



**Fast Electronic Identification
at Trust Substantial Level
using the Personal Bank Account**

Prof. Michael Massoth, Sam Louis Ahier

Hochschule Darmstadt - University of Applied Sciences



- **Darmstadt** is between Frankfurt am Main and Heidelberg.
- **Hochschule Darmstadt** has about 15,000 students in total.
- With about **1,600** students one of the largest Departments of Computer Science in Germany.

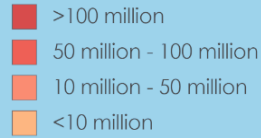
Introduction



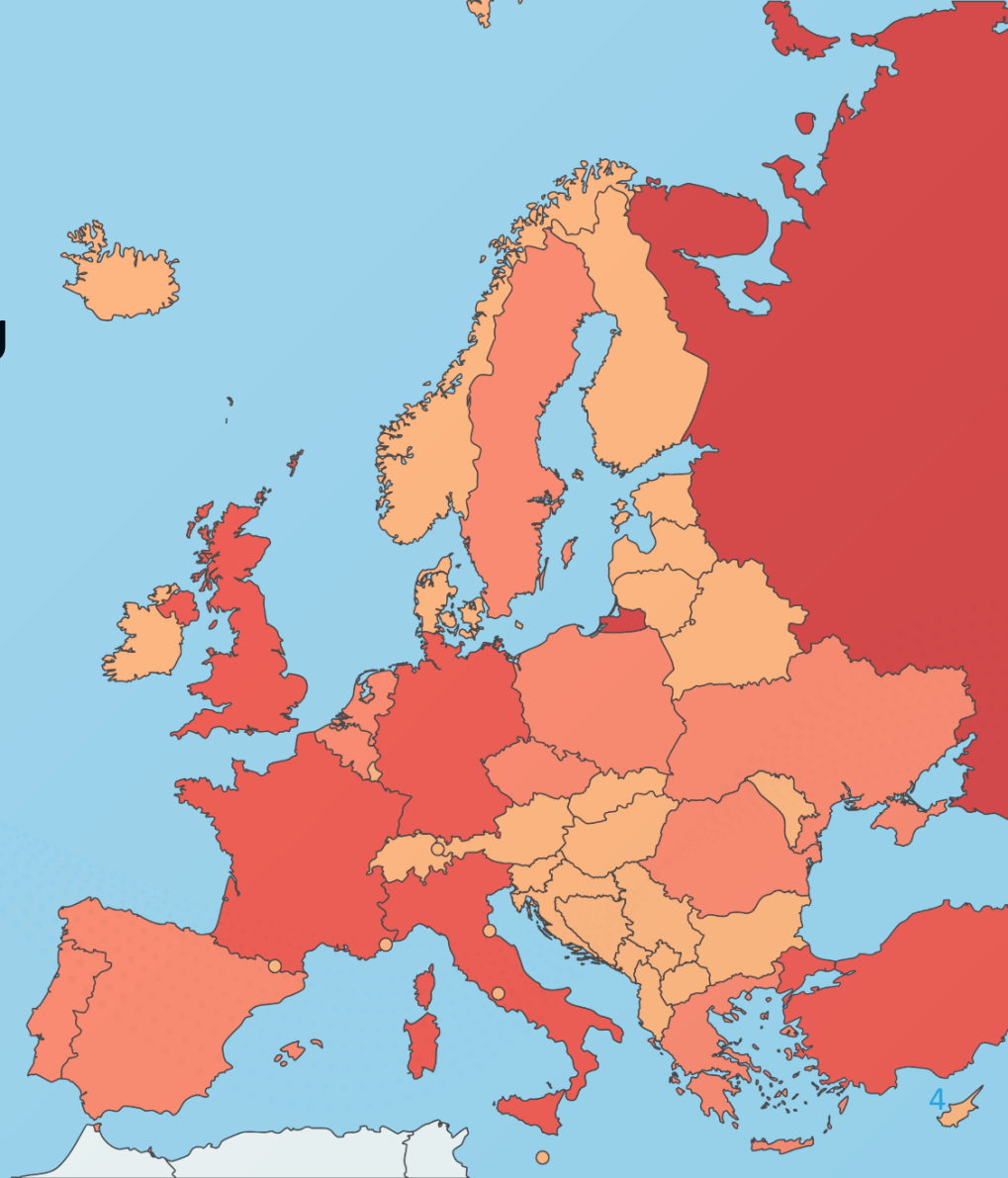
Online Identification should be:

- Fast
- Simple
- Not require additional Hardware
- Available 24/7

European countries by
population, 2018



- Over **440 million** people live in the EU
- **54%** of all people have access to online banking (*EBF, 2018*)
- More than **240 million** registered online banking accounts



Current Methods



Postal Identification

Requires you to physically go to the nearest postal office can take days/weeks.



Video Identification

May have long queue and relies on employees and AI to authenticate you.







eID-Card Identification

Requires you to have additional, possibly expensive, hardware.



Regulations & Directives

-  Electronic Identification, Authentication and Trust Services (eIDAS)
-  Payment Service Directive 2 (PSD2)
-  German Money Laundering Act (GwG)
-  General Data Protection Regulation (GDPR)



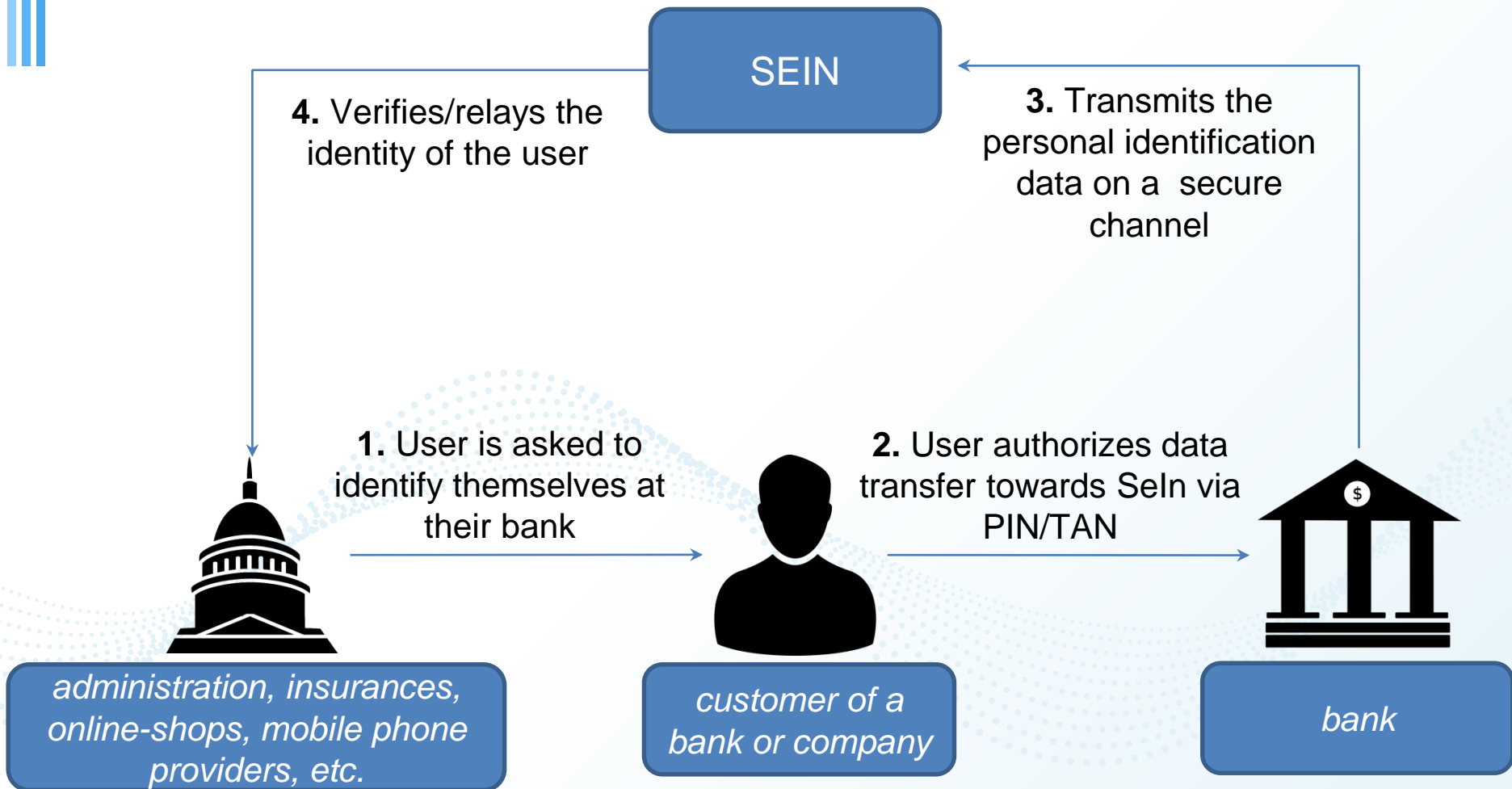
Protocols & Tools

⚙️ Access to Accounts (XS2A)

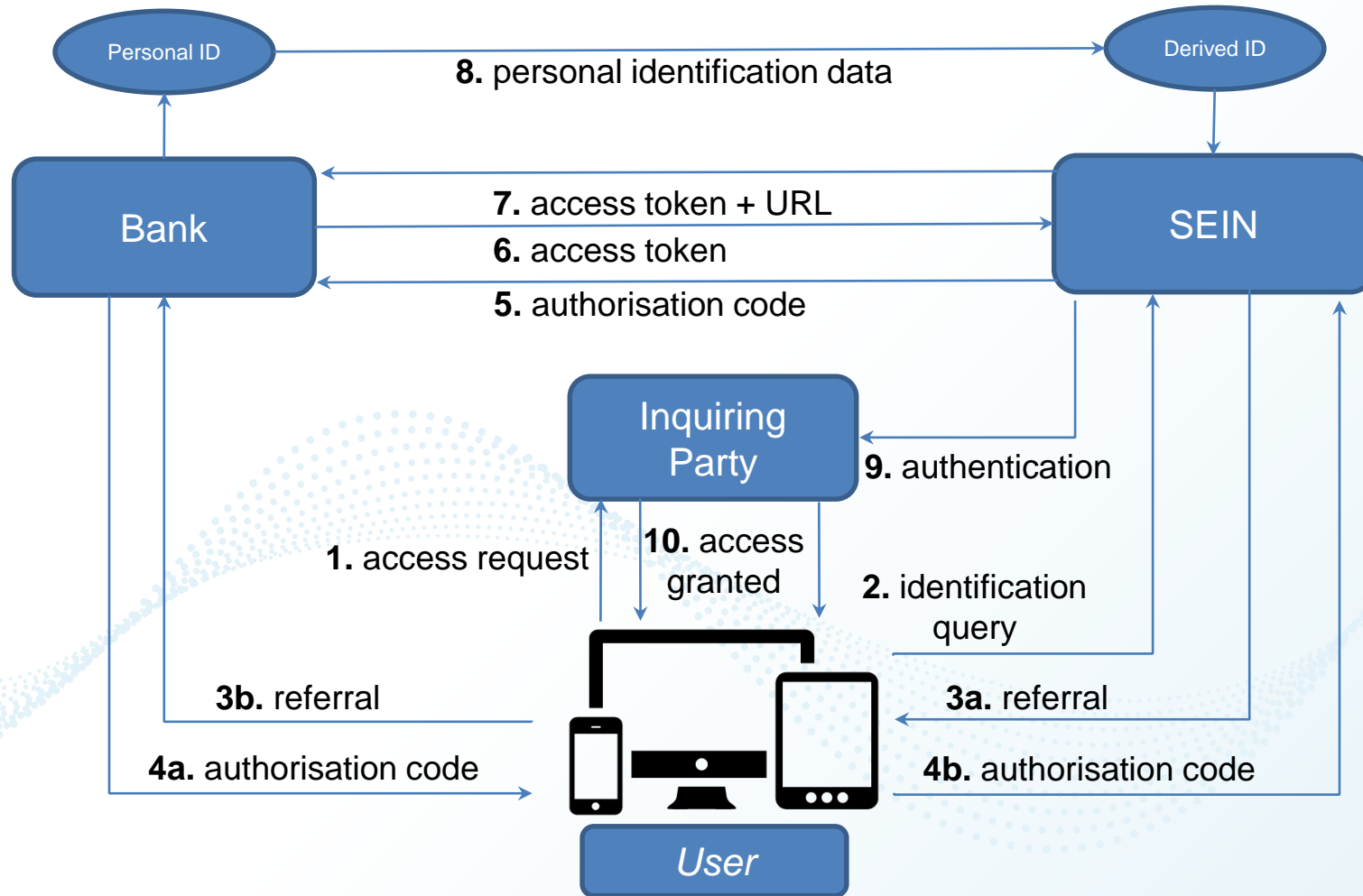
⚙️ OAuth 2.0 protocol

⚙️ OpenID Connect

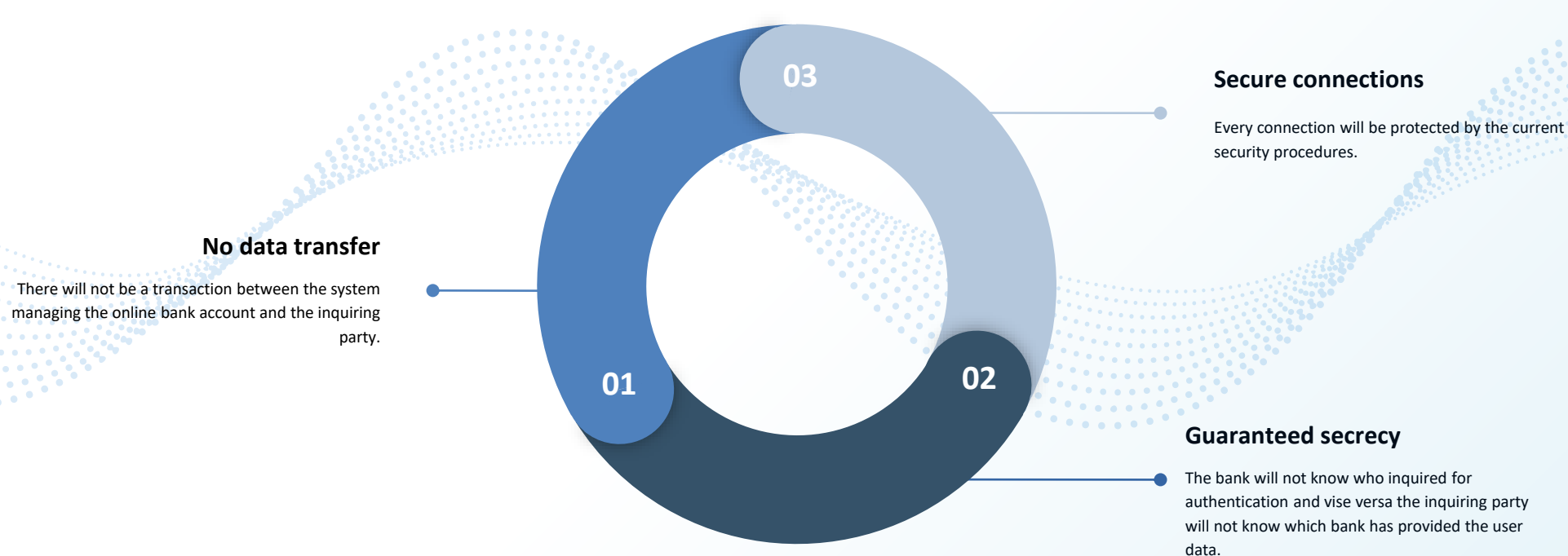
Approach of deriving an identity



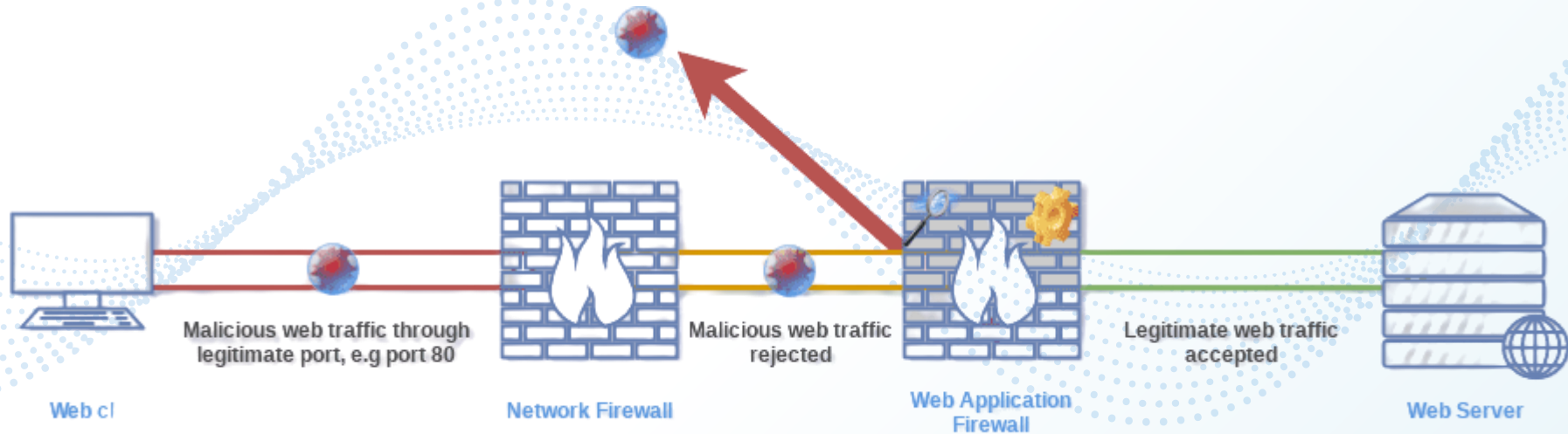
Detailed process of deriving an identity



Security and privacy by design

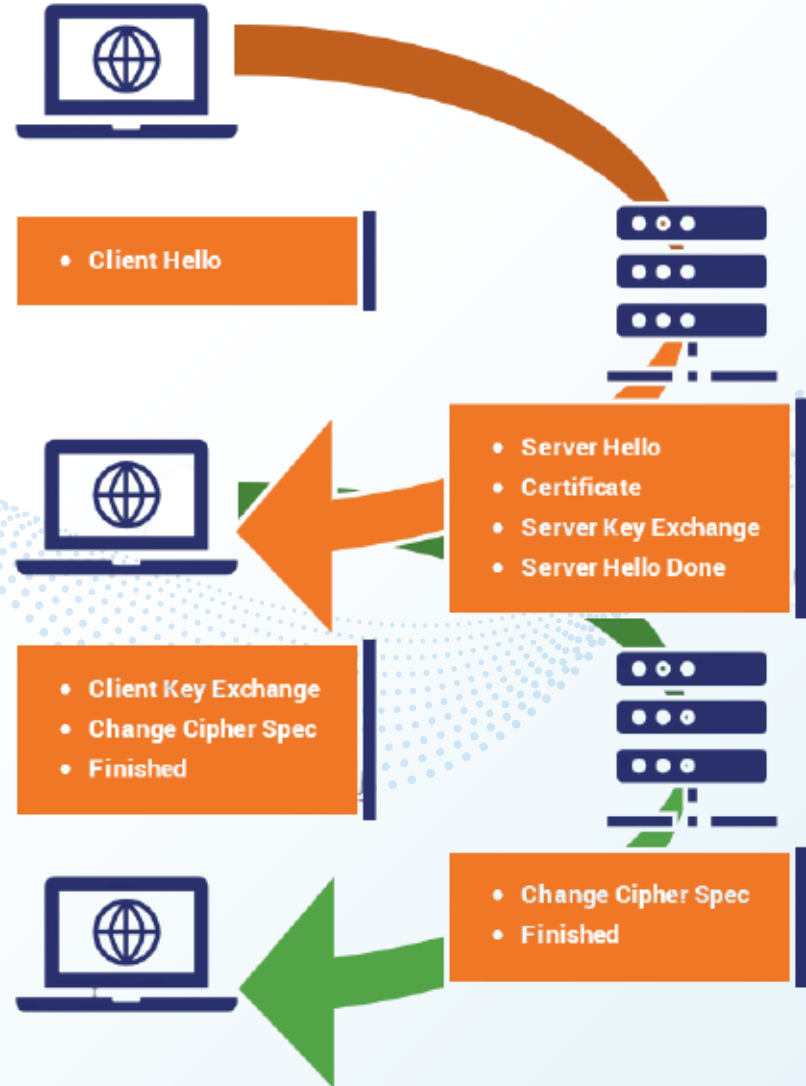


Security Concept



Security Concept

- rely on TLS-certificates with Extended Validation
- Qualified Website Authentication Certificates (QWAC)



Related papers

“Analysing the Security of Google’s Implementation of OpenID Connect”

by W. Li, C. J. Mitchell, and T. Chen

“OpenID Connect Security Considerations”

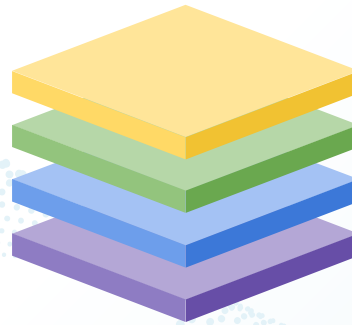
by V. Mladenov and C. Mainka

“Securing Digital Identities in the Cloud by Selecting an Apposite Federated Identity Management from SAML, OAuth and OpenID Connect”

by N. Naik and P. Jenkins.

“SoK: Single Sign-On Security – An Evaluation of OpenID Connect”

by C. Mainka, V. Mladenov, J. Schwenk, and T. Wich





Conclusion

We hope to innovate the way online authentication works.

The start-up SEIN has begun to implement the ideas presented in this paper and is currently 2 months deep into its development.



Electronic Identification, Authentication and Trust Services (eIDAS)

- Regulation managing electronic identification and trust services for electronic transactions.
- Sets standards for electronic signatures, qualified digital certificates and other forms of proof of authentication.
- First introduced in the EU regulation 910/2014 and became effective on July 1st 2016.
- States that any organization that provides a public digital service must recognize electronic identification from all EU member states.



Electronic Identification, Authentication and Trust Services (eIDAS)

- eIDAS describes trust at substantial level as either:
 - 1) Trust level low and a verified possession of genuine evidence.
 - 2) Trust level low and an ID document is physically presented during registration process.
 - 3) Previously collected Data at substantial level of trust does not have to be re-entrusted.
 - 4) Identity Providers already at substantial trust level authentications provide the same level of trust.



Payment Service Directive 2 (PSD2)

- Revised Payment Services Directive or Payment Services Directive 2 (EU) 2015/2366 replaced the former EU Directive 2007/64/EC.
- Declares that any bank must grant customer Access to Account (XS2A) data to third party providers.
- The PSD2 establishes a framework within which all payment service providers must operate



German Money Laundering Act (GwG)

- Obligates every bank to properly authenticate the customer whenever they open a new bank account.
- Aims to prevent money laundering and terrorist funding.
- Was passed in June 2017
- Stipulates the data which must be gathered and verified for both the natural person and the legal person. (e.g. first name and surname, place and date of birth, nationality, etc.)



General Data Protection Regulation (GDPR)

- Has been law since April 2016.
- Regulates the consequences if the held data is ever jeopardized.
- Sets rules for organizations and companies forcing them to take the protection of personal data seriously.



Access to Accounts (XS2A)

- Denotes the API financial establishments can use to implement certain online-banking-features.
- Enables third party providers to give non-discriminatory access to the linked customer account.
- Makes administering multiple accounts distributed among different banks within one central software solution possible.



OAuth 2.0 protocol

- Inhibits the theft of a user session.
- Framework enabling a third party entity to obtain limited access to an HTTP Service.
- Ensures no unknown third entity can impersonate our service to steal data.
- Introduces an authorization layer which separates the role of the client from that of the end user.
- Supports Transport Layer Security (TLS) 1.3.



OpenID Connect

- Is based on the OAuth 2.0 protocol with the extension of a JSON web token.
- Enables clients of all sorts, such as web based, mobile and JavaScript-Clients to receive data.
- Optimizes the OAuth-authentication process and extends it with the necessary functions for Login and Single Sign-On.