What signature should I trust most?

VERSUS

Qualified Electronic Signature
Compliance verified

Common Criteria EAL4+ Certified
Why the walrus?

He thinks he is safe but is he really?
How does the architecture differ? – legacy apps

Versus

**OS & Applications**

**MS CAPI**
- CSP 1
- SC A
- Card reader/driver
- USB
- PCICMIA
- PC/SC Library
- Physical secure hardware

OR

**PKCS#11**
- CSP 1
- SC A
- P11 lib
- I2C

**Secure communication channel based upon SRP encapsulated in a SSL/TLS session**

**Secure Hardware (HSM)**

**Forwarder / Server**
How does the architecture differ? – web environment

**Web application**

**Web Browser**
- Client-side scripting component (E.g. Applet, ActiveX or Javascript)

- PC/SC Library
  - Card reader/driver
    - USB
    - PCICMIA
    - I2C

- Physical secure hardware

**VERSUS**

**Web application**

**Web Browser**
- Client-side scripting component (E.g. Applet, ActiveX or Javascript)

**Server-side business intelligence**
Interaction with back-end
Generates HTML Pages

Secure communication channel based upon SRP encapsulated in a SSL/TLS session

**Forwarder /Server**

**Secure Hardware (HSM)**
# Forensic Security Analysis

<table>
<thead>
<tr>
<th></th>
<th>Smart card approach</th>
<th>Signature server</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Private key protection</strong></td>
<td>Tamper evident hardware (SSCD device)</td>
<td>Tamper evident hardware (HSM)</td>
<td>equal</td>
</tr>
<tr>
<td><strong>Sole control over private’s key</strong></td>
<td>Difficult to control: What app has access to the smart card? Is there any key logger? No usage log accessible as opposed to control what was signed when.</td>
<td>Under 2FA and based upon protocol resistant against MITM attacks (SRP) Key policy (may) prevents internal administrator to gain access to the key. Central logging allows for usage monitoring.</td>
<td>Advantage to Signer</td>
</tr>
<tr>
<td><strong>Authenticity of the message</strong></td>
<td>Message hashed by crypto layer</td>
<td>Message hashed by crypto layer but it is relatively easy to authenticate data to be signed together with the user.</td>
<td>Advantage to Signer</td>
</tr>
</tbody>
</table>
# Forensic Convenience Analysis

<table>
<thead>
<tr>
<th></th>
<th>Smart card approach</th>
<th>Signature server</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key/cert / CRL management</td>
<td>Cert renewal/ Rekey / PIN loss scenarios difficult to handle.</td>
<td>Can be managed centrally using E.g. a web service. Maintaining a CRL is (almost) optional (cert suspended ➔ key disabled)</td>
<td>Advantage to Signer</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Difficult to ensure (limited admin rights, availability of USB ports / Card readers, driver issues) Mobile devices difficult to integrate.</td>
<td>Easy to support multiple devices / multiple tokens. Fits well into <em>bring your own device</em> initiative.</td>
<td>Advantage to Signer</td>
</tr>
<tr>
<td>Cost</td>
<td>Fits with small deployments (E.g. Enterprises with controlled environment)</td>
<td>Small and large scale deployments. Can be deployed in soft only basis with AuthApp)</td>
<td>Advantage to Signer</td>
</tr>
</tbody>
</table>
Cryptomathic Signer

- Experience in nation-wide deployments (DK, LU, NO, Qatar)
- First solution on the market (2002)
- Awarded technology: From Davos WEF Form EPO
- Contributing member to standards WG 17 (TS 14167-5 + PP)
- Core business on building secure servers

Cryptomathic Signer Solution
The right balance

2FA
- User-friendly
- Affordable
- Easy to integrate

PKI
- Legal Value
- Security

Advantages
- Legal value
- Insures data integrity (documents, transactions, etc.)
- Makes it easy to add value added services (time stamping, archival)

Limits
- No data integrity, not resilient against sophisticated attacks
- No legal value
- Little standardisation

Cost
- EUR 25 → EUR 75

Advantages
- User-friendly
- Affordable
- Easy to integrate

Limits
- Not user-friendly (reduced mobility, difficult integration, client PC dependent)
  - Cost (EUR 25 → EUR 75)
Highlights on Signer security design

- Strong Security Design
  - Secure HW enabled logging
  - Strong Privilege based admin
  - Logical/physical split Auth/Sign
  - User privacy protected
  - Flexible Key/2FA Policy
Integration capabilities

Access your key from various devices
...transact on a device
...validate on another
Digital Signature as a service

**Application flow**

1 - need for signed transaction

2 - request for signature

3 - (strong) authentication

4 - signature

**User**

**User’s private key**

**e-Business Application**

**signed transaction**
Looks very much like eCommerce ...

Safe-deposit your key as you do it for your cash!

Keep sole control over it as you do for your cash!
Digital Signature Module

- **PDF adapter**
  - PAdES
  - PDF

- **Image adapter**
  - JPG/PNG

- **XML adapter**
  - XAdES

**WYSIWYG framework**

**Including:**
- Binary documents
- CAdES signature format
- Viewer
Thank you!

Experience & Security in Server Signing

Guillaume.forget@cryptomathic.com