eSignature at EC

EEMA BE Briefing
25/02/2016
Pierre A. Damas
European Commission
DIGIT.B.1.002
DIGIT.B1.002 – Digital services

Authentication
- ECAS
  - Authentication Service of the Commission
- CEF Building blocks of eIdentification DSI
  - CEF eID

eSignature
- ESSI
  - Electronic Signature Service Infrastructure
- CEF Building blocks of eIdentification DSI
  - CEF eSignature
Content

How it works? 4
Issues 13
Situation at EC 21
Impact of eIDAS 27
Next steps 30
Legal references 32
eSign application 36
eSignature
How it works
Signing a document

- Compute hash
Signing a document

• Compute hash

• Encrypt hash with private key
Signing a document

• Compute hash

• Encrypt hash with private key

• Send document with
  • encrypted hash
  • certificate containing the public key
Validating the signature

• Compute hash
Validating the signature

• Compute hash

• Decrypt the encrypted hash received with the public key
Validating the signature

• Compute hash

• Decrypt the encrypted hash received with the public key

• Compare results
Validating the signature

• Compute hash

• Decrypt the encrypted hash received with the public key

• Compare results

• Check that certificate is trusted
• Check that certificate is not revoked
eSignature

- **Integrity**
  - The hash would be different if the document changed

- **Authentication**
  - Your certificate confirms your identity and that you have the corresponding private key

- **Non-repudiation**
  - Only you could have signed, and if the private key is compromised, the certificate must be revoked
eSignature

Issues
Issues

• Signature
  • Where to store the private key?
  • How to get a certificate?
  • What application or device to sign?

• Validation
  • What application to validate?
  • Do I trust the certificate?
  • How to check revocation?
Where to store the private key?

- On a smartcard, USB device
- On a mobile device
- On a desktop computer
- On a Hardware Security Module (HSM)
How to get certificates?

• Internal PKI
• External provider

• Process
  • Create keys
  • Create a certificate request
  • Validate identity with CA
  • Install certificate
What application to sign?

• **Client side**
  • Need access to smartcards or local keystore
  • Java applets
  • Browser plugins
  • Native applications

• **Server side**
  • API to access service
  • Web User Interface
What application to validate?

• Client side
  • Java applets
  • Browser plugins
  • Native applications

• Server side
  • API to access service
  • Web User Interface
Do I trust the certificate?

• Closed circle
  • Certificate directly in trusted store
  • Certificate of Certification Authority (CA) in trusted store

• Interoperable signature
  • Availability of trusted lists & LOTL
How to check revocation?

• Certificate revocation list
  • URL in the certificate
eSignature

Situation at EC
What we do

Scope
Creation, validation and extension of interoperable AdES

European Commission
Service
Web Service
Proprietary SW library
Web Application

Member states
Open Source Software
- TL
- DSS
Service
- LOTL
- Demo Platform

EXPERTISE AND SUPPORT
What we do
For the European Commission

4 Use Cases for eSignatures @ EC:

**Physical person outgoing** signature
Create QES

**Legal person outgoing** signatures
Create AdES\textsubscript{QC}

**Physical person internal** signatures
Create AdES\textsubscript{EC}

**Received signatures**
Validate QES, AdES\textsubscript{QC}, AdES\textsubscript{EC}

Intra EC
Extra EC

Intra EC
Extra EC

Intra EC
Extra EC
What we do: ESSI

For the European Commission

2 sets of services available

Supporting services

**Web Service**

- electronic Seal service
- redundant qualified time stamping service
- EU-trusted-list based validation and extension service (generic ESSI policy)

**Web Application**

- eSig: The electronic signature service
- Creation, validation and extension of interoperable AdES
What we do: ESSI
For the European Commission

Examples of applications already using interoperable AdES in production at EC:

- **OP**
  - Official Journal

- **DG GROW**
  - Professional certificates

- **DIGIT**
  - eSig

- **DIGIT**
  - ePRIOR

- **JUST**
  - eCodex
What we do: CEF eSig
OPEN SOURCE for Member States

Software

DSS
- Creation
- Extension
- Validation of cross-border interoperable eSignatures

TL MANAGER
Management of
- MS TLs
- EU LOTL

Supporting services

LIST of TRUSTED LISTS

DEMONSTRATION PLATFORM

EXPERTISE AND SUPPORT
eSignature
Impact of eIDAS
Impact of eIDAS

• Format of advanced electronic signatures (not long-term archiving)
  • PAdES: ETSI TS 103172 v.2.2.2.
  • XAdES: ETSI TS 103171 v.2.1.1.
  • CAdES: ETSI TS 103173 v.2.2.1.
  • Container: ETSI TS 103174 v.2.2.1.

Ensure that DSS library, eSig application & ESSI services use these standards
Impact of eIDAS

• Trusted lists
  • Qualified Trusted services

• Qualified & non-qualified Trusted services in TL
• New certificates from Qualified Trusted Services
• Transition to the new LOTL
• LOTL sealed with eIDAS seal
eSignature

Next steps
Next steps

• Physical persons ongoing signature with ESSI HSM infrastructure
  • Need to have HR procedures matching Local Registration Authority procedures
• Mobile device signature
• Better integration in Office Automation tools
eSignature

Legal References
Legal references

• eSignature


• eSignature under Service directive

Legal references

• eIDAS

• Format of signatures and seals
  Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance)

• Format of trusted lists
Legal references

• eIDAS under Service Directive

eSignature

eSig application
Sign a PDF document

1 - Select a document:

2 - Select a destination:

3 - Select required signature type:

Qualified electronic signature

- QES
  - What does this button do? | What is QES? | How to get a certificate?

Seal (Advanced electronic signature based on a qualified certificate)

- Seal
  - What does this button do? | What is a seal? | How to get a certificate?

Commission internal signature

- AdES/EC
  - What does this button do? | What is AdES/EC? | How to get a certificate?
Sign a document

1 - Select a document:

2 - Select a destination:

3 - Select required signature type:

Qualified electronic signature

- QES
  What does this button do? | What is QES? | How to get a certificate?

- Seal
  What does this button do? | What is a seal? | How to get a certificate?

Commission internal signature

- AdES/EC
  What does this button do? | What is AdES/EC? | How to get a certificate?
Sign a document

1 - Select a document:

2 - Select a destination:

3 - Select required signature type:

Qualified electronic signature

- QES
  - What does this button do? | What is QES? | How to get a certificate?
  - Qualified Certificate: ✓
  - SSCD: ✓
  - Server signature: -

Seal (Advanced electronic signature based on a qualified certificate)

- Seal
  - What does this button do? | What is Seal? | How to get a certificate?
  - Qualified Certificate: ✓
  - SSCD: -
  - Server signature: ✓

Commission internal signature

- AdES/EC
  - What does this button do? | What is AdES/EC? | How to get a certificate?
  - Qualified Certificate: -
  - SSCD: -
  - Server signature: -
 Validate a signature

1 - Select signature :: (Attached):

2 - Validate signature:

The validation process checks whether the signatures are valid QES, AdES/QC or AdES/EC signatures.

Qualified electronic signature

Advanced electronic signature based on a qualified certificate

Commission internal signature

---

Qualified Certificate: ✓ ✓

SSCD: - -