronic signature
3. Explain a signature format that can be used to sign a PDF document

Overview

- Electronic Signatures
- Legal Framework
- Signature Formats
- Official Signature
- Signature Verification
- Research
- Conclusion

Signature Verification



Signature Verification | Cryptographic verification

- Comparison of the hash value
  - message not modified
- Check of the signature value
  - ensure the signatory's authenticity
  - Check if the public key (from the certificate) matches private key the document was signed with
- What information is missing?
  - Validity?
  - Revocation? – e.g. private key is compromised, etc.

Signature Verification | Certificate verification

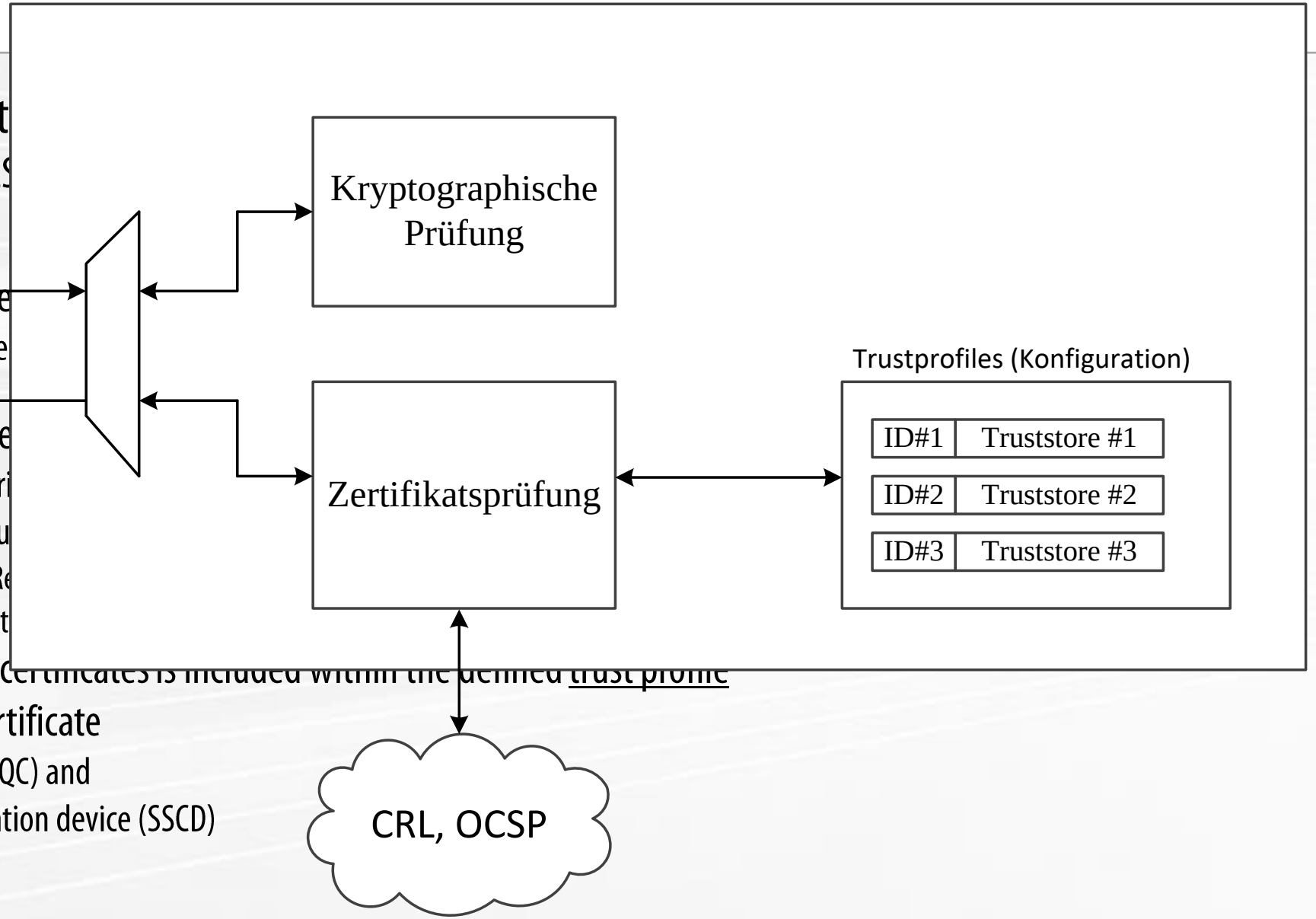
- X.509 Certificate

- Validity period
- Quality of the authenticity (via certification authority or qualified certificate)
- Key usage
- Revocation check

Signature Verificat

MOA-SP

- Cryptographic verificat
  - As specified (e.g. PAdE
- VerifySignatureRequest
  - (1) Build the certificate
- VerifySignatureResponse
  - (2) For every certificate
    - Verify the validity peri
    - Verify for revocation u
      - CRL: Certificate Re
      - OCSP: Online Cert
  - (3) Verify if one of the certificates is included within the defined trust profile
  - (4) Verify signatory certificate
    - Qualified certificate (QC) and
    - Secure signature creation device (SSCD)

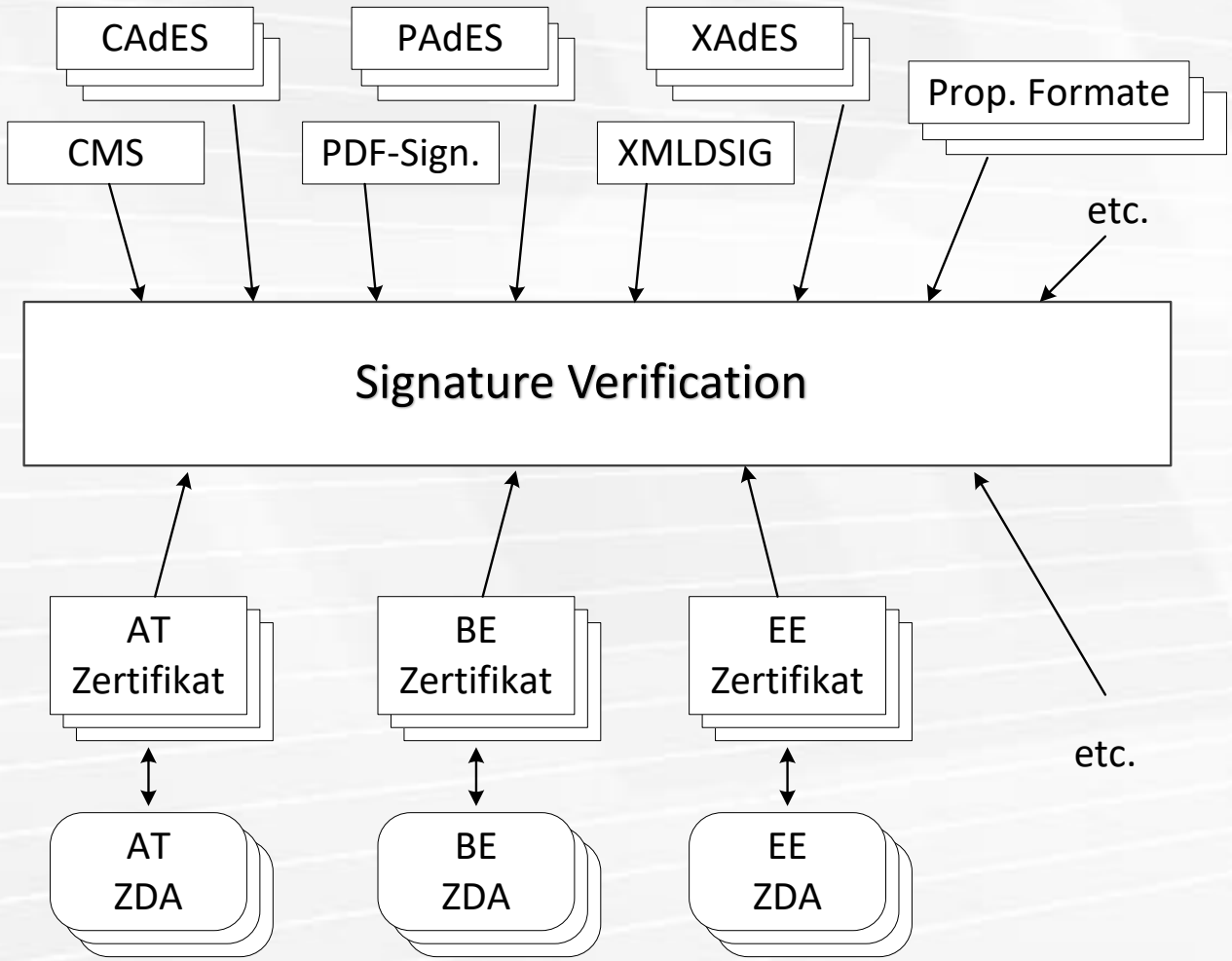


Signature Verification

- On EU level
  - Target: Growing together of the EU Member States,

    Free and easy movement of citizens and businesses
  - Acceptance of both electronic identity and documents play a vital role
  - → Signature verification on EU level!
  - EU Services Directive
  - eIDAS Regulation

Signature Verification



- Signature formats
  - Different signature formats (also proprietary)
  - Complex format specifications → interpreted differently
- QC/SSCD Check
  - How to identify the qualification of a foreign trust service provider?

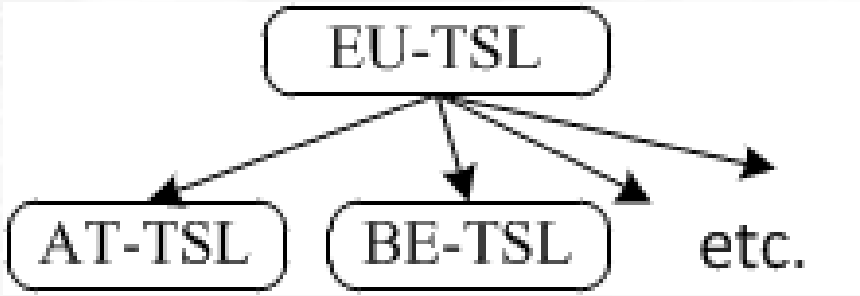
Signature Verification

Signature Formats

- EU Commission Decision 2014/148/EU
- Definition of reference formats with exactly defined content
  - CAdES BES/EPES
  - XAdES BES/EPES
  - PAdES BES/EPES
  - ASiC
- When using a proprietary format, an online signature validation mechanism must be provided.

Signature Verification

- QC/SSCD Check
  - Basis: EU Commission Decision 2009/767/EC
  - Every member state must provide a trustworthy list containing the trust service providers that are allowed to issue qualified certificates
  - Implementation: Trust-Service Status List (TSL)
  - EU TSL refers to national TSLs



Signature Verification

Trust-Service Status List

- ETSI Standard (TS 102 231)
- TSL provides a structured representation (XML) regarding status information about the Trust Service Providers (TSP)
- Logical Structure
  - General information regarding the TSL
  - Information regarding the TSP and the services it provides
  - For every service:
    - Information regarding the current status (under supervision, accredited, accreditation rejected, etc.), the appropriate certificate corresponding to the service and the support of QC/SSCD.
    - Historical status information

Overview

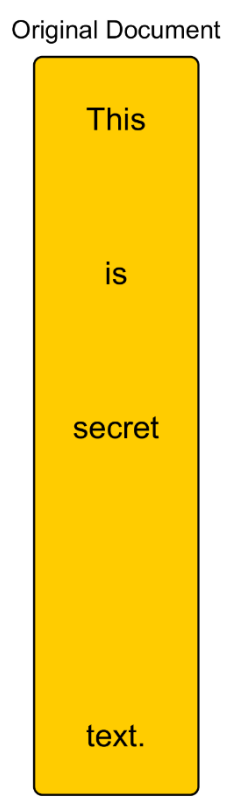
- Electronic Signatures
- Legal Framework
- Signature Formats
- Official Signature
- Signature Verification
- Research
- Conclusion

Research

- Malleable Signatures
  - Redactable Signatures
    - Selective disclosure
  - Blank Digital Signatures
    - Define document templates
  - Sanitizable Signatures
    - Selective sanitizable parts
- Privacy-Preserving Signatures
  - Blind Signatures
  - Group Signatures

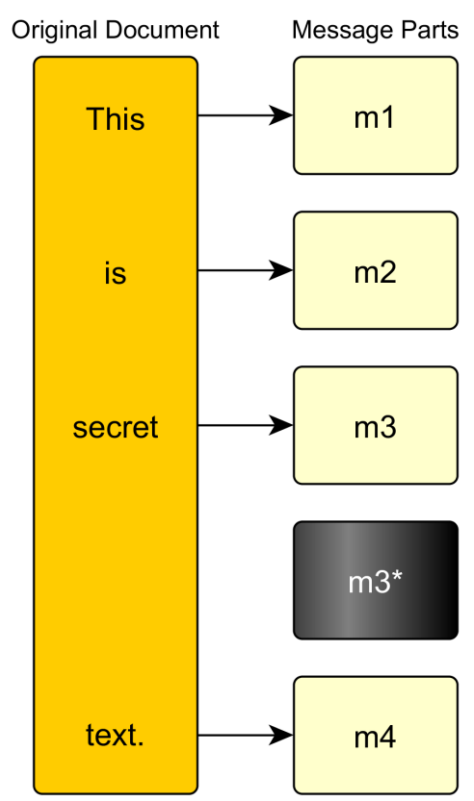
Research

« Redactable Signatures



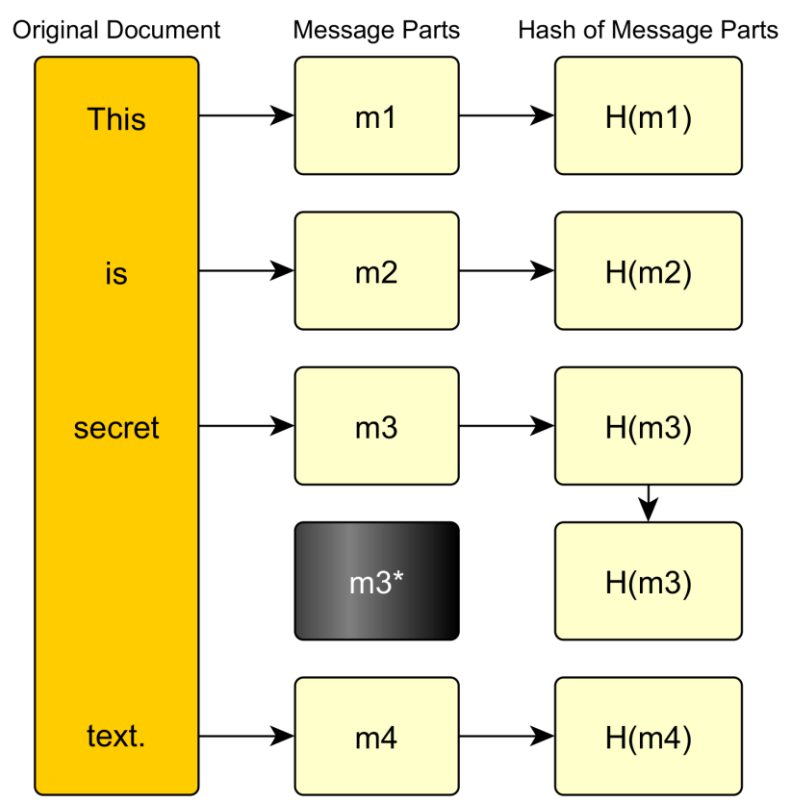
Research

« Redactable Signatures



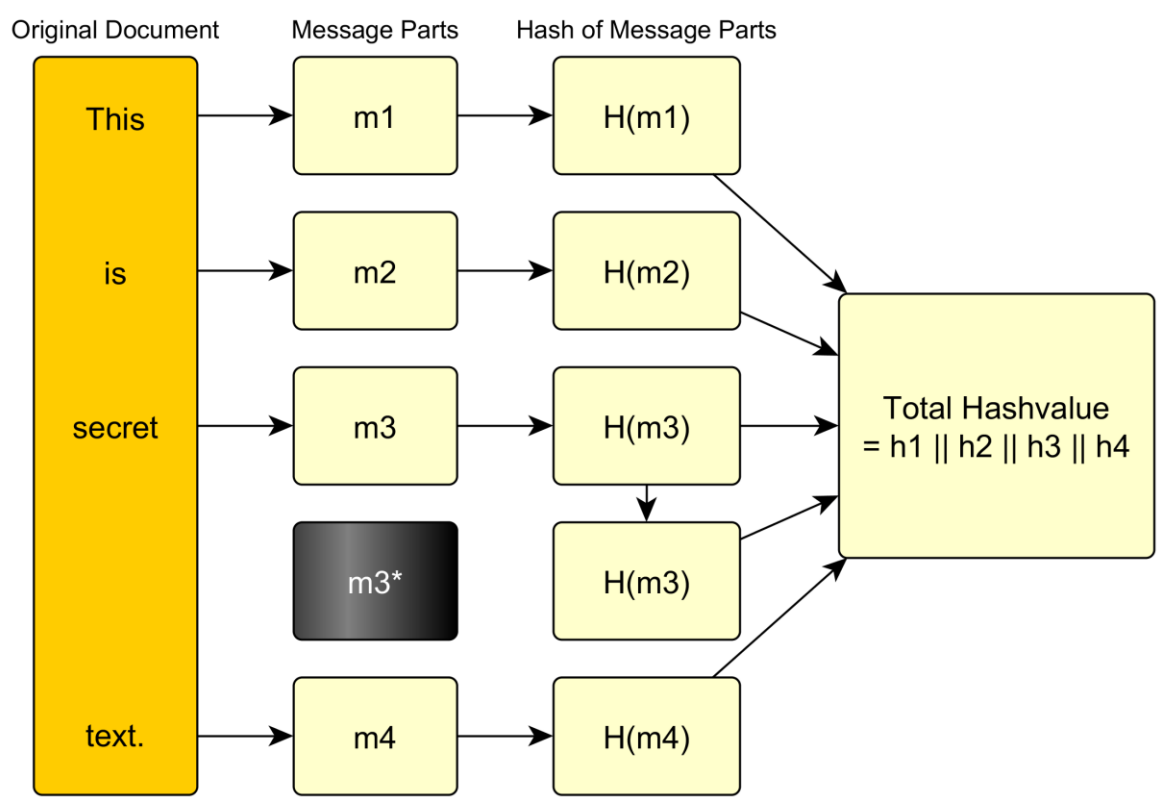
Research

« Redactable Signatures



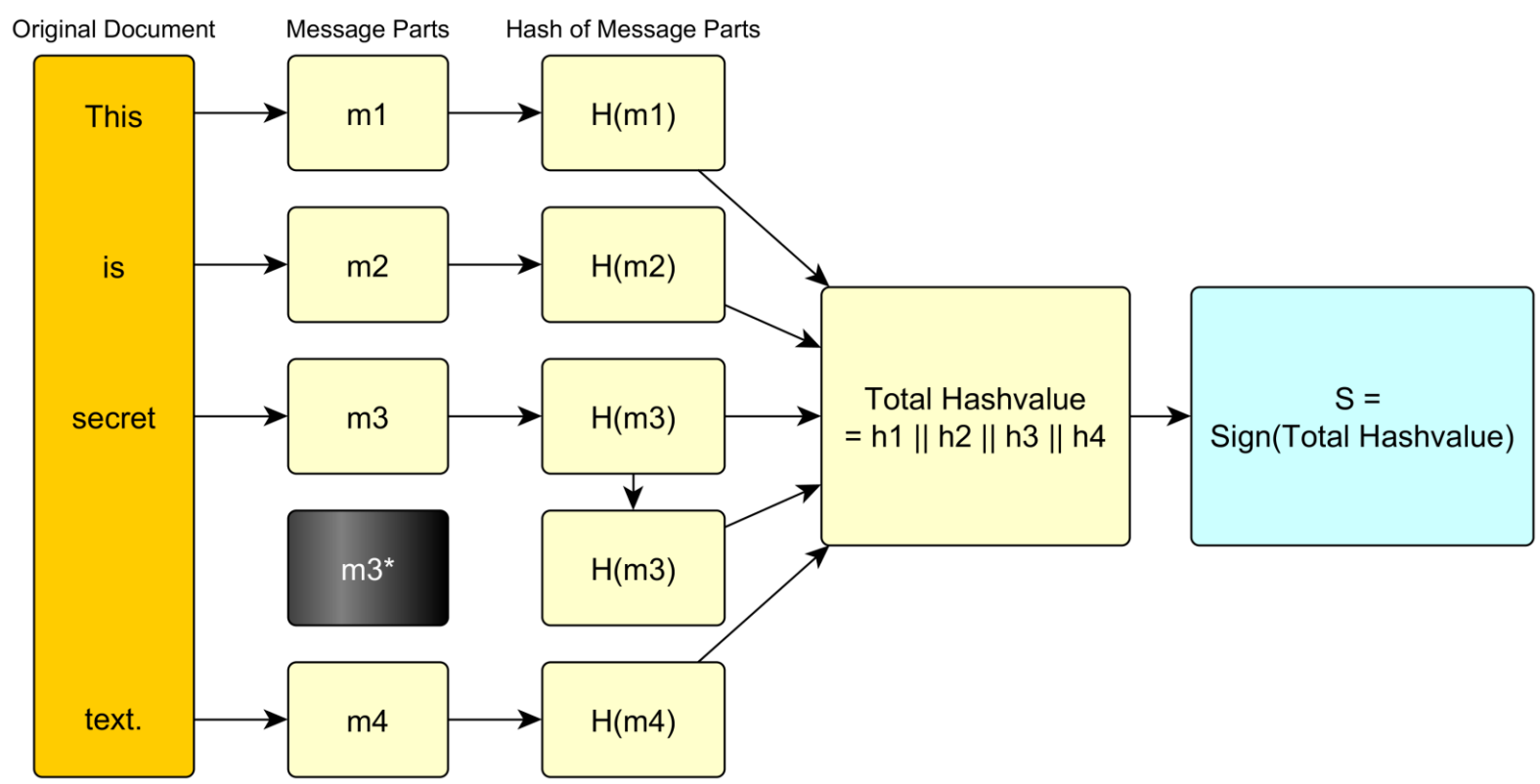
Research

« Redactable Signatures

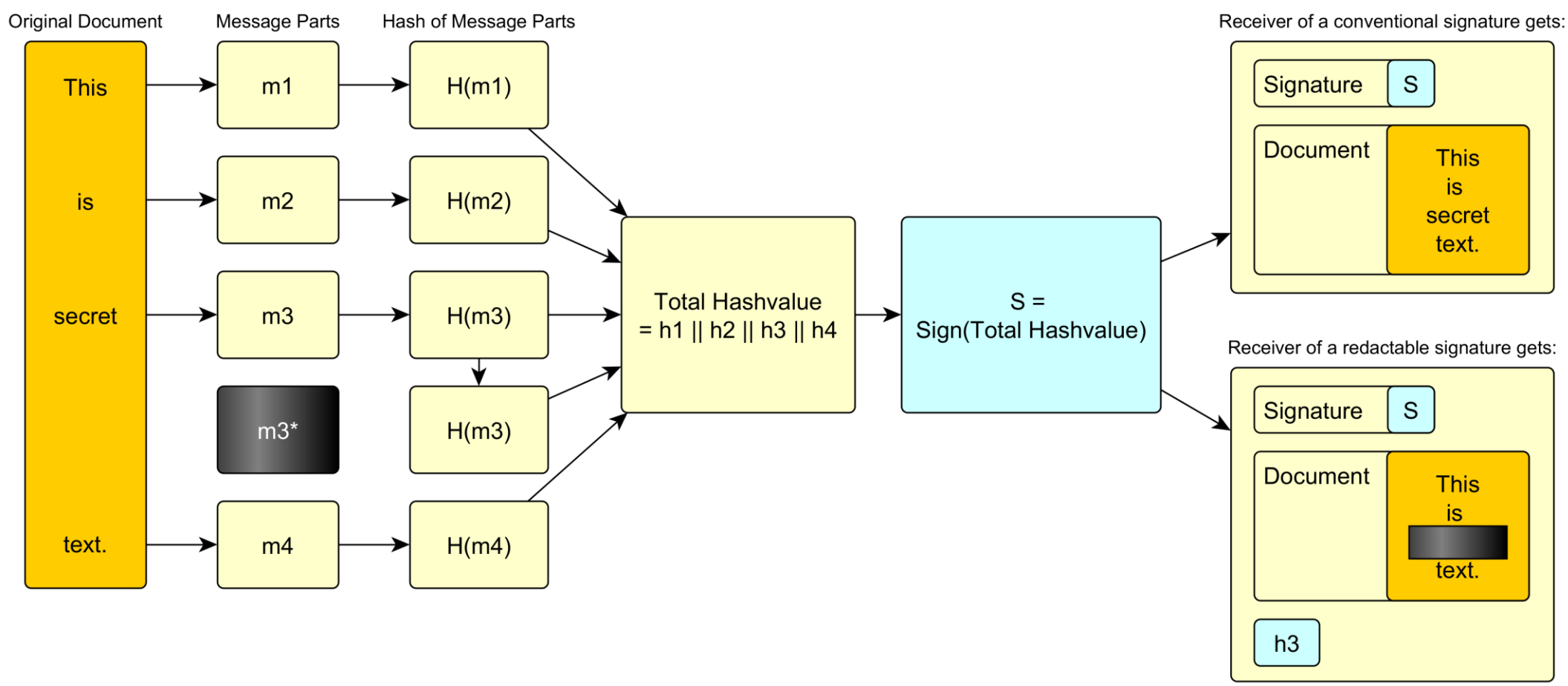


Research

« Redactable Signatures

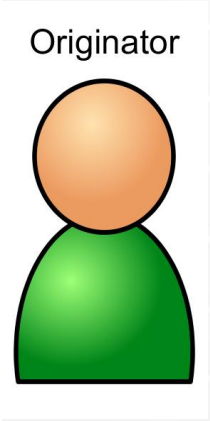


« Redactable Signatures



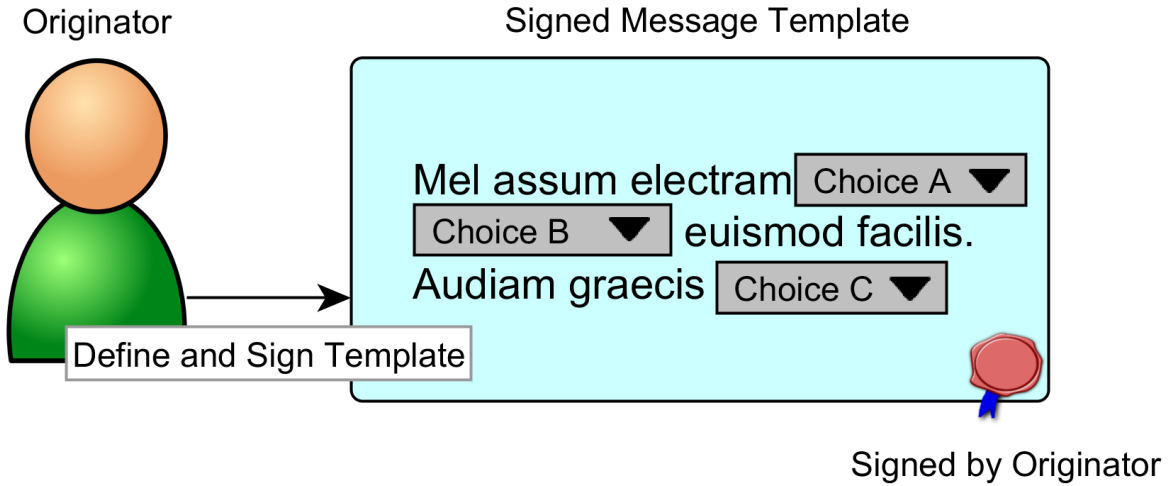
Research

« Blank Digital Signatures



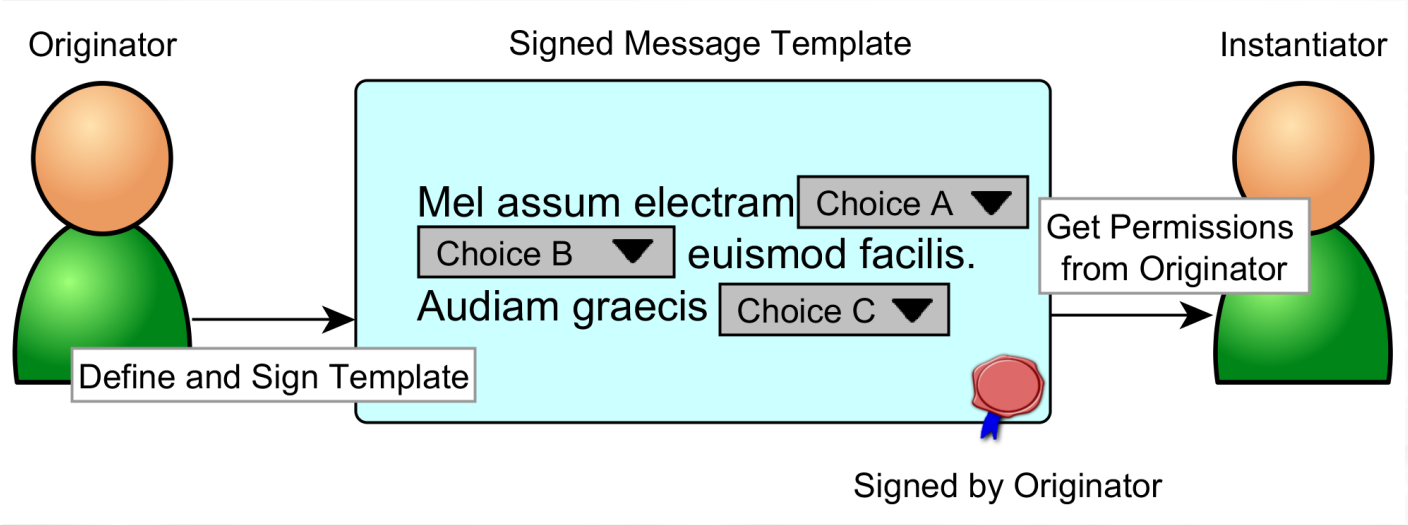
Research

« Blank Digital Signatures



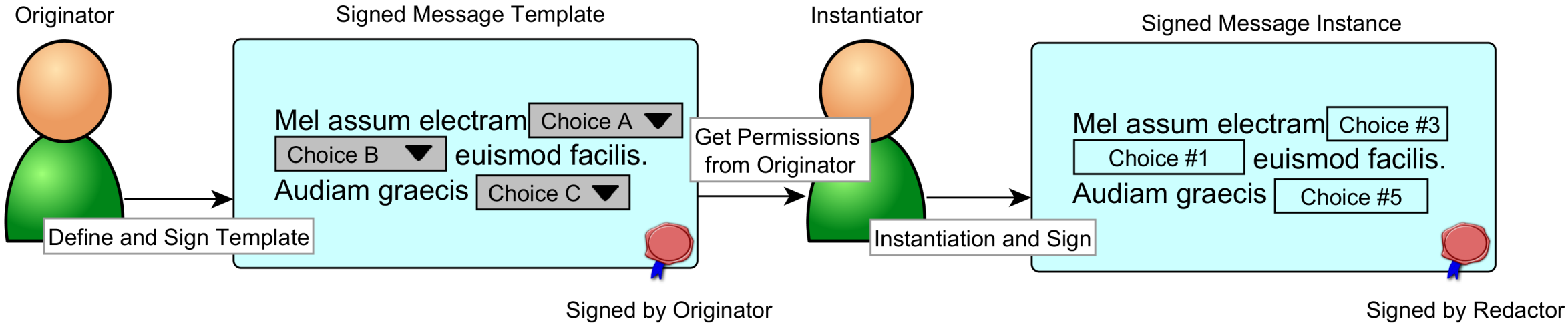
Research

« Blank Digital Signatures



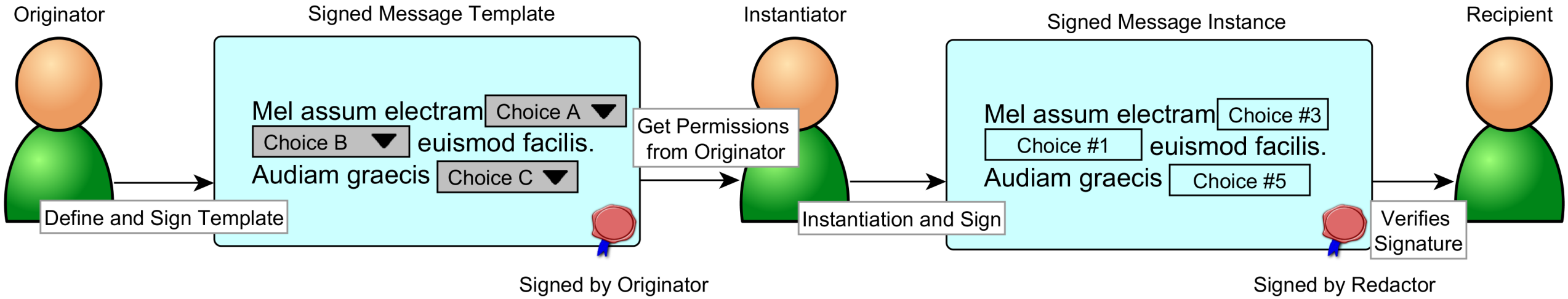
Research

« Blank Digital Signatures



Research

« Blank Digital Signatures

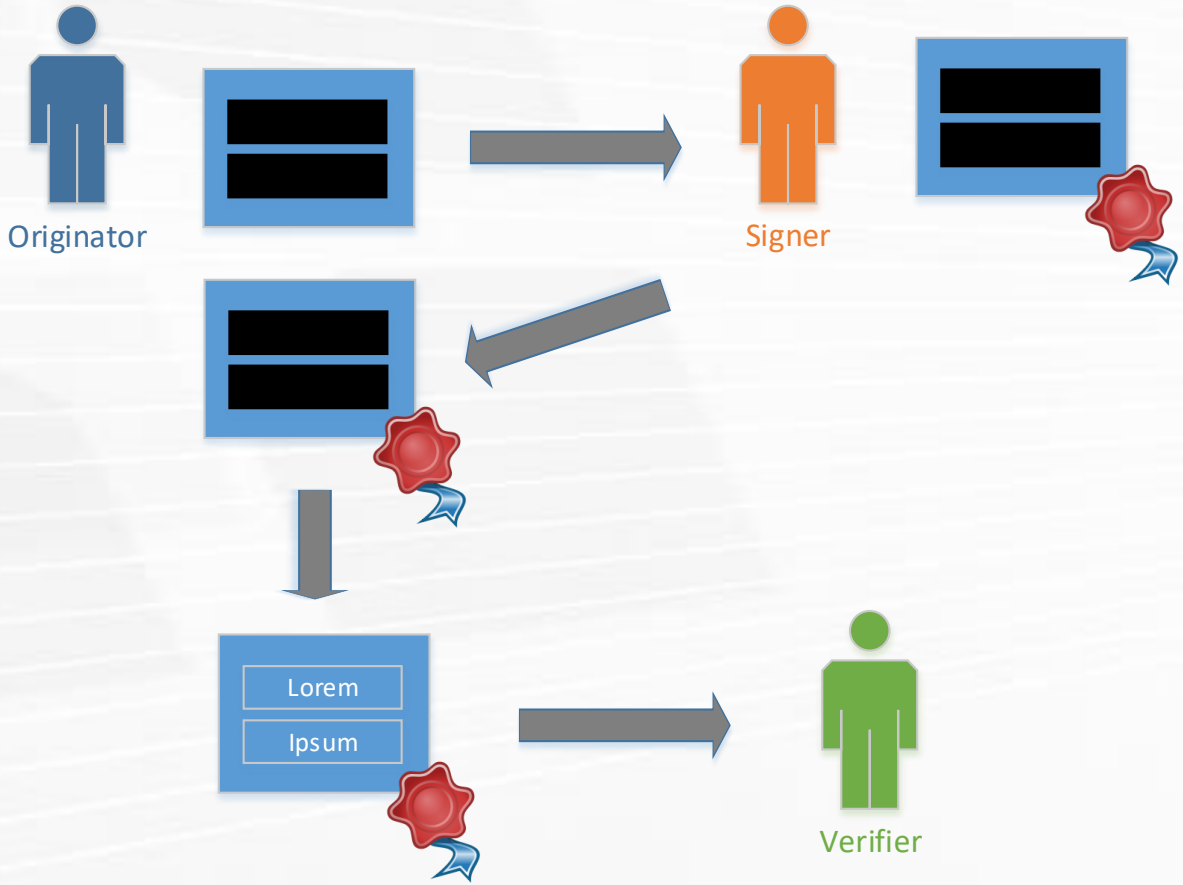


Research

- Sanitizable Signatures
  - Originator signs message with predefined sanitizable parts
  - Desegnated parties can perform sanitize operation
    - Using the sanitize key
  - Based on Chameleon Hash
  - Judge operation to determine if message was sanitized
  - Can be used to redact information
    - Only by holder of the sanitize key
  - The modifications of the sanitizable parts can be predefined

Research – Privacy Preserving Signatures

- Blind Signatures
  - Originator creates blinded message
  - Signer signs the blinded message
  - Originator unblinds the message
  - Receiver verifies the signature



Research – Privacy Preserving Signatures

- Group Signatures
  - A designated party (group manager/master) provides the keys to members of the group
  - The members use the signing key to create a signature
  - Preserves privacy of the signers
  - In some schemes
    - An authorized party has an open key
    - Open key used to reveal singers identity

Control Questions

1. Explain the signature verifiction process
2. Explain the problems and solutions for cross-border signature verification on EU level
3. Explain TSL and how it is used in the electronic signature verification process
4. Explain the basic priniciple of redactable signatures and where such scheme can be used

Overview

- Electronic Signatures
- Legal Framework
- Signature Formats
- Official Signature
- Signature Verification
- Research
- Conclusion

Conclusion

- Use of advanced and qualified signatures in E-Government processes
- Legal framework
- Signature formats (CAdES, XAdES, PAdES, etc.)
- Signature tools
- Official signature (Amtssignatur)
- Signature validation
  - International: Problems + Solutions
- Research: Malleable Signatures and Privacy-Preserving Signatures

References

[clarke] http://www.rogerclarke.com/DV/HumanID.html

[DiAut] Digital Austria https://www.digitales.oesterreich.gv.at/

[EGIZ] eGovernment Innovation Centre (EGIZ) https://www.egiz.gv.at/en

[EU-IM] European Union: Commission Implementing Decision (EU) 2015/1506 http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015D1506&from=EN#ntr2-L_2015235EN.01004101-E0002

[eIDAS] eIDAS Regulation http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

[help] https://www.help.gv.at/

[RTR] Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) https://www.rtr.at/