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 GDPR, 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
Agenda

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

IdP

Client

SP

1. IS

2. IS

3. IS

4. IdP

5. IdP

6. IS

7. IS

8. IS

© 2017 ecsec GmbH
www.skidentity.com
Strong Authentication in the Cloud

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

Client

IdP

IS

SP

SAMLA v2.0

© 2017 ecsec GmbH
www.skidentity.com
Agenda

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

- Art. 5 Principles relating to personal data processing
- Art. 6 Lawfulness of processing
- Art. 7 Conditions for consent
- Art. 8 General conditions for imposing administrative fines
- Art. 9 Processing of special categories of personal data
- Art. 17 Right to erasure (‘right to be forgotten’)
- Art. 20 Right to data portability
- Art. 25 Data protection by design and by default
- Art. 28 Processor
- Art. 32 Security of processing
- Art. 83 General conditions for imposing administrative fines
- Accountability
- Consent
- Data Export (e.g. XML, JSON)
- Fines up to 20 Mio € (or 4% of turnover)
- Privacy by Design
- State of the Art Security

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

- **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
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 by:

Federal Ministry for Economic Affairs and Energy

on the basis of a decision by the German Bundestag

SkIDentity Service

SecurITy

powered by esec

Service Provider

User

© 2017 ecsec GmbH

www.skidentity.com
Supported eID and Authentication Means
SkIDentity – Patented Authentication Technology

Supported by:

- Federal Ministry for Economic Affairs and Energy

EN 2439900

Service Provider

User

...
Awards

- Germany Land of Ideas Landmark 2013/14
- Trusted Cloud Award 2011
- Bavarian Innovation Award 2016
- EuroCloud Award 2015
- Landmark 2015 in the Land of Ideas

- EuroCloud Germany Award 2015
- Landmark 2015 in the Land of Ideas
- EuroCloud Europe Award 2015
Seals, Accreditations and Certifications

BSI TR-03124 Certificate for Open eCard App 2015

BVA Authorization Certificate according to § 21 PauswG

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