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

Michael Massoth, Sam Louis Ahier
Department of Computer Science
Hochschule Darmstadt – University of Applied Sciences
Darmstadt, Germany
E-mail: michael.massoth@h-da.de, sam.ahier@stud.h-da.de

***Abstract*—In the era of digitization, proper online authentication is as important to public administration as it is to the economy. In the past, different solutions have been developed, such as postal authentication, identification by video or by eID-Cards. All of these solutions either take days or even weeks, rely on human interaction or require additional, possibly expensive, hardware. At the current moment there is a lack of a fast, automated, secure and most importantly simple process to properly authenticate yourself online. Therefore, fast electronic identification (SEIN) has conceptualized a new way of automatically authenticating natural and legal entities, using tokenization and already authenticated data sets collected by financial institutions as a result of the German Money Laundering Act (GwG) which are made accessible through the Payment Service Directive (PSD2) using well known and widely used technologies such as OAuth 2.0, OpenId Connect and Transport Layer Security (TLS) 1.3. The startup company SEIN aims to provide fast authentication at substantial trust level without collecting any data from the user and without a data transfer between the bank and the inquiring entity. The bank will not know who made the request for authentication and vice versa, the inquiring party will not know which bank has provided the user data. In this paper, we will go into more detail on how SEIN plans to provide a new and innovative way to authenticate yourself online.**

Keywords-authentication; identity management; tokenization; substantial trust level; Payment Service Directive 2.

I. INTRODUCTION

Registering for insurance, getting a new mobile phone contract or paying a mortgage online and many other online services as shown in Figure 1 require you to authenticate yourself. The commonly used methods for online authentication are postal identification, video identification or identification via electronic Identification (eID) Card. Waiting for the posted authentication documents, queuing up for an online video conference with an employee of an identification provider while possibly relying on an unstable Internet connection or needing specific and potential expensive hardware takes a heavy toll on the overall user experience and usability.

Our goal is to make online identification more easily accessible, not only in Germany but in Europe. Our solution requires no hardware, doesn't involve any human contact and most importantly aims to provide authentication within minutes instead of days or weeks. The only requirement is that the person requiring authentication has access to an online banking account. According to the European Banking Federation (EBF) that means more than half the population (54%) of the EU (state of 2018) [1]. This means there are more than 240 million [2] registered online bank accounts, which have already been properly authenticated. This figure has been increasing steadily for years and it is assumed that it will continue to increase in the future.

Figure 1. Possible applications of SEIN [4].

Why identify manually, if you could use the already authenticated data sets from a trustworthy institution? We aim to provide a fully automated electronic identification, authentication and trust service. Our service is compliant at the substantial trust level with the regulations of the electronic Identification, Authentication and trust Services (eIDAS) [3] while only using the data provided by the already authenticated identities from financial institutions. The eIDAS Commission implementing regulation (EU) 2015/1502 [5] specifies the criteria for trust and security at substantial level. Trust at substantial level can be achieved by guaranteeing trust at low level plus one of the 4 listed points:

(1) The person has been verified to be in possession of evidence when applying for the electronic identity and the evidence is checked to be genuine or according to an authoritative source is known to exist and relate to a real

person and steps have been taken to minimize the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence.

(2) An identity document is physically presented during a registration process and steps have been taken to minimize the risks of known identification fraud as mentioned above.

(3) Procedures used previously by an company or entity for a purpose other than the issuance of electronic identification provide for an equivalent assurance to those set in the points listed above, do not have to be repeated provided such equivalent assurance is confirmed by a conformity assessment body or an equivalent body.

(4) The electronic identification requests are issued on the basis of a valid notified electronic identification provider having the assurance level substantial or high, and taking into account the risks of known identification fraud, namely the risk of lost, stolen, suspended, revoked or expired evidence. The assurance level must be confirmed by a conformity assessment body or an equivalent body.

The account holding bank has to fulfill all the prerequisites that the eIDAS regulation establishes. So, we can assume a trust level of substantial or higher as a result of regulations such as eIDAS, the Money Laundering Act (GwG) [6] and the General Data Protection Regulation (GDPR) [10] in place. The GwG requires each financial institution to properly check the authenticity of an account when opened and to make sure that the presented authentication is at minimum risk of known identification fraud.

Furthermore, the Interpretation and Application Guide in relation to the German Money Laundering Act [8] states, that the verified identities can be used as proof of identity for third parties. Henceforth, SEIN will use the data already securely collected by financial institutions and thanks to the guarantee provided by the eIDAS regulation provide a level of trust equal to that provided by the financial institutions.

The identifying data is accessible via a corresponding Application Programming Interface (API), which has to be provided according to the Payment Service Directive 2 (PSD2) [7]. The access to the saved data is usually secured via a strong two-factor authentication using a Personal Identification Number (PIN) and a Transaction Authorization Number (TAN), thus providing us with a legitimization check.

Not only is the data we access already verified to be secure and at least at substantial trust level but SEIN plans on being ISO 27001 [9] certified. This will ensure an even higher level of security, a functional Information Security Management System (ISMS) and will also add to our compliance to the GDPR.

In Section I we provide an introduction. Section II gives additional information about the directives and regulations we reference and apply. Section III outlines how SEIN plans on deriving an identity at a modular level as well as an example of a web service. Section IV states our approach to privacy by design. The conclusion lists some of our goals for the future, and the acknowledgements close the paper.

II. TERMINOLOGY

A. *Electronic Identification, Authentication and Trust Services [2]*

eIDAS is an EU regulation managing electronic identification and trust services for electronic transactions in the European Single Market and the European Economic Area. It was first introduced in the EU regulation 910/2014 and became effective on July 1st 2016. It states that any organization that provides a public digital service must recognize electronic identification from all EU member states, provided that the provider meets the established eIDAS standards.

It also sets standards for electronic signatures, qualified digital certificates, electronic seals, timestamps and other forms of proof of authentication to give them an equal legal standing as the transactions performed on paper. Moreover, eIDAS introduces three levels of assurance namely low, substantial and high to better assess the security different authentication services provide.

B. *Payment Service Directive 2 [7]*

Revised Payment Services Directive or Payment Services Directive 2 (EU) 2015/2366 replaced the former EU Directive 2007/64/EC to expand the pan-European competition and participation in the financial industry, not exclusively limit to banks by coordinating consumer protection and defining rights and obligations for payment providers and users. The PSD2 establishes a framework within which all payment service providers must operate.

Most importantly for us, the PSD2 regulation declares that any bank must grant customer Access to Account (XS2A) data to third party providers.

C. *Access to Accounts [11]*

XS2A is the abbreviation used to express Access to Accounts and denotes the API financial establishments can use to implement certain online-banking-features. The API enables third party providers to give non-discriminatory access to the linked customer account. This also makes administering multiple accounts distributed among different banks within one central software solution possible.

It is expected that that different financial establishments will harmonize their API access to further enhance the user experience. While there have already been some amalgamating actions, it is still an ongoing process.

D. *German Money Laundering Act [6]*

The German Money Laundering Act (GwG german: Geldwäsche Gesetz), which was passed in June 2017, obligates every bank to properly authenticate the

customer whenever they open a new bank account. This is to prevent money laundering and terrorist funding. The GwG stipulates the data which must be gathered and verified for both the natural person and the legal person.

Natural person:
- first name and surname
- place of birth
- date of birth
- nationality
- residential addresses

Legal person or company:
- company or trading name
- legal form
- commercial register number (if available)
- address of registered office/head office
- name of the members of its representative bodies/ names of its legal representatives
- name of owner (additional data from owner may be required)

E. International Standard for Organization 27001 [9]

Published in 2005 and revised in 2013 the International Standards Organization (ISO) 27001 is the international standard on how to manage information and data security.

To achieve our goal of trust at substantial level we have to prove that, we meet the requirements of ISO 27001 and this has to be verified by a neutral entity. Therefore, not only will SEIN need an Information Security Management System (ISMS) that ensures that the information security controls continue to meet our organization information security needs but also systematically examine our information security risks in regards to threats, vulnerabilities and impacts.

F. General Data Protection Regulation [10]

The General Data Protection Regulation has been law since April 2016 and regulates who the GDPR applies to and the consequences if the held data is ever jeopardized. The mainstay of the GDPR is a rule set for organizations and companies forcing them to take the protection of personal data seriously.

III. APPROACH IN DETAIL

A. Concept of deriving an identity

A schematic overview, on how inquiring mandates verify the identification of a customer is shown in the Figure 2 below. First, the customer has to select the bank which will provide the authorization. The authorization works via a strong 2-factor-authentication, (eg. PIN/TAN). After a successful authentication, the bank forwards the personal identification data which in the final step will authenticate the user.

SEIN will not require any additional hardware, which will greatly improve the user experience since there are no media discontinuities. Furthermore the encryption and the reliability of the data of the financial institutions provide us with a high level of security. Finally, SEIN plans on maximizing the level of automation, so the service can be available 24/7 without any human interaction.

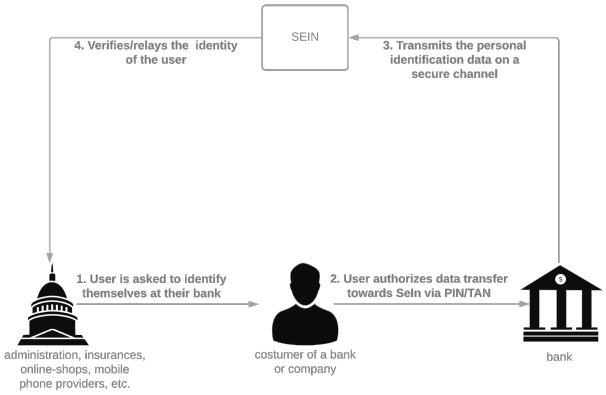

Figure 2. Approach of deriving an identity.

This should mean that there is no queue time and the cancellation rate should be minimal since the internet connection has only got to send and receive small data packages. The planned maximal time it should take to verify an identity is 90 seconds, thus greatly increasing the overall user experience.

B. Derived identification

The main idea is to use a derived identity, to ensure that SEIN never has access to critical data. This differentiates our solution from other methods such as Screen Scraping. We never have access to the users TAN and/or PIN.

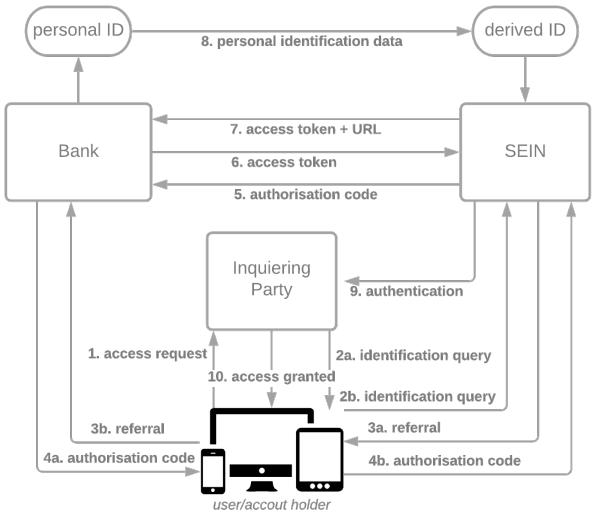

Figure 3. Detailed process of deriving an identity.

The process of deriving an ID is as follows (using the example of a Web service) as shown in Figure 3:

(1) A user or an account holder requests access to a service, which requires authentication.

(2) The inquiring party will be forwarded to our service (SEIN) by their web browser.

(3) Our service will request the user to select their bank; they will then be redirected to the financial institution of their choice.

(4) The user logs into their online banking account. This process may differ for different financial institutions, but most of the time a PIN and a TAN are required. The TAN in this case is used as the verification to verify the users agreement for his personal data to be transferred to the potential mandate/entity. Upon properly authenticating themselves, an authorization code will be sent back from the bank to the users web browser and then transparently passed onto our service.

(5) SEIN forwards the received authorization code to the bank.

(6) The received authorization code will be then be automatically exchanged for an access token and sent back from the bank to SEIN.

(7) As part of the automated process the access token and the URL will be sent to the bank. So that the authentication data required can be fetched by the bank.

(8) The personal identification data will then be sent back by the bank to SEIN as a derived ID.

(9) Finally, the website requesting authentication for the user will receive said authentication from SEIN.

(10) Access to the requested service is granted to the user.

C. Security analysis and evaluation

The technical security measures are implemented by the OAuth 2.0 protocol [12]. The protocol inhibits the theft of a user session. Additionally it ensures no unknown third entity can impersonate our service to steal data. Its framework enables a third party entity to obtain limited access to an HTTP Service. In order not to store critical data, gain undue access to the users protected resources or to comprise any passwords from the user OAuth 2.0 has introduced an authorization layer which separates the role of the client from that of the end user [15]. Furthermore OAuth 2.0 supports Transport Layer Security (TSL) 1.3 and is compliant with the most up-to-date data protection standards.

Our start-up project also uses OpenID Connect [13] for a fast proof of identity. OpenID Connect is based on the OAuth 2.0 protocol with the extension of a JSON web token which we use for further authentication. These protocols and frameworks enable clients of all sorts, including but not limited to web based, mobile and JavaScript-Clients to receive information about authenticated sessions and users. As a result OpenID Connect optimizes the OAuth-authentication process and extends the OAuth2.0 protocol with the necessary functions for Login and Single Sign-On.

In our search as part of the preparation for the first security evaluation we found 4 papers discussing the security of OpenID. In the following section we will provide a short summarization of each of the papers.

The first paper is “Analysing the Security of Google’s Implementation of OpenID Connect” [18] which was the first field study in this field. It examined 103 of the relying parties (RP) that implemented the Google OpenID service, revealing a series of vulnerabilities of a number of types. It provides recommendations for both RPs and OpenID Provider (OP) to improve the security of the OpenID Connect systems. These enhancing recommendations for the RPs include not customizing the Hybrid Server-side Flow, taking countermeasures to Cross-Site-Request-Forgery (CSRF) attacks and improving the use of *state value* to not be predictable. The OPs are advised to remove the token from the authorization request in the Hybrid Server Flow and add a state value in the sample code.

In “OpenID Connect Security Considerations” the authors Vladislav Mladenov and Christian Mainka [19] examine specification and implementation (client and Identity Provider side) flaws. For each flaw they list different kinds of possible attacks. For example the specification flaws open OpenID Connect up for 4 attacks using the malicious Discovery service: the Broken End-User Authentication, the Server Side Request Forgery (SSRF), the Code Injection Attack and the Denial-of-Service (DoS) Attack. The paper also highlights the problem of Session Overwriting and Identity provider (IdP) Confusion.

The third paper was “Securing Digital Identities in the Cloud by Selecting an Apposite Federated Identity Management from SAML, OAuth and OpenID Connect” [20] by Nitin Naik and Paul Jenikins. It assesses 3 different Federated Identity Management (FidM) standards, namely Security Assertion Markup Language (SAMPL), OAuth and OpenID Connect (OIDC), on architectural design, working, security strength and security vulnerability to ascertain effective usages for secure online identification. It compares these three standards in depth to help other FidM users and researchers to select an apposite FidM service for their projects.

The final paper “SoK: Single Sign-On Security – An Evaluation of OpenID Connect” [21] categorized known attacks on Single-Sign-On (SSO) into two classes: Single-Phase Attacks which abuse the lack of single security checks and Cross-Phase Attacks which require a complex setup and a manipulation of multiple messages during the entire protocol workflow. Furthermore the paper provides an evaluation of official open source OpenID libraries and worked with the corresponding developers to help them fix the issues. From this paper we have identified the OpenID-Connect-Service-Libraries “MITREid Connect” and “Ruby OpenID Connect” as secure candidates. These two libraries are secure against all known SSO Single-Phase Attacks and

Issuer Confusion Cross-Phase Attacks. In the case of attacks abusing specification flaws such as IdP Confusion all tested libraries were vulnerable. This is because even a correct implementation, following every rule is still susceptible.

D. Security concept

To further secure the platform we plan to also use a network firewall, as well as a Web Application Firewall (WAF), similar to Apache-webserver using ModSecurity or nginx-webserver using NAXSI. The identification through SEIN as an identity provider will exclusively rely on TLS-certificates with Extended Validation, which we plan to archive through Qualified Website Authentication Certificates (QWAC) according to eIDAS and the BaFin / PSD2-Registration-KID. Qualified Website-TLS-Certificates used to authenticate and encrypt the communication for applications implementing the PSD2-policy can be acquired through D-Trust (Bundesdruckerei). To ensure the integrity of the IT-based-processes our Information Security Management System (ISMS) must fulfill all the ISO/IEC 27001/2013 requirements set by IT-Grundschutz Methodology/BSI-Standard 200-2 [16]. Additionally the Technical Guideline TR-03147 Assurance Level Assessment of Procedures for Identity Verification of Natural Persons [17] requires an identity provider, especially the E-Government ones, to be ISO/IEC 27001 certified.

IV. Data protection

A. Privacy by design

There will not be any data transfer between the system managing the online bank account and the inquiring party. Therefore, the bank will not know who inquired for authentication and vise versa the inquiring party will not know which bank has provided the user data. This guarantees the highest level of data protection and privacy by design. All the data of the user required for authentication is already stored by the financial institutions. A derived version of that data will be sent to the requesting entity. Every connection will be protected by the current security procedures.

Our start up fulfills every requirement set by the GDPR, and also established a compliance-, a data protection and a GwG detection management.

Conclusion and future work

The regulations and directives provide us with the necessary information we need to authenticate an entity. With this legal foundation (eIDAS, GwG, GDPC, PSD2), the secure technologies we plan on using (OAuth 2.0, OpenID Connect, TSL 1.3) and the measures we take to secure our product (ISO 27001), 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 development. Evaluations and results will be part of another paper, to be expected at the end of next year (2021).

Acknowledgment

The authors would like to thank Jan Roring and Alexsander Küchler [14] who summarized much of the here presented information. Additionally this work is supported by the German Federal Ministry of Education and Research (BMBF), Project "Schneller elektronischer Identitätsnachweis auf Vertrauensniveau „substanziell" .

References

[1] *European Banking Federation Press Release, "Banking in Europe: EBF publishes 2019 Facts & Figures", 2019 [https://www.ebf.eu/ebf-media-centre/banking-in-europe-ebf-publishes-2019-facts-figures/], [retrieved September 2020]*

[2] *Eurostat, "Size and Population", [https://ec.europa.eu/eurostat/databrowser/bookmark/c0aa2b16-607c-4429-abb3-a4c8d74f7d1e?lang=en], [retrieved September 2020]*

[3] *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, [https://eur-lex.europa.eu/eli/reg/2014/910/oj], [retrieved September 2020]*

[4] *The European Union Agency for Cybersecurity 'Enisa' Press, [https://www.enisa.europa.eu/news/enisa-news/a-digital-europe-built-on-trust], [retrieved September 2020]*

[5] *Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance, [https://eur-lex.europa.eu/eli/reg_impl/2015/1502/oj], [retrieved September 2020]*

[6] *Federal Financial Supervisory Authority, "Money Laundering Act" trans. Geldwäschegesetz GwG, [https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.html], [retrieved September 2020]*

[7] *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance) [https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32015L2366], [retrieved September 2020]*

[8] *Federal Financial Supervisory Authority, "Interpretation and Application Guidanceinrelation to the German Money Laundering Act" trans. "Auslegungs-und Anwendungs-hinweisezum Geldwäschegesetz", December 2018, [https://www.bafin.de/SharedDocs/Downloads/EN/Auslegungsentscheidung/dl_ae_auas_gw_2018_en.pdf], [retrieved September 2020]*

[9] *International Standards Organization, "ISO/IEC 27001", [https://www.iso.org/isoiec-27001-information-security.html], [retrieved September 2020]*

[10] *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies*

and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.)[https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1725], [retrieved September 2020]

[11] *finAPI, "Cost-efficient: PSD2 XS2A server (Access to Account) especially for banks", [https://www.finapi.io/en/finapi-psd2-xs2a-fur-banken/]*

[12] *OAuth, [https://oauth.net/2/]*

[13] *OpenID Connect , [https://openid.net/connect/]*

[14] *J. Roring and A. S. Küchler, "Fast Electronic Proof of Identity (SEIN), on trust substantial level. Documentation for a Master Project System Devolpment Class", trans. "Schneller elektronischer Identitätsnachweis (SEIN) auf Vertrauensniveau substanziell Dokumentation zum Masterprojekt Systementwicklung Zwischenstand & Erkenntnisse", May 2020, " unpublished.*

[15] *D. Hardt, Ed., "The OAuth 2.0 Authorization Framework", October 2012, [https://www.hjp.at/doc/rfc/rfc6749.html#sec_1]*

[16] *BSI-Standard 200-2: IT-Grundschutz-Methodology, 07.05.2018, Englisch Version of the BSI-Standard 200-2 [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.html], [retrieved September 2020]*

[17] *BSI, "Technical Guideline TR-03147 Assurance Level Assessment of Procedures for Identity Verification of Natural Persons" trans. "Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen (BSI TR-03147)" [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03147/TR03147.pdf?__blob=publicationFile&v=1], [retrieved September 2020]*

[18] *W. Li, C. J. Mitchell, and T. Chen, "OAuthGuard: Protecting User Security and Privacy with OAuth 2.0 and OpenID Connect. In Proceedings of the 5th ACM Workshop on Security Standardisation Research Workshop (SSR'19)." Association for Computing Machinery, New York, NY, USA, pp. 35–44. DOI:https://doi.org/10.1145/3338500.3360331*

[19] *V. Mladenov and C. Mainka, "OpenID Connect Security Considerations", Bochum, January 2017, Ruhr-Univeristät Bochum*

[20] *N. Naik and P. Jenkins, "Securing digital identities in the cloud by selecting an apposite Federated Identity Management from SAML, OAuth and OpenID Connect", 11th International Conference on Research Challenges in Information Science (RCIS), Brighton, 2017, pp. 163-174, doi: 10.1109/RCIS.2017.7956534.*

[21] *C. Mainka, V. Mladenov, J. Schwenk, and T. Wich, "SoK: Single Sign-On Security — An Evaluation of OpenID Connect," 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris, 2017, pp. 251-266, doi: 10.1109/EuroSP.2017.32.*