AK IT Security 1 (E-Government)
Electronic Signatures

Klaus Stranacher
Overview
Overview

- Electronic Signatures
- Legal Framework
- Signature Formats
- Official Signature
- Signature Verification
- Conclusions
Why do we need Signatures?

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

- **Authenticity of originator and data**
  - Mapping data to signatory
  - Protection against repudiation by the signatory
  - Protection against data manipulation
    - On the channel
    - By the recipient
Basis 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 security
    - Quality of the authenticity depends on this identification
    - Issuing and identification by the certification service provider (CSP)
Basis Principle

- **Signature Creation**
  - Creating the document
  - Calculating the hash value
  - Signing hash value with private key
  - Distribution of the signed message (including the public key/certificate)
Basis Principle

**Signature Verification**

- The hash value is **again calculated** from the received document
- The signature is verified using the signatory’s **public key** and the **original hash value** is revealed
- Comparing the original hash value with the calculated one
- 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 and E-Government

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

Identification and authentication
Signed documents
Signed request
Officially signed administrative decision

Portal
Backoffice
Elektronische Zustellung

Dokumente
Bürger/in
Example: Criminal Record Certificate

1. Login to fill in a form
2. Sign the request
3. Pay using ePayment
4. Back office processing (ELAK)
5. Electronic delivery

www.help.gv.at
www.elak.gv.at
www.meinbrief.at
Forwarding to the police department
Login using the Citizen Card

BM.I

BUNDESMinisterium für INNeres

Wenn Sie in Folge die Schaltfläche "Anmeldung mit Bürgerkarte" aktivieren, werden Sie zur Signatur Ihrer Anmeldedaten aufgefordert. Wenn Sie diese personalisierten Anmeldedaten signieren, werden Sie am Portal angemeldet.

Anmeldung mit Bürgerkarte

Weitere Informationen zur Überprüfung der Zertifikate.

Bundesministerium für Inneres - Stammportal
Displaying and Signing the Login Data
Antrag auf Ausstellung einer Strafregisterbescheinigung

Abender/in

Akad. Grad: Dok.-lng
Familienname: Stroacher
Vorname: Hepp
E-Mail Adresse:

Zur Anfrage im Register benötigte Personenmerkmale

Geschlecht: männlich
Folger Familienname:
Weitere frühere Familienname:
Geburtsdatum:
Geburtsort:
Vorname des Vaters:
Vorname der Mutter:

Verwendungsort

Zur Verfügung ausschließlich bei der post auszustellen an z.B. Behörden, Versicherung, Bank, Unternehmen, Vereine, um Antragsteller verschiedener natürlicher Personen etc. (Gefahr EUR 14.42)

Name:
Straße Hausnr:
PLZ Ortsschaft:
Staat:

Art der Zustellung

Elektronische Zustellung

Ich bin bei einem elektronischen Zustellungsersteller registriert und ersuche nach Möglichkeit um Zustellung der diese (Strafregisterbescheinigungen können d.h. dann elektronisch zugestellt werden.

Datentechnik

INNOVATION
Art der Zustellung

Ich bin bei einem elektronischen Zwillingservice registriert und erachte 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 (kombinationellen) Weg die Strafregisterbescheinigung zugestellt werden soll.

Brief-Qualität
- Normal-Brief
- RSa-Brief

Auswahl der Zustelladresse (Hauptwohnzit laut ZMR ODER andere Adresse)
- Hauptwohnzit laut ZMR
- andere Adresse

Postale Zustelladresse (Hauptwohnzit laut ZMR)
- Straße
- Hausnummer
- Stiege
- Tür
- Postleitzahl
- Ort
- Staat

Antrag signieren
Signing Request using Citizen Card

Unterschrift mit Bürgerkarte

Wählen Sie die Bürgerkartenumgebung aus, mit der Sie unterschreiben wollen.
Displaying and Signing the Request

Antrag auf Ausstellung einer Strafregisterbescheinigung

Absender/in
- Akad. Grad
- Familienname
- Vorname
- E-Mail Adresse

Dipl.-Ing.
Stranacher
Klaus

Zur Anfrage im Register benötigte Personenmerkmale
- Geschlecht: männlich
- Frühere Familienamen

Weitere frühere Familienamen
- Geburtsdatum
- Geburtsort
- Vorname des Vaters
  "unbekannt" eintragen, falls Name nicht bekannt
- Vornamen der Mutter
  "unbekannt" eintragen, falls Name nicht bekannt
Payment using EPS
Antrag wurde angenommen.

Von LPD-W-SVA-FB-Strafregisteramt@polizei.gv.at 13:43
Betreff Antrag wurde angenommen.
An  Klaus Stranacher

Sehr geehrter Herr Dipl.-Ing. Klaus Stranacher!

Ihr Antrag mit der Nummer SRB20130927133500082 wurde registriert.

Sollten Sie Fragen zu Ihrem Antrag haben, wenden Sie sich bitte an die Landespolizeidirektion Wien, Strafregisteramt e-Mail (LPD-W-SVA-FB-Strafregisteramt@polizei.gv.at) bzw. telefonisch unter 01/33310/79231 (Mo-Fr 07:30 - 15:30).

Ihre Landespolizeidirektion Wien
Strafregisteramt
DVR Nr. 8003586
Notification by the Delivery Service

Verständigung über die Bereithaltung
eines behördlichen Dokuments zur Abholung

Absender: Bundespolizeidirektion Wien, Strafregisteramt
Geschäftszahl: SRR2013092713350082
Empfänger: Klaus Stranacher
Zustellung: mit Zustellnachweis

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


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

Wichtige Information!
1. Eine zweite elektronische Verständigung wird nur dann versendet, wenn Sie das Dokument nicht innerhalb von 48 Stunden nach Versendung der ersten Verständigungsabholung haben. Holen Sie das Dokument auch innerhalb der
Login at the E-Delivery Service

Mein Brief.at
Das sichere elektronische Postfach.

Willkommen beim ersten elektronischen Zustelldienst in Österreich!
Hier können Sie Ihre Dokumente und Schriftdstücke gesichert elektronisch empfangen.

Erstmalige Registrierung
Hier klicken um sich zu registrieren

Mein elektronisches Postfach öffnen
Bereits registriert? Hier geht's direkt zum Zustelldienst.

Ich möchte mich mit meiner Vollmacht anmelden

Mobile BKU
Einfacher Einstieg mit mobiler Signatur!

Online BKU
Einfacher Einstieg ohne Bürgerkarten Software!

Lokale BKU
Starten Sie Ihre Bürgerkarten Software!

Stork
Zertifikat
Für bereits registrierten User.
Displaying and Signing the Login Data

Willkommen beim ersten elektronischen Zustelldienst in Österreich!
Hier können Sie Ihre Dokumente und Schriftstücke gesichert elektronisch empfangen.

Erstmalige Registrierung
Hier klicken um sich zu registrieren

Mein elektronisches Postfach öffnen
Bereits registriert? Hier geht’s direkt zum Zustelldienst.

Identifikation zum Zugang zum elektronischen Zustelldienst

Durch die elektronische Signatur bestätige ich, [Name], [Datum der Geburt] die Signaturverpflichtung gemäß Artikel [Artikel].

Datum: [Datum der Signatur]
Stunde: [Stunde der Signatur]

[Signaturdetails]

Speichern  Schließen
## Postfach von Klaus Stranacher

<table>
<thead>
<tr>
<th>Status</th>
<th>Datum</th>
<th>Absender</th>
<th>Typ</th>
<th>Größe</th>
<th>Aktionen</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑</td>
<td>27.09.2013</td>
<td>Bundespolizeidirektion Wien, Streifenpolizeiamt</td>
<td>RSA</td>
<td>220533 Byte</td>
<td>☑ ☒</td>
</tr>
<tr>
<td>☑</td>
<td>21.07.2012</td>
<td>Finanzamt Graz-Stadt</td>
<td>RSA</td>
<td>286239 Byte</td>
<td>☑ ☒</td>
</tr>
<tr>
<td>☑</td>
<td>21.07.2012</td>
<td>Finanzamt Graz-Stadt</td>
<td>RSA</td>
<td>74442 Byte</td>
<td>☑ ☒</td>
</tr>
<tr>
<td>☑</td>
<td>21.07.2012</td>
<td>Finanzamt Graz-Stadt</td>
<td>RSA</td>
<td>65398 Byte</td>
<td>☑ ☒</td>
</tr>
<tr>
<td>☑</td>
<td>21.10.2008</td>
<td>BMI TV/SU/ZNR</td>
<td>normal</td>
<td>31302 Byte</td>
<td>☑ ☒</td>
</tr>
</tbody>
</table>
Officially signed Criminal Record Certificate
Overview

- Electronic Signatures
- Legal Framework
- Signature Formats
- Official Signature
- Signature Verification
- Conclusions
Legal Framework

- European Framework given by the EU Signature Directive
  - Implementation of the Directive by the national laws
    - Signature act SigG
    - Signature regulation SigV

- Different types of signatures:
  - Electronic signature
  - Advanced electronic signature
  - Qualified electronic signature
Legal Framework

- Electronic Signature

  §2
  1. ‘electronic signature’ means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

- Advanced Electronic Signature

  §2
  2. ‘advanced electronic signature’ means an electronic signature which meets the following requirements:
     (a) it is uniquely linked to the signatory;
     (b) it is capable of identifying the signatory;
     (c) it is created using means that the signatory can maintain under his sole control;
     and
     (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
Legal Framework

- Advanced Electronic Signature

§2
2. ‘advanced electronic signature’ means an electronic signature which meets the following requirements:
   (a) it is uniquely linked to the signatory;
   (b) it is capable of identifying the signatory;
   (c) it is created using means that the signatory can maintain under his sole control; and
   (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

- Signature-creation data (e.g. private key) and the complementary signature-verification data (e.g. public key) must NOT – at least within one certification service provider – occur more than once.
Advanced Electronic Signature

§2
2. ‘advanced electronic signature’ means an electronic signature which meets the following requirements:
   (a) it is uniquely linked to the signatory;
   (b) it is capable of identifying the signatory;
   (c) it is created using means that the signatory can maintain under his sole control; and
   (d) it is linked to the data to which it relates in such a manner that any subsequent change of 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

§2
2. ‘advanced electronic signature’ means an electronic signature which meets the following requirements:
   (a) it is uniquely linked to the signatory;
   (b) it is capable of identifying the signatory;
   (c) it is created using means that the signatory can maintain under his sole control; and
   (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

- Creation by an **authorized person only**
- Binding by **possession and knowledge**
Legal Framework

Advanced Electronic Signature

§2
2. ‘advanced electronic signature’ means an electronic signature which meets the following requirements:
   (a) it is uniquely linked to the signatory;
   (b) it is capable of identifying the signatory;
   (c) it is created using means that the signatory can maintain under his sole control; and
   (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

- It is practically impossible, that
  - Different electronic data leads to the same hash value
  - Other electronic data leads to an given hash value
Legal Framework

- **Qualified Electronic signature**

  §2 3a. *advanced electronic signatures* which are based on a *qualified certificate* and which are created by a *secure-signature-creation device*

- **Legal Effects**

  §5
  (a) *satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature* satisfies those requirements in relation to paper-based data; and
  (b) *are admissible as evidence in legal proceedings.*

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

- **Qualified Certificate (QC)**
  - Must contain information according to §5 SigG
  - Issued by the CSP according to the requirements in §7 SigG

- **Information according to §5 SigG**
  - Indication that the certificate is a qualified one
  - The unique name of the CSP and the country where it operates
  - The signatory’s name
  - Signature-verification data (signatory’s public key)
  - Validity period of the certificate
  - The CSP’s signature
  - Optionally attributes (limitations, mandates, etc.)
Legal Framework

- **CSP requirements according to §7 SigG**
  - Necessary reliability
  - Directory and revocation service
  - Qualified time
  - Identification of the potential signatories
  - Reliable personal
  - Appropriate financial means and third party insurance
  - Recording
  - Safety measures
  - Supervision by the supervisory authority (RTR)
    RTR…Rundfunk und Telekom Regulierungs-GmbH
  - Some additional requirements
Legal Framework

- Secure Signature Creation Device (SSCD)

  §18 (5)
  The technical components and procedures for creating qualified electronic signatures have to be inspected sufficient and continuous according to the state of the art. The compliance of this safety requirements, regarding the secure signature-creation device according to the federal law and its regulations, have to be certified by a confirmation party (Bestätigungsstelle) according to § 19.

  - 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)
Overview

- Electronic Signatures
- Legal Framework
- Signature Formats
- Official Signature
- Signature Verification
- Conclusions
Signature Formats

- Have to include all information required for the signature verification

- Raw signature data (e.g. signature value, signature algorithm)
- Signed data
- Certificates
- Additional information (e.g. signature creation date, etc.)

CMS/PKCS#7
- CAdES

PDF Signatures
- PAdES

XMLDSIG
- XAdES

PGP
- S/MIME

PDF-AS (Austria)
- etc...

Requirements regarding advanced/qualified signatures

EU Commission decision 2014/148/EC: Definition of reference formats

Interoperability
Signature Formats

- **Advanced Signature Formats *AdES:**
  - **CAdES (ETSI TS 101 733)**
    - CMS Advanced Electronic Signatures
    - Based on CMS
  - **PAdES (ETSI TS 102 778)**
    - PDF Advanced Electronic Signatures
    - Based on PDF Signatures
  - **XAdES (ETSI TS 101 903)**
    - XML Advanced Electronic Signatures
    - Based on XMLDSIG
XMLDSIG

- XML Signature Syntax and Processing
- W3C Recommendation

\[\text{<Signature ID>}
\text{<SignedInfo>}
\text{<CanonicalizationMethod/>}
\text{<SignatureMethod/>}
\text{<Reference URI>}
\text{<Transforms>}
\text{<DigestMethod>}
\text{<DigestValue>}
\text{</Reference>}
\text{</SignedInfo>}
\text{<SignatureValue>}
\text{<KeyInfo>}
\text{<Object ID>}
\text{</Object ID>}
\text{<KeyInfo>}
\text{</SignatureValue>}
\text{</Signature>}\]

Defines which data and how it should be signed
Method for data normalization
Signature method (RSA, DSA, ECDSA, ...)
Definition of the signed data
Signature value
Certificates
Arbitrary data objects (e.g. signed
Data objects referenced by Reference URI)
XMLDSIG

- Processing – Signature creation
  - Reference generation (dsig:References)
  - Signature creation (dsig:SignedInfo)

- Processing – Signature validation
  - Reference validation
  - Signature validation
XMLDSIG

- Reference Generation

```xml
<dsig:Reference URI="uriValue">
  <dsig:Transforms>
    <dsig:Transform Algorithm="tranformID1"/>
    <dsig:Transform Algorithm="tranformID2"/>
  </dsig:Transforms>
  <dsig:DigestMethod Algorithm="digMethID"/>
  <dsig:DigestValue>
    ...fJk3dyKe...
  </dsig:DigestValue>
</dsig:Reference>
```

- Resolving the reference
- Resolved reference is the input for the first transformation (e.g. XPath filtering, XSLT transformation)
- Result from the first transformation is the input for the second transformation
- Result from the last Transformation is the input for the hash calculation
- Calculated hash value is stored within the `dsig:DigestValue` element

Source: Gregor Karlinger, Security Layer Workshop, Vienna, 19.08.2003
XMLDSIG

- Signature Creation

```xml
<dsig:Signature>
  <dsig:SignedInfo>
    <dsig:C14nMethod
      Algorithm="c14nID"/>
    <dsig:SignatureMethod
      Algorithm="sigMethID"/>
    <dsig:Reference ...>
      ...
    </dsig:Reference>
  </dsig:SignedInfo>
  <dsig:SignatureValue>
    ...feHicqRyKe...
  </dsig:SignatureValue>
</dsig:Signature>
```

» Canonization (Normalization) of the `dsig:SignedInfo` element

» Normalized data is the input for the calculation of the signature value

» Signature value is stored within the `dsig:SignatureValue` element

Source: Gregor Karlinger, Security Layer Workshop, Vienna, 19.08.2003
XMLDSIG Example

```xml
<dsig:Signature Id="86afa191-1" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
  <dsig:SignedInfo Id="SignedInfo-86afa191-1">
    <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <dsig:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"/>
    <dsig:Reference Id="Reference-86afa191-1" URI="#Object-86afa191-1">
      <dsig:Transforms>
        <dsig:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
          <XPath xmlns="http://www.w3.org/2002/06/xmldsig-filter2" Filter="intersect">id("Object-86afa191-1")/node()</XPath>
        </dsig:Transform>
      </dsig:Transforms>
      <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <dsig:DigestValue>ck5CfKRJ6J4x7YusP2LmJXRBo3sPoSgTCXlujYNFvI=</dsig:DigestValue>
    </dsig:Reference>
  </dsig:SignedInfo>
  <dsig:SignatureValue Id="SignatureValue">r+6ofFdf0TcO9TlpOrMEime/hegWz/Qdf6XPpZTkS7g==</dsig:SignatureValue>
  <dsig:KeyInfo>
    <dsig:X509Data>
      <dsig:X509Certificate>MIIEwjCCACgqAwIBAgI...PoGXd6AhnuOTubArgBCqKBIWn1w==</dsig:X509Certificate>
    </dsig:X509Data>
  </dsig:KeyInfo>
  <dsig:Object Id="Object-86afa191-1">Ich bin ein einfacher Text.</dsig:Object>
</dsig:Signature>
```
XMLDSIG

- Enveloping Signature

```xml
<Signature>
  <SignedInfo>
    ...
    <Reference URI='#Data'>
      ...
      <DigestValue>xA5c5dA</DigestValue>
    </Reference>
  </SignedInfo>
  ...
  <Object Id='Data'>
    Data to be signed!
  </Object>
</Signature>
```

Source: Gregor Karlinger, Security Layer Workshop, Vienna, 19.08.2003
XMLDSIG

- Enveloped Signature

```xml
<MyDocument Id='MyDocument'>
  <MyData>Data to be signed!</MyData>
  <Signature>
    <SignedInfo>
      ...
      <Reference URI='#MyDocument'>
        ...
        <DigestValue>xAC5dA</DigestValue>
      </Reference>
    </SignedInfo>
    ...
  </Signature>
</MyDocument>
```

Source: Gregor Karlinger, Security Layer Workshop, Vienna, 19.08.2003
XMLDSIG

- Detached Signature

```
<MyDocument>
  <MyData Id='Data'>
    Data to be signed!
  </MyData>
  <Signature>
    <SignedInfo>
      ...
      <Reference URI='#Data'>
        ...
      </Reference>
    </SignedInfo>
    ...
  </Signature>
</MyDocument>
```

```
<Signature>
  <SignedInfo>
    ...
    <Reference URI='http://i.com/d.txt'>
      ...
    </Reference>
  </SignedInfo>
  ...
</Signature>
```

Source: Gregor Karlinger, Security Layer Workshop, Vienna, 19.08.2003
XMLDSIG vs. XAdES

- **XAdES** defines a standard for **advanced XML signatures**
- Specified by ETSI
- Based on XMLDSIG
- Defines multiple signature types:
  - XAdES-BES (Basic Electronic Signature)
    - Fulfills the requirements defined within the Signature Directive
  - XAdES-EPES (Explicit Policy based Electronic Signature)
    - Additionally: Declaration of a signature policy
  - XAdES-T (with Time-stamp)
    - Additionally: Time-stamp for signature creation time
  - XAdES-C (Complete validation data)
    - Additionally: Complete references to certificate and revocation information
  - XAdES-X (eXtended validation data) and XAdES-A (Archiving validation data)
    - For long-time applications
XAdES

Additional XAdES data object

Signed XAdES properties:
* Signature properties
  - Signature creation time
  - Unique reference to the signature certificate
  - Signature policy (EPES)
  - Signature creation location
  - Signatory’s role
* Data object properties:
  - Data object format (MIME type)
  - Binding consent of the signatory (e.g. acknowledgment that the signatory received the data.
  - Time-stamp about (selected) data objects

Unsigned XAdES properties:
* Signature properties
  - Additional signatures (Multiple signature, counter-signature)
XAdES-EPES Example

```xml
<dsig:Signature>
  [[...]]
  <dsig:Reference Id="Reference-86afa191-2" Type="http://uri.etsi.org/01903/v1.1.1#SignedProperties" URI="#xmlns(xades=http://uri.etsi.org/01903/v1.1.1#)%20xpointer(id('Object-86afa191
  2')/child::xades:QualifyingProperties/child::xades:SignedProperties")>
    <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <dsig:DigestValue>MX7krTPP14weU8O/GHWyyOjegyD4/RrkSeZel1AAATlc=</dsig:DigestValue>
  </dsig:Reference>

  [[...]]
  <dsig:Object Id="Object-86afa191-2">
    <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.1.1#" Target="#86afa191-1">
      <xades:SignedProperties Id="SignedProperties-86afa191-1">
        <xades:SignedSignatureProperties>
          <xades:SigningTime>2013-10-01T09:38:59Z</xades:SigningTime>
          <xades:SigningCertificate>
            <xades:Cert>
              <xades:CertDigest>
                <xades:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <xades:DigestValue>VTTr04ilanbEB0lN0jgrNBe3Yhsq2uisGe3j1BjGdhk=</xades:DigestValue>
              </xades:CertDigest>
              <xades:IssuerSerial>
                <dsig:X509IssuerName>CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,...</dsig:X509IssuerName>
                <dsig:X509SerialNumber>1010106</dsig:X509SerialNumber>
              </xades:IssuerSerial>
            </xades:Cert>
          </xades:SigningCertificate>
          <xades:SignaturePolicyIdentifier/>
          <xades:SignedDataObjectProperties>
            <xades:DataObjectFormat ObjectReference="#Reference-86afa191-1">text/plain</xades:DataObjectFormat>
          </xades:SignedDataObjectProperties>
        </xades:SignedSignatureProperties>
      </xades:SignedProperties>
    </xades:QualifyingProperties>
  </dsig:Object>
</dsig:Signature>
```

Used within certificate validation

Used for signature certificate validation defined in KeyInfo
What about Austria?

- Supported formats within Austria:
  - XMLDSIG and XAdES-BES/EPES (according to the Security Layer specification)
  - CMS and CAdES-BES/EPES (according to the Security Layer specification)
  - PDF-AS (proprietary format based on PDF)  
    - to be replaced by PAdES

- Available Tools
  - Citizen card environment (CCE): Signature creation utilizing the citizen card → next Lecture
  - MOA-SPSS: Modules for (server-side) signature creation and verification
  - PDF-Over: Client-application for creating PDF-AS/PAdES signatures
  - Prime Sign: 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
- Conclusions
Official Signature (Amtssignatur)

- Official Documents

How to recognize a document issued by a public authority?

- Invention of the official signature
- Recognition of origin
- Authenticity
Official Signature

- The E-Government law defines the official signature to identify a document's origin
- Using the official signature for electronically signing issued documents (see § 18 AVG)
- The official signature is, except from the need to be an advanced electronic signature, more a regulation of the look than a technical requirement.
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)
  - Requirement to provide information about the signature verification
E.g. Signature Block
Official Signature

- Example: Official signature using MOA-SS and PDF-AS
  - MOA-SS
    - Module for Online-Applications – Server Signature
    - Open source software for creating server-side signatures according to
      - XMLDSIG, XAdES
      - CMS, CAdES
  - PDF-AS
    - Open source library for creating PDF-AS/PAdES signatures
    - Signature creation using the citizen card or MOA-SS
  - Official signature:
    - Creation of PDF-AS/PAdES signed documents including signature blocks via MOA-SS
Overview

- Electronic Signatures
- Legal Framework
- Signature Formats
- Official Signature
- Signature Verification
- Conclusions
Signature Verification

- Signature verification

- (1) Cryptographic verification
  - Comparing the hash value → message not modified
  - Checking the signature value → ensure the signatory’s authenticity

What means authenticity?
Signature Verification

- Why checking the signature value?
  - Check if the public key (from the certificate) matches private key the document was signed with.

- What information is missing?
  - Quality of the authenticity?
  - Validity?
  - Revocation? – e.g. private key is compromised, etc.
X.509 Zertifikat

Seriennummer: 0F69BA
Aussteller: CN=a-sign-Premium-Sig-02 [...]
Antragsteller: CN=Klaus Stranacher
Öffentlicher Schlüssel: 04EF2835ABFE81F...
Schlüsselverwendung: Digitale Signatur
Widerrufsinfo.: OCSP/CRL URL
Qual. Zertifikat: Ja
Sichere Sig.erst.einh.: Ja
Etc.
Signature Verification

- Signature verification

- (2) Certificate validation
  - Time validity
  - Quality of the authenticity (via certification authority or qualified certificate)
  - Key usage
  - Revocation check
Signature Verification

- Signature verification via MOA-SP
  - MOA-SP = MOA signature verification (Prüfung)
  - Counterpart to MOA-SS
Signature Verification

- Cryptographic verification:
  - As specified (e.g. XAdES verification)

- Certificate validation:
  - (1) Build the certificate chain
    - From the signatory certificate to the root certificate
  - (2) For every certificate in the chain:
    - Verify the time validity
    - Verify for revocation using CRL/OCSP
      - CRL: Certificate Revocation List
      - OCSP: Online Certificate Status Protocol
  - (3) Verify if one of the chain’s certificate is included within the defined trust profile.
  - (4) Verify signatory certificate for
    - Qualified certificate (QC) and
    - Secure signature creation device (SSCD)
Signature Verification

- Example MOA-SP Response

```
<VerifyXMLSignatureResponse>
  <SignerInfo>
    <dsig:X509Data>
      <dsig:X509SubjectName>CN=Test Signaturdienst aller Kunden...</dsig:X509SubjectName>
      <dsig:X509IssuerName>C=AT,O=IAIK,CN=IAIK Test Intermediate CA</dsig:X509IssuerName>
      <dsig:X509SerialNumber>10958758428710</dsig:X509SerialNumber>
    </dsig:X509IssuerSerial>
    <dsig:X509Certificate>MIIEKzCCA5...tNGS0wG</dsig:X509Certificate>
    <QualifiedCertificate/>
    <SecureSignatureCreationDevice/>
    <IssuerCountryCode>AT</IssuerCountryCode>
  </dsig:X509Data>
  <SignatureCheck>
    <Code>0</Code>
  </SignatureCheck>
  <CertificateCheck>
    <Code>0</Code>
  </CertificateCheck>
</VerifyXMLSignatureResponse>
```

Signatory information including QC/SSCD

Result cryptographic verification

Result certificate validation
Signature Verification

- On EU level
  - Digital Agenda for Europe
  - E-Government action plan
  - EU Services Directive
  - Target: Grow together of the EU Member States, Free and easy movement of citizens and businesses
  - Mutual acceptance of electronic identity and documents play a vital role
  - Signature verification on international level!
Signature Verification

- **Signature formats**
  - Different signature formats (even proprietary)
  - Complex format specifications → interpreted differently

- **QC/SSCD Check**
  - How to identify the qualification of a foreign certification 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
  - 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 certification service providers that are allowed to issue qualified certificates
  - Implementation: Trust-service Status List (TSL)
  - EU TSL references national TSLs

![Diagram showing EU-TSL, AT-TSL, BE-TSL, and etc.](image-url)
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) → in the case of signature verification the CSP represents the 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 (CSP under supervision, accredited, Accreditation rejected, etc.), the appropriate certificate corresponding to the service and the support of QC/SSCD.
      - Historical status information
Signature Verification

- Example

Austrian TSL

- Operator of the TSL (RTR)
- TSP = CSP (A-Trust)
- Service run by A-Trust
- TSL signed by RTR

http://www.signatur.rtr.at/currenttsl.xml
Signature Verification

- **TSL and MOA-SP**

  ![Diagram of MOA-SP](image)

  - VerifySignatureRequest
  - VerifySignatureResponse
  - Kryptographische Prüfung
  - Zertifikatsprüfung
  - Trustprofiles [Configuration]
    - ID01, Truststore #1
    - ID02, Truststore #2
    - ID03, Truststore #1 [TSL enabled]
  - MOA-SP
  - TSL Wrapper
  - TSL Unit
  - TSL Library
  - TSL Database
  - CRL, OCSP
  - EU-TSL
  - AT-TSL
  - BE-TSL etc.

- **International signature verification**
  - XMLDSIG/XAdES
  - CMS/CAdES
  - PDF/PAdES

- **International certificate validation**
  - Trust profiles are updated by the certificates from the TSL → validation against foreign trusted certificates possible
  - Recognition of QC/SSCD via appropriate TSL request.
Overview

- Electronic Signatures
- Legal Framework
- Signature Formats
- Official Signature
- Signature Verification
- Conclusions
Conclusions

- Use of advanced and qualified signatures in E-Government processes and applications
- Legal framework
- Signature formats (XMLDSIG, XAdES, etc.)
- Official signature
- Signature validation
  - National
  - International: Problems + Solutions
Conclusions

- What is the qualified signature in Austria?

Citizen Card

Details: NEXT WEEK!
Electronic signature are used either for ensuring data integrity or ensuring the signatory’s authenticity.

- [ ] True
- [ ] False
Control Questions

- An advanced electronic signature must provide the following criteria. Select the right answers:
  - [ ] it is exclusively assigned to the signatory
  - [ ] it must be based on a qualified certificate
  - [ ] it enables the identification of the signatory
  - [ ] it was created with equipment solely controlled by the signatory
  - [ ] it has to be created by using a secure signature creation device
  - [ ] it is bound to the signed data in such a way, that every alteration of the signed data will be recognized by the verifying entity
Control Questions

- Match the signature types to the statements below.

  - A  Official signature
  - B  Qualified electronic signature
  - C  Advanced electronic signature

  - [ ] From a legal point of view it is equal to a handwritten signature
  - [ ] It must contain information regarding the signature verification
  - [ ] It defines the minimum requirements for applications within the scope of the EU Service Directive
Control Questions

- Define the correct ordering of the steps carried out for creating an XMLDSIG signature (Fill in numbers from 1 to 7).
  - [ ] Creating the dsig:Signature element
  - [ ] Perform the transformation(s)
  - [ ] Calculate the signature value
  - [ ] Canonicalization of the dsig:SignedInfo element
  - [ ] Resolve the reference
  - [ ] Add certificate information
  - [ ] Calculate the hash value
Control Questions

Complete the sentence by filling out the gaps:

- A ___________ electronic signature is an _______ electronic signature, that is based on a
  ____________ _________ and created using a ______ signature _______ _______.

A ___________ electronic signature is an _______ electronic signature, that is based on a
___________ _________ and created using a ______ signature _______ _______.
Control Questions

- Which technical means is used to simplify the cross-border certificate validation?
  - Answer: ______________ (1 Word)
Control Questions

- Explain and draft on ½ sheet of paper the problems that may occur within a cross-border signature verification and the possible solutions.
Control Questions

- Explain and draft on ½ sheet of paper the basics of electronic signatures and their applications within the E-Government.
Control Questions

- Explain and draft on ½ sheet of paper how the legal requirements on the advanced digital signature are fulfilled.
Control Questions

- Explain and draft on ½ sheet of paper the functional principle of the given signature (a given XAdES signature). Explain the process of the signature verification.
**Control Questions**

- Explain and draft on ½ sheet of paper the principle of TSL. Explain how TSLs are used within the area of signature verification.