

Datenbank mit CertificateDescription für Berechtigungszerifikate

IT Security Workshop WS 10/11
Martin Stapel

Der neue Personalausweis

- Teil der eCard Strategie (2005)
 - WPA/ePA, eGK, ELSTER, ELENA
- Einführung 1.11.2010
- jährlich ca. 8 Mio Ausstellungen
- Einführung 2020 abgeschlossen

Der neue Personalausweis

- Sichtausweis
- Elektronische Funktionen
 - Biometrische Identitätsfunktion
 - Elektronischer Identitätsnachweis
 - Qualifizierte elektronische Signatur

Berechtigungszerifikate

- Berechtigtes Interesse
- Erforderlichkeitsprüfung
- offizielle Berechtigungs-CA
 - Bundesdruckerei

Motivation

welche Daten werden ausgelesen?

BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE

PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE

T22000129

Name/Surname/Nom
MUSTERMANN
GEB. GABLER

Vornamen/Given names/Prénoms
ERIKA

Geburtsort/Place of birth/Lieu de naissance
BERLIN

Geburtsort/Place of birth/Lieu de naissance
BERLIN

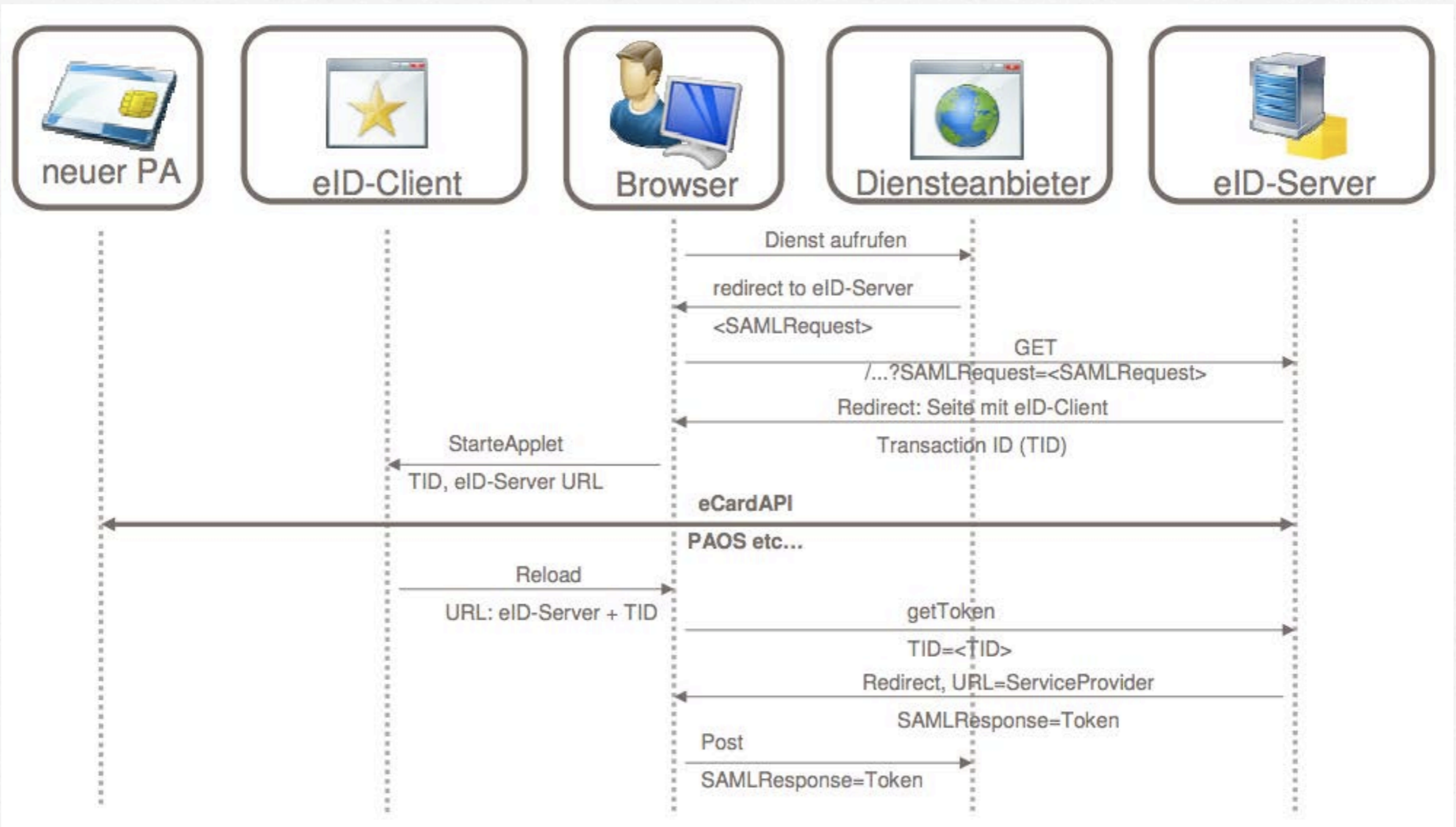
Gültig bis/Date of expiry/
Date d'expiration
31.10.2020

Staatsangehörigkeit/Nationality/
Nationalité
DEUTSCH

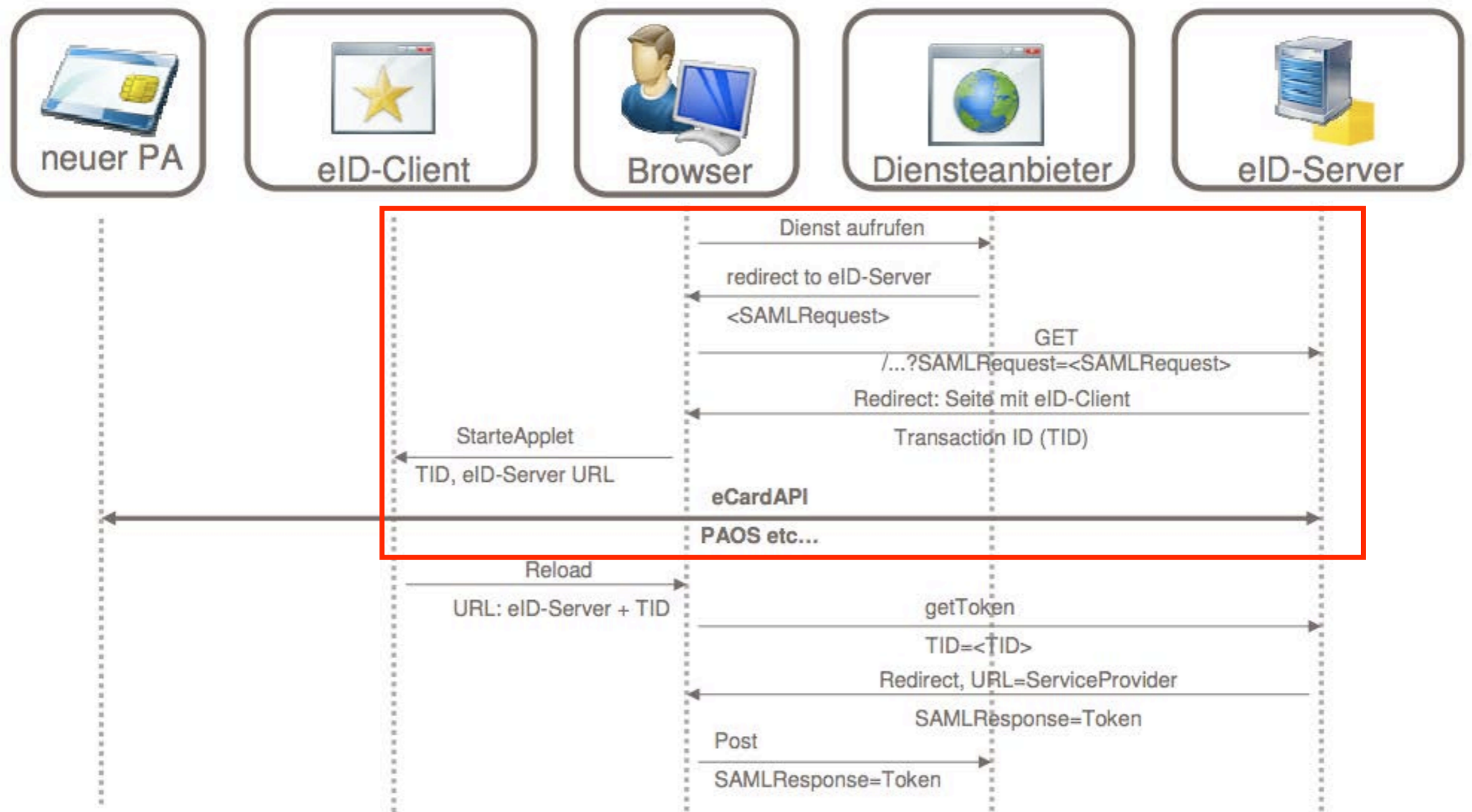
938568

Unterschrift der Inhaberin/des Inhabers -
Signature of bearer - Signature de la titulaire/du titulaire

Online Identitätsnachweis



Online Identitätsnachweis



Online Identitätsnachweis

Registrieren

Registrieren mit

Standard-Registrierung

neuem Personalausweis* 



Legen Sie Ihren neuen Personalausweis in das Kartenlesegerät und klicken Sie "Weiter".

◀ Zurück

▶ Weiter

 SSL-verschlüsselte
Datenübertragung

Download mit nPA



Sofern Sie den Text nicht erkennen können, klicken Sie bitte hier: [neues Bild laden](#)

Weiter

Online Identitätsnachweis

Redirect zum eID-Server

```
<form action="https://eid002.init-ag.de/epa" method="post">
<div>
<input type="hidden" name="SAMLRequest" value="xVbZkqJIFH33Kwz6kk
<input type="hidden" name="SigAlg" value="http%3A%2F%2Fwww.w3.org
<input type="hidden" name="Signature" value="CYBccpc7wCepMAcHHLpM
</div>
<noscript>
<div>
<input type="submit" value="Continue" />
```


Online Identitätsnachweis

Start der AusweisApp

```
<HTML><HEAD><TITLE> eCard Client Initiator</TITLE></HEAD><BODY><object type="application/vnd.ecard-client" width=
<param name="ServerAddress" value="eid002.init-ag.de:443"/>
<param name="SessionIdentifier" value="6d7846510dcb338aff77579e6343"/>
<param name="Binding" value="urn:liberty:paos:2006-08"/>
<param name="PathSecurity-Protocol" value="urn:ietf:rfc:4279"/>
<param name="PathSecurity-Parameters" value="<PSK>34b08dd0bd67fb0dfbdaa65500eb3ddb7ee29890alab9b16ef844222662b5
<param name="SHA256ofSAMLRequest" value="MDEwDQYJYIZIAWUDBAIBBQAEIO1mt1bAS3OUQ28I5olYFwOaDDYXtlf7gEAaaxZBfaY9"/
<param name="RefreshAddress" value="https://eid002.init-ag.de:443/epa/plugin?UESDBBQACAAIAG%2ByPT8AAAAAAAAAAAAAA
</object>
```


Online Identitätsnachweis

Proof of identity – Provider information

Service provider's statements

Service provider's name:
SCHUFA Holding AG

Service provider's internetaddress:
<http://www.meineSCHUFA.de>

Service provider's statements:
Name, Anschrift und E-Mail-Adresse des Diensteanbieters:
SCHUFA Holding AG
Kormoranweg 5
65201 Wiesbaden
epa@schufa.de

Geschäftszweck:
- Registrierung und Login am Portal "Meine SCHUFA-Auskunft Online"-

Hinweis auf die für den Diensteanbieter zuständigen Stellen, die die Einhaltung der Vorschriften zum Datenschutz kontrollieren:
Der Hessische Datenschutzbeauftragte

Requested data

Please submit the following data from your ID card for the purpose shown above.

<input checked="" type="checkbox"/> Given names	<input type="checkbox"/> Religious/artistic name
<input checked="" type="checkbox"/> Family names	<input type="checkbox"/> Type of ID card
<input type="checkbox"/> Doctoral degree	<input type="checkbox"/> Issuing state
<input checked="" type="checkbox"/> Address	<input type="checkbox"/> Address confirmation
<input checked="" type="checkbox"/> Date of birth	<input type="checkbox"/> Age confirmation
<input checked="" type="checkbox"/> Place of birth	<input checked="" type="checkbox"/> Restricted identification

If you agree to submit the selected data, please enter your 6-digit PIN.

ID card-PIN

On-screen keyboard

Back Next Cancel

On-screen keyboard

Back Next Cancel

Geht's auch ohne?



 **Jetzt laden**
AusweisApp^{1.4.0}
Kostenloser Download für
Windows XP, Vista, 7 / 56,3 MB

↓



 **Jetzt laden**
AusweisApp^{1.3.0}
Kostenloser Download für
Ubuntu ab 10.04 / 92 MB

↓



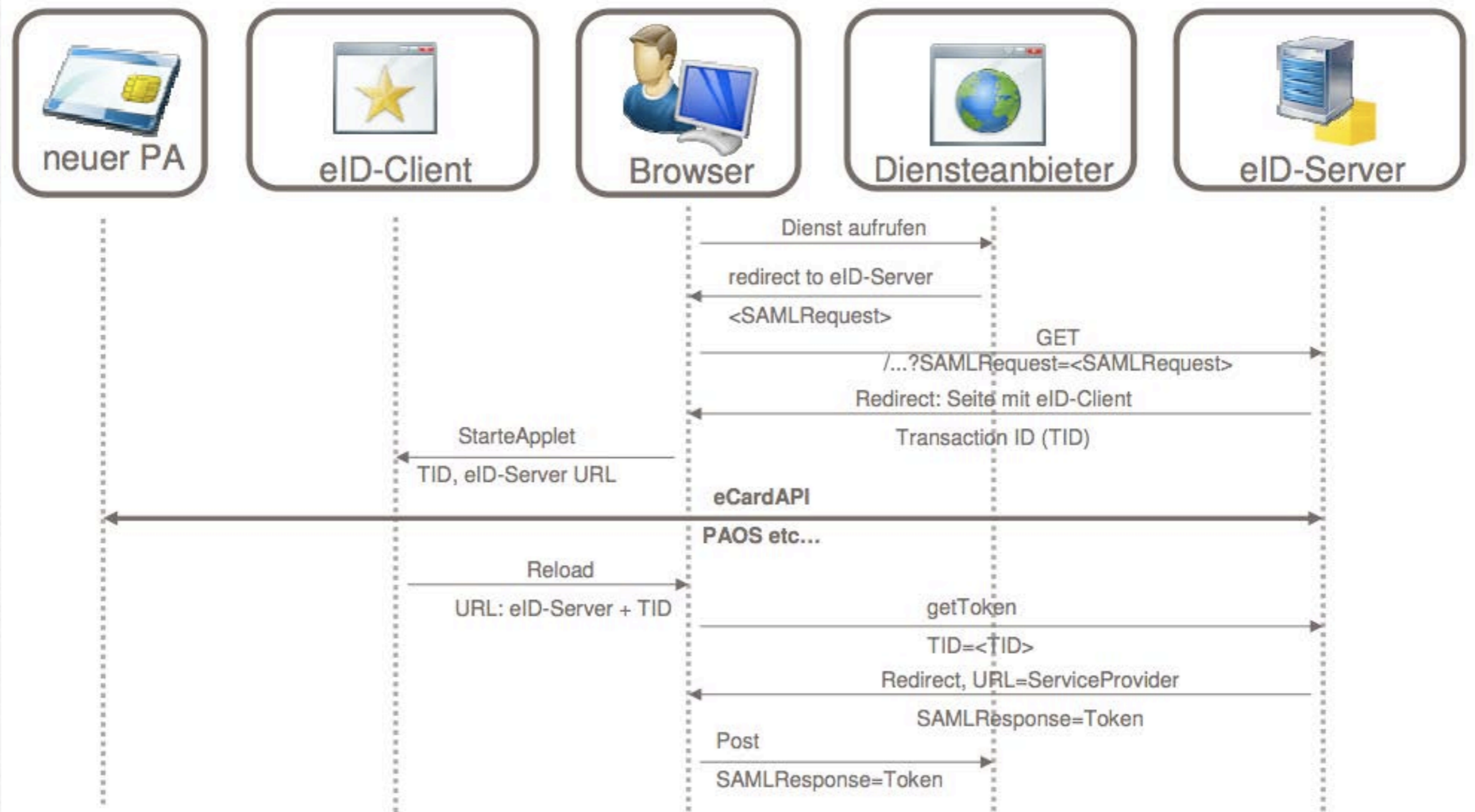
 **Jetzt laden**
AusweisApp^{1.3.0}
Kostenloser Download für
Debian 5 & 6 / 92 MB

↓

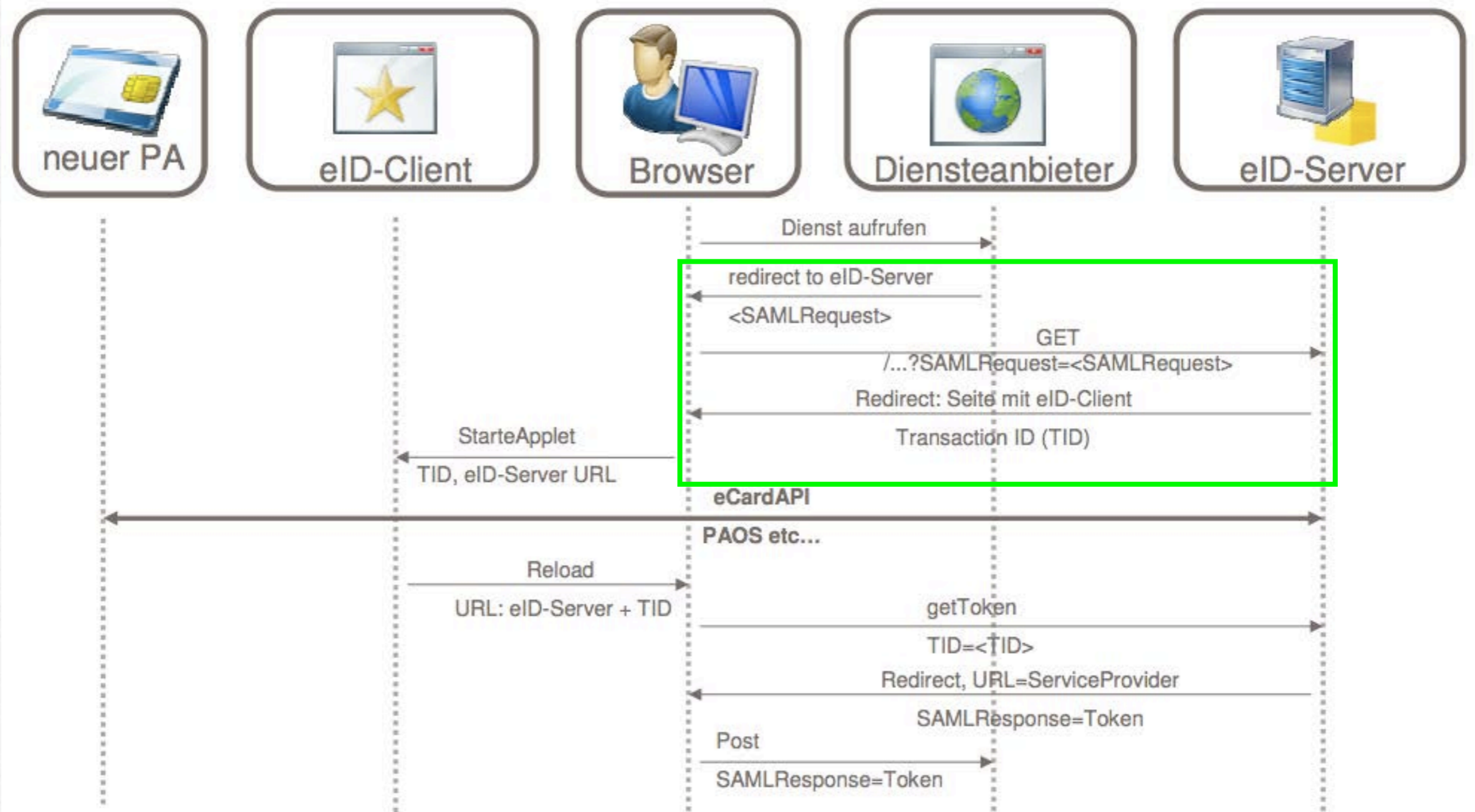
Mit den richtigen Informationen,

ja!

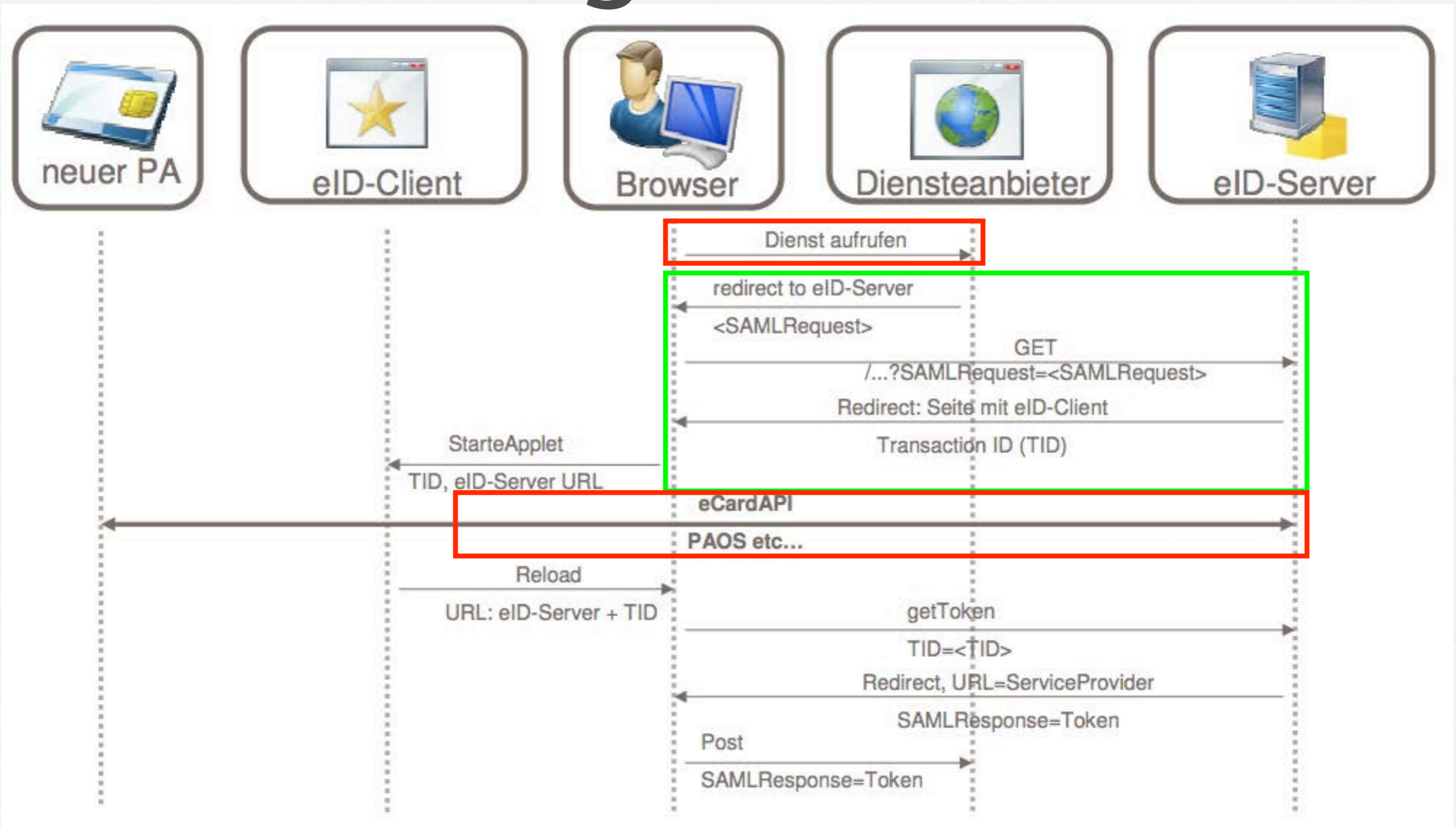
So wird's gemacht - fast!



So wird's gemacht - fast!



So wird's gemacht - fast!



So wird's gemacht - fast!

- AusweisApp <-> eID-Server
 - TLS-PSK Verbindung
- Reverse HTTP-Binding for SOAP

So wird's gemacht - fast!

- AusweisApp <-> eID-Server
 - TLS-PSK Verbindung
- Reverse HTTP-Binding for SOAP

GET /eService?SessionIdentifier=6055279a208990b3195d45322015 HTTP/1.1

Host: eid.eid-service.de:443

Accept: text/html; application/vnd.paos+xml

PAOS: ver="urn:liberty:paos:2006-08"; "urn:iso:std:iso-iec:24727:tech:schema"

So wird's gemacht - fast!

- AusweisApp <-> eID-Server
 - TLS-PSK Verbindung
- Reverse HTTP-Binding for SOAP

GET /eService?SessionIdentifier=6055279a208990b3195d45322015 HTTP/1.1

Host: eid.eid-service.de:443

Accept: text/html; application/vnd.paos+xml

PAOS: ver="urn:liberty:paos:2006-08"; "urn:iso:std:iso-iec:24727:tech:schema"

So wird's gemacht - fast!

HTTP/1.1 400 Bad Request

...

...

com.openlimit.ecard.paos.exceptions.InvalidHTTPHeaderException: Not a HTTP GET/POST request or valid HTTP response!

at com.openlimit.ecard.paos.schemata.HTTPHeader.parse(HTTPHeader.java:366)

at com.openlimit.ecard.paos.tools.HTTPTools.readHTTPHeader(HTTPTools.java:104)

at com.openlimit.eidserver.httphandler.HTTPHandler.jndiConnection(HTTPHandler.java:1037)

at com.openlimit.eidserver.httphandler.HTTPHandler.processRequest(HTTPHandler.java:472)

at com.openlimit.eidserver.httphandler.HTTPHandler.doGet(HTTPHandler.java:234)

at javax.servlet.http.HttpServlet.service(HttpServlet.java:617)

...

So wird's gemacht - fast!

HTTP/1.1 400 Bad Request

...

...

com.openlimit.ecard.paos.exceptions.InvalidHTTPHeaderException: Not a HTTP GET/POST request or valid HTTP response!

at com.openlimit.ecard.paos.schemata.HTTPHeader.parse(HTTPHeader.java:366)

at com.openlimit.ecard.paos.tools.HTTPTools.readHTTPHeader(HTTPTools.java:104)

at com.openlimit.eidserver.httphandler.HTTPHandler.jndiConnection(HTTPHandler.java:1037)

at com.openlimit.eidserver.httphandler.HTTPHandler.processRequest(HTTPHandler.java:472)

at com.openlimit.eidserver.httphandler.HTTPHandler.doGet(HTTPHandler.java:234)

at javax.servlet.http.HttpServlet.service(HttpServlet.java:617)

...



So wird's gemacht - fast!

HTTP/1.1 400 Bad Request

...

...

com.openlimit.ecard.paos.exceptions.InvalidHTTPHeaderException: Not a HTTP GET/POST request or valid HTTP response!

at com.openlimit.ecard.paos.schemata.HTTPHeader.parse(HTTPHeader.java:366)

at com.openlimit.ecard.paos.tools.HTTPTools.readHTTPHeader(HTTPTools.java:104)

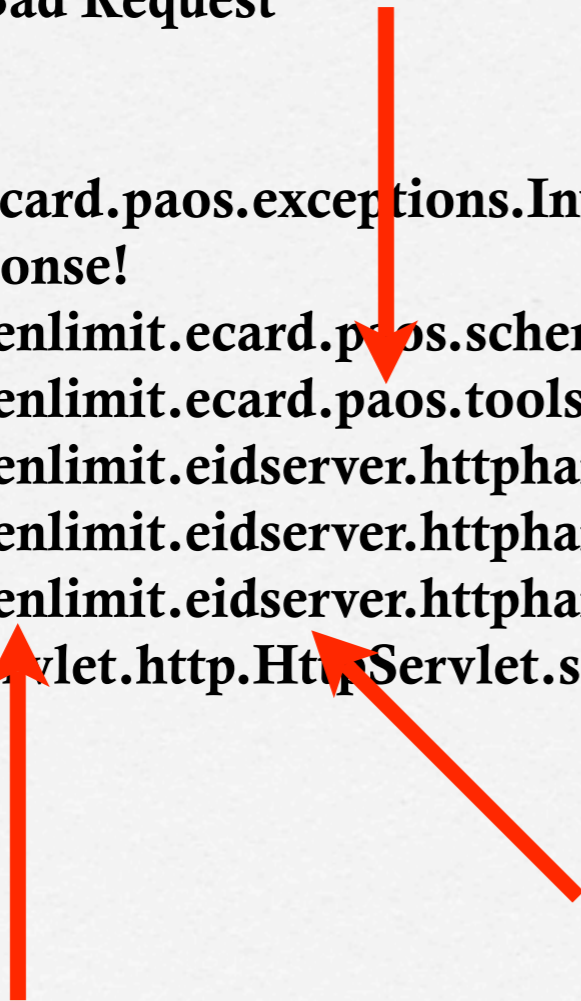
at com.openlimit.eidserver.httphandler.HTTPHandler.jndiConnection(HTTPHandler.java:1037)

at com.openlimit.eidserver.httphandler.HTTPHandler.processRequest(HTTPHandler.java:472)

at com.openlimit.eidserver.httphandler.HTTPHandler.doGet(HTTPHandler.java:234)

at javax.servlet.http.HttpServlet.service(HttpServlet.java:617)

...



Fazit

- Dienstanbieteraufruf
 - Browser-Plugin?
- eCard-API-Kommunikationsprotokoll
 - PAOS
 - Weitere Protokollschritte nötig?

Quellen

- Das Berechtigungszertifikat - Bundesdruckerei GmbH
http://www.bundesdruckerei.de/de/service/service_downloads/produkte_berechtigungszertifikat.pdf
- Der neue Personalausweis und Governikus®. - bremen online services (CeBIT 2010)
<http://files.messe.de/cmsdb/D/007/22145.pdf>
- The New German eID Card: Concepts, Technologies and Opportunities - Fraunhofer SIT (DESY Computing Seminar 2011)
www.desy.de/dvsem/WS1011/waldmann_talk.pdf
- Der elektronische Identitätsnachweis des zukünftigen Personalausweises - Bundesministerium des Inneren
http://www.e-konsultation.de/netzpolitik/sites/default/files/Hintergrundinfo_Elektronischer%20Identitätsnachweis%20PA.pdf