Strong Authentication based on the German ID Card

Protocols and Use Cases

10th ICCC / 2009-09-22 / Dr. Klaus Lüttich

bremen
online services

Present Registration / Identification

- filling in an (electronic) form
  (print out with hand-written signature)
- copy of id card by letter or fax
- “postident”
  (German ID card and address verification)
- verification link in e-mails
- by personal identification in an office
- by (qualified) electronic signature

Present Authentication and Verification

- username / password
- TLS with client X.509 certificate
- smart card

- verification of credit card details
- age verification by delivery service
- PIN / TAN (online banking)

Issues of the e-Service user

- managing many registrations and username / password combinations
- more data than needed is inquired by the service provider
- each provider offers its own data protection policy
- no truly anonymous access with e.g. age verification

Issues of the e-Service provider

- costly registration processes in special offices
- self registration with unreliable data
- two-factor authentication needs issuance of costly security tokens (e.g. smart cards)
- collected personal data needs protection and maintenance

German ID card

- proximity card with extended travel documents standard
- sovereign tasks and border control are supported by biometry

- ID function for eGovernment and eBusiness
- optional: qualified electronic signature

ID function of German ID card

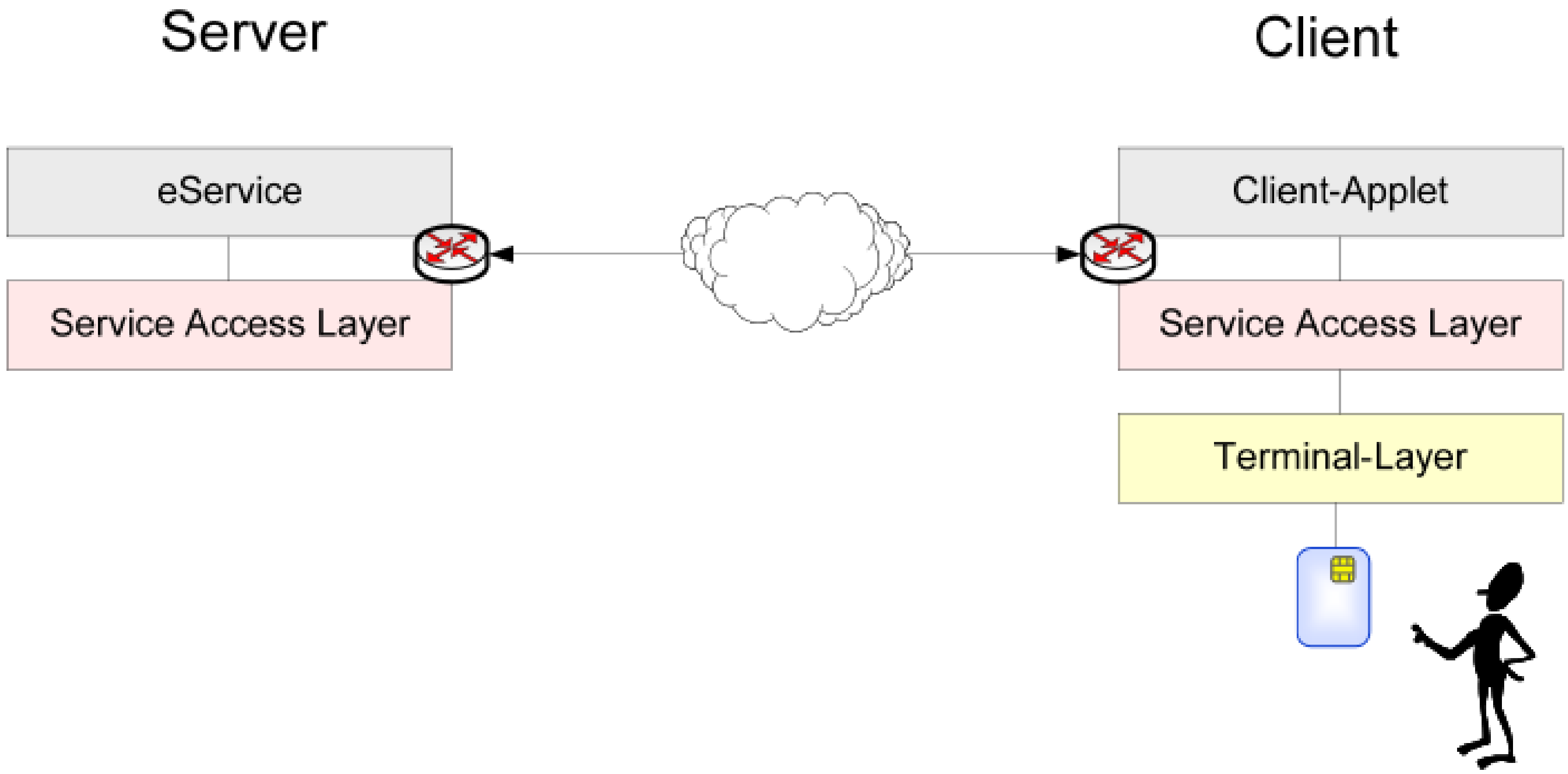
- Restricted Identification by sector-specific identifier
- personal data
  (e.g. name, first-name, address, date of birth)
- age verification (date of birth not disclosed)
- regional verification (residence not disclosed)

Protected by PIN and authorization certificate / card verifiable certificate (CVC)

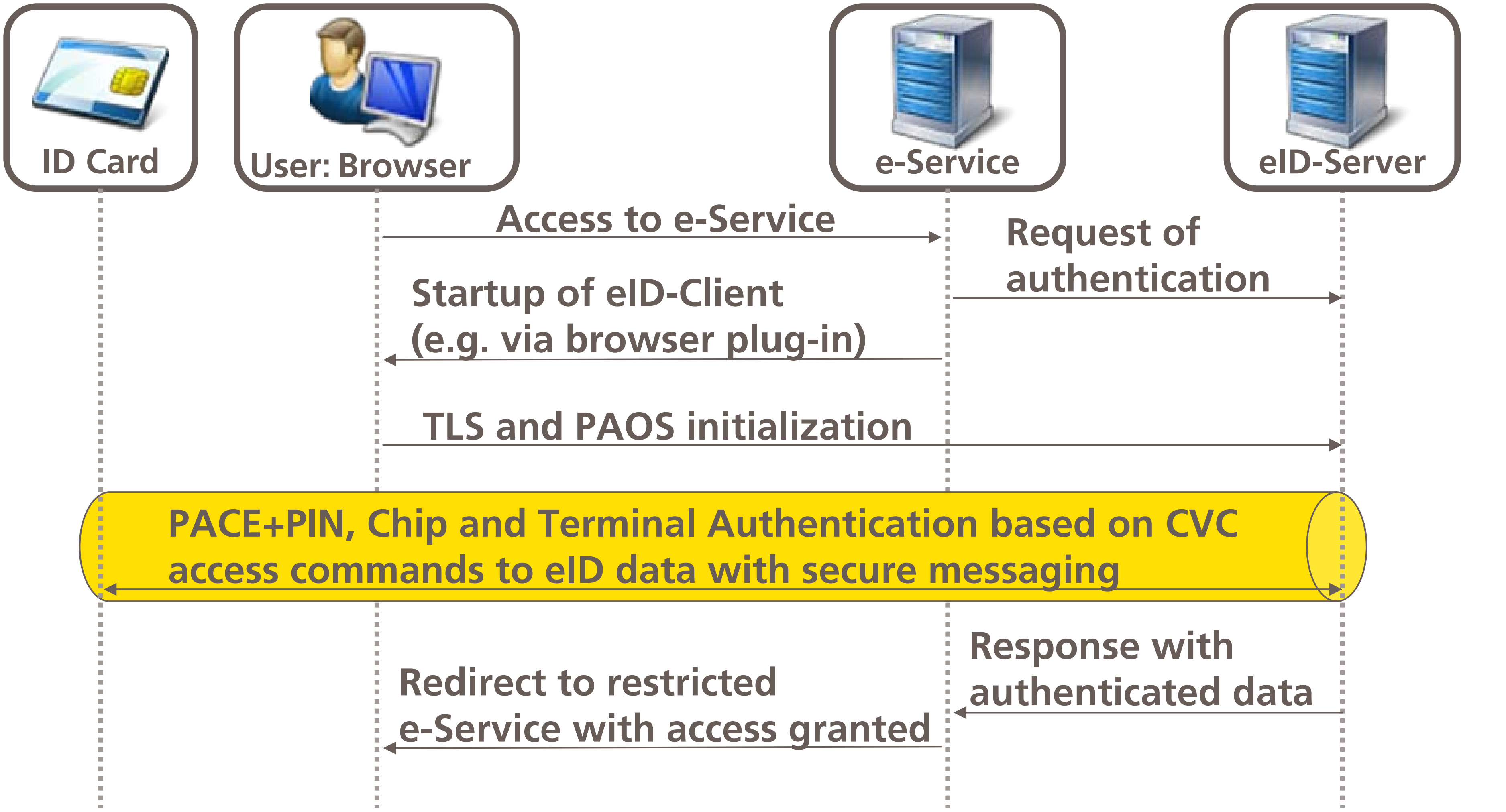
CVC for the e-Service provider

- application for authorization certificate includes statement of purpose and of data fields to be accessed
- right to access is granted by the federal government
- CVC issued online by governmental office after authentication with authorization cert.
- CVC has short duration of validity (2 days)

eCard API layers of eID software components



Authentication example (simplified protocol)



ID Card

User: Browser

e-Service

eID-Server

Access to e-Service

Request of authentication

Startup of eID-Client (e.g. via browser plug-in)

TLS and PAOS initialization

PACE+PIN, Chip and Terminal Authentication based on CVC access commands to eID data with secure messaging

Response with authenticated data

Redirect to restricted e-Service with access granted

Registration with pseudonym

- user has to register once and will be recognized by pseudonym on next login
- pseudonym / sector specific identifier is e-service dependent. An user cannot be tracked across service boundaries.

Use Case 1

Verification of residence

- the residence of a user can be verified to be a specific city / place, without disclosure of concrete residence
- can be used for instance in eGovernment-portals

Use Case 2

Age verification

- age of the user could be verified
- some services require a certain minimum-age to be accessed

Ongoing Work

- access software to the data on the German ID card is under development
- Protection Profiles are under development
- conformance to a testbed must be proofed
- CC EAL 4 evaluation certified by BSI
- confirmation to German signature law (SigG) by BSI

application tests will be starting autumn 2009

ID card will be available from 2010-11-01

Thanks for your attention

Dr. Klaus Lüttich
bremen online services GmbH & Co. KG
Am Fallturm 9
28359 Bremen, Germany
Phone +49 421 20495 - 70
E-Mail kl@bos-bremen.de