Towards GDPR, eIDAS and PSD2 as a Service

Dr. Detlef Hühnlein, ecsec GmbH
Agenda

- Introduction
  - Background
    - Strong Authentication in the Cloud
    - GDPR
    - eIDAS
    - PSD2
  - Towards GDPRS, eIDAS and PSD2 as a Service
- Summary
ecsec GmbH – competences

- IT-Security
- Identity Management
- Electronic Signatures
- Smart Card Technology
- Cloud Services
- Open Source
- Security Management
- Mobile Solutions
- eGovernment

www.ecsec.de
Agenda

- Introduction
- Background
  - Strong Authentication in the Cloud
    - GDPR
    - eIDAS
    - PSD2
- Towards GDPR, eIDAS and PSD2 as a Service
- Summary
Authentication in the Cloud

1. Client sends a request to SP.
2. SP sends an IS to the Client.
3. IdP sends an IS to the Client.
4. Client sends an IS to the IdP.
5. IdP sends an IS to the SP.
6. SP sends an IS to the IdP.
7. IdP sends an IS to the SP.
8. SP sends an IS to the IdP.

IdP

SP
Strong Authentication in the Cloud

- EAC (BSI-TR-03110)
- C2C (EN 14890)
- TLS (RFC 5246)
- HOTP (RFC 4226)
- FIDO U2F

IdP

Client

SP
Agenda

- Introduction
- Background
  - Strong Authentication in the Cloud
  - GDPR
  - eIDAS
  - PSD2
- Towards GDPR, eIDAS and PSD2 as a Service
- Summary
General Data Protection Regulation (GDPR)

- Regulation (EU) 2016/679
- aka „General Data Protection Regulation“
- Entry into force on 25 May 2018
- Various new, and sometimes challenging requirements, with respect to data protection
GDPR at a Glance

Fines up to 20 Mio € (or 4% of turnover)

State of the Art Security

Privacy by Design

Accountability

Consent

Data Export (e.g. XML, JSON)

Agenda

- Introduction
- Background
  - Strong Authentication in the Cloud
  - GDPR
  - eIDAS
  - PSD2
- Towards GDPR, eIDAS and PSD2 as a Service
- Summary
eIDAS-Regulation

- Regulation **(EU) 2014/910** on electronic identification (eID) and trust services for electronic transactions aka „eIDAS-Regulation“
- In force since **17 September 2014**
- Mutual recognition of notified eID schemes
- Legal framework for trust services for
  - electronic signatures and seals (generation and validation)
  - certificates for signatures, seals and website-authentication
  - time stamps
  - new trust services for
    • validation
    • preservation and
    • electronic delivery
eIDAS-related Implementing Acts

- **2015/1501/EU**: eID Interoperability Framework and Voluntary Recognition of eID
- **2015/1502/EU**: eID Assurance Levels
- **2015/296/EU**: eID Collaboration
- **2015/1984/EU**: eID Notification
- **2015/806/EU**: Trust Mark
- **2015/1505/EU**: Trusted List
- **2015/1506/EU**: AdES Formats
- **2016/650/EU**: QSCD Security Assessment

*(EU) No 910/2014 fully applicable as of 2016/07/01*

*https://eid.as*
eIDAS-Ecosystem

https://blog.skidentity.de/en/eidas-ecosystem/
eIDAS-TSP-Map

https://eid.as/tsp-map
Agenda

- Introduction
- Background
  - Strong Authentication in the Cloud
  - GDPR
  - eIDAS
  - PSD2
- Towards GDPR, eIDAS and PSD2 as a Service
- Summary
Payment Services Directive 2 (PSD2)

- Directive (EU) 2015/2366 on payment services aka „Payment Services Directive 2“ (PSD2)
- Requires Account Servicing Payment Service Providers (ASPSP) (e.g. Banks) to
  - apply strong customer authentication (Art. 97)
  - provide access to accounts (X2A) for other payment service providers such as
    - Payment Initiation Service Provider (PISP) (Art. 66)
    - Account Information Service Provider (AISP) (Art. 67)
    - Payment Card Issuer (PCI) (Art. 65)
Outline of PSD2 System Architecture

Payment Service User (PSU) (User)  

Account Servicing Payment Service Provider (ASPSP) (Identity Provider)

Accessing Payment Service Provider (XPSP) (Service Provider)

Strong Authentication

Steps:
1. Request from PSU to ASPSP
2. ASPSP validates PSU's identity
3. PSU authenticates with ASPSP
4. ASPSP requests payment data from XPSP
5. XPSP provides payment data to ASPSP
6. ASPSP provides payment data to PSU
Agenda

- Introduction
- Background
  - Strong Authentication in the Cloud
  - GDPR
  - eIDAS
  - PSD2
- Towards GDPR, eIDAS and PSD2 as a Service
- Summary
SkIDentity – GDPR, eIDAS and PSD2 as a Service
Supported eID and Authentication Means
SkIDentity – Patented Authentication Technology

EN 2439900

Service Provider

User
Seals, Accreditations and Certifications

- BVA Authorization Certificate according to § 21 PauswG
- BSI TR-03124 Certificate for Open eCard App 2015
- ISO 27001 based on BSI Baseline Protection for „Secure Cloud Infrastructure (SkIDentity)“ (BSI-IGZ-250)

“Trusted Cloud Data Protection “ Certificate for „SkIDentity-Service“
Agenda

- Introduction
- Background
  - Strong Authentication in the Cloud
  - GDPR
  - eIDAS
  - PSD2
- Towards GDPR, eIDAS and PSD2 as a Service
- Summary
Summary

- GDPR imposes new requirements, which should better not be neglected
- eIDAS provides framework for eID and trust services for electronic transactions
- PSD2 is expected to redefine the relationship between customers, banks and related service providers throughout Europe
- eID and 2FA is the intersection of GDPR, eIDAS and PSD2

SkIDentity provides GDPR, eIDAS and PSD2 as a Service!
Thank you very much for your kind attention!

Contact

c/o ecsec GmbH
Sudetenstraße 16
96247 Michelau, Germany
Phone +49 9571 604 8014
Mobile +49 171 9754980
detlef.huehnlein@ecsec.de

Dr. Detlef Hühnlein
CEO / Project Manager