E-Identity Solutions in Europe

An european overview

Andrea Müller
Dr. Andreas Windisch
Digital identity solutions are essential for a European internal market. Europe can benefit from the existing experience and diversity of solutions in European countries. The present study examines the European e-identity landscape as well as success factors for high dissemination and acceptance. In addition to the ease-of-use, which is essential for e-identity solutions as a digital service, a clear focus on dedicated use cases and the rigorous development of use cases along the business model are essential for the success of those solutions.

Introduction

The increasing diversity and presence of online services is increasing the need for online, secure and trusted identities. In the context of eIDAS, public and national e-identity solutions are increasingly becoming visible. For example, following Germany, Italy launched the EU-wide peer review for the national e-identity system SPID at the end of last year. Other countries will follow. In addition, private-sector solutions, that do not necessarily want to play the role of a national e-identity scheme, are increasingly pushing into the field of vision of a broad public. There are a whole range of different solutions and initiatives across Europe: several solutions from individual companies, several initiatives in entire corporate sectors and solutions in cooperation between several companies.

In our post "E-Identity Initiatives - The European Way" we have already summarized the relevance and basic history of the topic e-Identity together with the current regulatory frameworks. This post was already based on the study we conducted on e-identity solutions in Europe, the results of which should now be examined in more detail in this post.

Theory Lessons: Today "e-Identity Vocabulary"

When talking about e-Identity, players from different domains meet with different perspectives and emphases. The topic is relevant to providers of technical infrastructure, public authorities, banks, industrial production, e-commerce and media companies. The diversity of perspectives additionally is reflected in different languages. Frequently, terms are used differently in the context of e-identity. Therefore, for the sake of common understanding, we start with a brief definition of the vocabulary used in both the study and in this post:

e-Identity means a physical and/or immaterial entity that contains personal identification data and is used for authentication in online services (as defined by
eIDAS Article 3, point 2). An ID means can thus for example be an ID card, as well as an electrified badge or even a Facebook account.

**e-Identity Provider** Are the publishers of the ID means under an ID scheme. For the German identity card, the ID provider is the respective national registration office, for a Facebook-account it is Facebook.

**e-Identity Scheme** Is the set of rules and technical standards for the execution of ID functions using the underlying ID systems. The electronic German ID card in combination with AusweisApp2 is such an e-identity scheme.

**e-Identity System** or Initiative Is a technical electronic identification system in which electronic means of identification are issued to natural or legal persons or natural persons representing legal persons (definition in eIDAS, Article 3, point 4). For example, Facebook is an ID system. If the system is still in development, we denote it as an e-identity initiative.

**Relying Party** Is a natural or legal person who trusts in electronic identification or trust service. Usually these are the service providers (e.g. an online retailer), which depend on an identification and thus integrate the ID system.

**Methodology of the study conducted**

In 2015, the Dutch Ministry of the Interior commissioned PBLQ, a Dutch e-Government-focused consultancy, to conduct a study on the e-identity solutions in selected EU countries, taking into account their political motivation to create the systems. A total of eleven European countries were examined: Austria, Belgium, Denmark, Estonia, France, Germany, Great Britain, Luxembourg, Netherlands, Portugal, Spain and Sweden. The focus of this study explicitly was on ID means belonging to a national ID scheme.

Analogous to this study, we also examined individual countries in Europe to find out which e-identity means (in this case, initiatives or systems) exist, and whether these are public, private or partnership-oriented models. The comparison of the two studies already allows an interesting temporal comparison. Thus, the identified systems or initiatives show that over the past two years, above all, the involvement of private-sector initiatives or public–private partnerships has increased significantly.

That is why, as part of our investigation, we also looked at ID means that do not necessarily belong to national ID schemes. Moreover, we have expanded the geographic scope of the study and analysed all European countries. In addition, we have taken account of
current developments in e-Identity Services and have differentiated the e-ID approach, as explained below.

**Classification in public vs. private sector solutions**

When classifying public or private ID means, we proceeded in the same way as the colleagues at PBLQ: We examined who is responsible for the creation, implementation and maintenance of the project, and who is in charge of direct control.

A public ID means is one for which the government of the respective country is primarily responsible for creation, implementation and maintenance as well as for directly controlling it.

A private ID means is one for which one or more private companies are primarily responsible for creation, implementation, and maintenance and for directly controlling it. If a private ID fund grants access to public services, the state's responsibility for controlling the ID means remains set.

An ID means of a public–private partnership (PPP) is one for which both the government of the respective country and one or more private companies are primarily responsible for creation, implementation and maintenance as well as for directly controlling it. Again, in case of granting access to public services by means of the ID means, the public control of the ID means is still set.

**Range of functions or added value**

When analysing the individual ID means, we examined which functionalities are supported, as these have a direct impact on the potential fields of application. For example, there are ID means that are aimed at the transfer of personal data in the sense of identification, but also those that additionally enable authentication in order to act as a universal key for a wide range of services. Others offer the possibility of specific data management or even the signing of electronic documents using a qualified electronic signature (QES).

The functional blocks examined are described below. If one of the examined ID-means fulfils these requirements, we have added this function block to the functionality of the ID-means.

1 - Identification - Is the provision and transfer of all application-related characteristics of an entity, here natural person (e.g. name, address, e-mail address) to the Relying Party. On the one hand, depending on the relying party and use case, the transferred data record can vary in scope; on the other hand, different levels of trust can be used. Metadata for subsequent authentications can also be transferred.
A - Authentication - Is the recognition (often following an initial identification) of a natural person - usually it is the login at a Relying Party. The ID means provides a technical solution, using which the user authenticates, whereby this user in consequence is legitimized by the Relying Party for a particular service. For this reason, we also include verification use cases in which the Relying Party transmits data to the e-identity provider for verification. Depending on the application, it can be a simple (one-factor) or two-factor authentication.

D - Data transfer - Some providers offer the possibility, given the consent of the user, to hand over personal data to the Relying Party that go beyond the data used for identification. This may, for example, also be context-related information.

T - Data Tracking - The exploitation of explicit and implicit transaction data of the user is of primary importance for some providers. For example, these may be solutions for digitally collecting tracking opt-ins offered in connection with the use of the ID means.

S - QES - In addition to digital identification, legally compliant digital consent is an essential element in creating a digital trust space. Some e-ID systems integrate the ability to sign digital documents. In this case, a qualified digital signature is used.

Overview of the European e-identity landscape

For the overview of the e-identity landscape, a total of 30 countries have been considered: the 28 countries of the European Union as well as Norway and Switzerland. During our research, we identified 94 e-Identity solutions, which we analyzed in more detail.

As described in our previous post ‘E-Identity Initiatives - The European Way’, the first steps towards the creation of digitally useable identities were the digitization of official identity means many years ago. So, it is not surprising that a large part of the identified e-identity solutions has just this origin: Our overview contains 48 governmental initiatives or solutions that are based predominantly on the publicly issued identification means; usually these are the national digital identity cards. However, some of these solutions also include the ability to perform identifications or verifications for less safety-related use cases without an identity card. In total, 43 private-sector initiatives or solutions are available, some of which also integrate state-owned identifiers for higher-value identifications. A total of 3 public-private partnerships were identified in which state and private sector partners offer a common solution.

The following infographic shows in which country only publicly or privately driven e-identity solutions can be used, where both governmental and private solutions are available or where no relevant solutions have been identified.
It can be observed that almost all the countries surveyed in the European Union meanwhile have provided digitally available ID means or have announced this at least in the short term. More and more private-sector offers are available in a large number of countries, in particular representatives from the banking sector are active here. In Germany, Finland and the Netherlands, public-private partnerships can also be found at national level.

Particularly noteworthy here are the Nordic countries, such as Denmark, Finland, Norway and Sweden, where the subject of e-Identity looks comparatively well-organized and is already in widespread use in society. For example, many of the aforementioned countries have developed the e-ID capability of their national identification means many years ago or formulated alternative offers. In Denmark this is NEM ID, in Finland FINeID and in Norway MinID, which has been issued to citizens as standard for many years. In addition, private sector solutions have emerged, such as TUPAS of the Finnish Bankers’ Association FFI, bankID in Norway and BankID in Sweden, in each case cooperations of the largest Norwegian and Swedish banks. Depending on the distribution of the available e-identity means, additional federation solutions are available, such as ID Porten in Norway, which ensures the interoperability of all available e-identity solutions. Thus, in each case separate e-identity ecosystems were established at an early stage that can be used for almost all governmental and economic matters, from simple log-on at energy and water suppliers or public transport services to the digital signature of documents and the digital declaration of intent for e.g., the submission of tax returns or transfers to the national registration office. In Denmark, citizens have been required by law since 2012 to handle official communication exclusively in digital form – a correspondingly widespread use is logical. It is close to 100% in Denmark, more than 60% in Finland and more...
than 70% in Norway and Sweden. An interesting insight into the digital normality of the Nordic countries is given in the FinTech Podcast # 136 "Payment in the Nordics" by colleagues from Arkrwright Consulting.

In the following, we specifically selected the DACH region and would like to describe the respective solution landscape in Germany, Austria and Switzerland as an example.

e-Identity in Germany

With the publication of the identity card in check card format with integrated RFID chip, Germany started in 2010 with the establishment of a state-owned e-identity scheme. The hardware and software for using the online ID function is provided by different companies, but the state has a control function. The solutions must meet the criteria specified. Although the dissemination of the e-ID means is large due to the attachment to the ID card, the usage is far below expectations. The reason for this was, among other things, the optional activation of the online ID function for citizens until last year. At least as strong an impact are the so far limited fields of application of the online identification function, in which the lack of incentive to use the function is to be seen.

<table>
<thead>
<tr>
<th>Product (alphabetical order)</th>
<th>Provider</th>
<th>Ownership</th>
<th>I</th>
<th>A</th>
<th>D</th>
<th>T</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>German e-Identity-Scheme based on german national ID card (nPA)</td>
<td>Germany</td>
<td>Public</td>
<td>x</td>
<td>x</td>
<td>-</td>
<td>-</td>
<td>x</td>
</tr>
<tr>
<td>Giropay-ID</td>
<td>Giropay GmbH</td>
<td>Private</td>
<td>-</td>
<td>x</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Helix Alpha (Release Alpha)</td>
<td>Blockchain Helix</td>
<td>Private</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Identity™ Giro</td>
<td>Identity Trust Management AG</td>
<td>Private</td>
<td>x</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IdentityOne (in development)</td>
<td>Orbiter GmbH</td>
<td>Private</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Logon-Allianz DEA (in development)</td>
<td>United Internet AG (Sponsor)</td>
<td>Private</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>-</td>
</tr>
<tr>
<td>PostID</td>
<td>Deutsche Post AG</td>
<td>Private</td>
<td>x</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>SmartWallet, SmartLogin (in development)</td>
<td>Jolocom GmbH</td>
<td>Private</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Verimi (in development)</td>
<td>Verimi GmbH</td>
<td>Private</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>YES (in development)</td>
<td>YES Europe GmbH</td>
<td>Private</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 1: Overview e-Identity-Initiatives and -systems in Germany / as of January 2018

In addition to the public e-identity scheme, private-sector solutions are also active in Germany. However, the functionality of the solutions is lower than that of the state scheme, they do not achieve digital identifications according to the provisions of the AML. With PostID, Deutsche Post has been offering a solution since 2015 that enables customers to archive the identity data after an initial identification has been made and to reuse it in other identification processes that are not subject to AML-requirements. The distribution and frequency of use of this service has unfortunately fallen short of expectations. With Identity™ Giro and Giropay-ID, there are also solutions that make the user data collected in the banking systems available for identification or verification (age verification). This is also where YES comes in. The aim is to enable the user to use
his identity data collected at his bank digitally for other providers. YES intends to provide the infrastructure that allows the ID data of the user to be transferred from the banking system to the requesting company with the consent of the customer. Digital approval and signature services will also be part of YES's offer, presented by CEO Daniel Goldscheider at NOAH17 in London last November. The timing is deliberate: YES is positioning itself at banks as an enabler of a freemium model for the opening of online banking imposed on banks by the PSD2. Fiducia & GAD IT AG has already announced its own similar trust service for the Genossenschaftliche Finanzgruppe (working title CAS).

In 2017, two cross-company private-sector initiatives announced their market entry. Verimi has set itself the goal of becoming "the safest and most user-friendly trust platform for identity services and payments in Europe". The joint venture, in which several companies with a large user base such as Allianz, Axel Springer, Deutsche Bank and Telkom are invested, announced in December 2017 that it will enter the market this spring with a login solution. Users can register centrally with verimi and use this registration to register for other services and log in. The transfer of data is only at the request of the user, the integration of an opt-in for electronic communication data according to e-Privacy Regulation is also announced. In addition to its own authentication system, the cooperation with Mobile Connect has been announced. In expansion phases the integration of the electronic identity card is planned. The second initiative, which was also the result of an initiative by client companies, plans to go live by 25th May at the latest. The initiators RTL, ProSiebenSat.1 and United Internet plan to establish a Login Alliance on the market in the legal form of a foundation. Details on the functionality of the solution are currently not officially communicated.

In addition to these cross-company e-ID systems, there are other private-business-driven initiatives to establish an e-identity solution. The Blockchain Helix AG, the Jolocom GmbH and the Orbiter Group rely on the Blockchain technology. With Helix Alpha, Blockchain Helix has released a first release last year. The client application should act as a personal data cockpit and archive for the user and allow the user in the future to use the planned trust provider network. Tailored trust providers, such as banks and insurance companies, can use this to exchange identity data with the consent of the user. Jolocom also offers an alpha version that provides access to its Smart Wallet where users can store their ID data and use it with different providers. Idento. One of the Orbiter Group also focuses on data management and positions itself as the trustee for the secure custody of data and digital assets.

In addition to the established state e-identity scheme, there are a number of private-sector initiatives in Germany that have announced the establishment of an e-identity system in the near future. For eGovernment, the key factor will be the digitization of administrative services to make room for the application of the state identity. And the
private-sector initiatives - assuming market-driven convenience and security - also stand in the way of user acceptance with the application cases. Crucial here is how far it is possible to establish not only unique applications, but ecosystems that offer numerous, mutually beneficial services for the users. The year 2018 will certainly be the beginning of a longer journey.

e-Identity in Austria

In 2003, Austria established an official and electronic ID card for the use of individual digital eGovernment applications comparably early - the Citizen Card. Since then, private-sector solutions have been developed and established for this state-owned identification medium, which summarizes the following table.

<table>
<thead>
<tr>
<th>Product (alphabetical order)</th>
<th>Provider</th>
<th>Ownership</th>
<th>Functional Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bürgerkarte</td>
<td>Austria</td>
<td>Public</td>
<td>I A D T S</td>
</tr>
<tr>
<td>e-Identifikation</td>
<td>STUZZA - Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr GmbH</td>
<td>Private</td>
<td>x x - - x</td>
</tr>
<tr>
<td>Handy-Signatur und App</td>
<td>A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH</td>
<td>PPP</td>
<td>x x - - x</td>
</tr>
<tr>
<td>MIA (prior to market entry)</td>
<td>Österreichische Staatsdruckerei GmbH</td>
<td>Private</td>
<td>x x x - -</td>
</tr>
</tbody>
</table>

Table 2: Overview e-Identity-Initiatives and -systems in Austria / as of January 2018

As mentioned in the beginning, the citizen card of Austria is a national e-identity tool, which allows access to eGovernment applications and can be used for digital signing. A Trust GmbH is responsible for the development and technical infrastructure of the mobile phone signature. A Trust offers the possibility to use the services of the citizen card with various media. Thus, a plurality of smart cards, for example, service cards, access cards or health cards can be activated as an e-ID means, the digital signature is unlocked thereon. But also a mobile solution of the citizen card was launched with the mobile phone signature. This currently represents the most widespread form of the e-ID in Austria and reaches a circulation of approx. 12% of the Austrian population with an average daily transaction number of 18,000. In addition, there has been an offer from the Austrian banks on the market for five years now, the product e-Identifikation carried out by STUZZA. This makes the identity data available at the banks usable for electronic identifications. The Österreichische Staatsdruckerei presented another e-ID product in 2015 with MIA. It is a digital identification system for smartphones, which allows the digital ID card, driver’s license and other identity documents to be used digitally. MIA is currently not available as there is no decision by the Republic of Austria to officially launch MIA.

For many years, Austria has remained faithful to its policy of continuously rolling out e-identity means. A universally applicable signature-based method available for various media allows the necessary flexibility of different approaches. In order to further increase the eIDAS conformity in the output of this e-identity medium, an activation of
this functionality for passport orders and renewals is to be enforced as the output method in the future. In addition, the number of supported areas of use is to be expanded by integrating additional attributes, such as the date of birth and the address.

**e-Identity in Switzerland**

Switzerland, as a non-EU member, thus only governed by an accompanying "delayed de-facto regulation", finds itself in the comfortable position of observing new regulatory initiatives from Europe up close and only after the situation has sorted out, triggering the successful solutions. In the field of e-identity solutions, Switzerland launched its own solution draft in 2010 with the SuisseID, but it was unable to prevail on the market. The table below summarizes the currently available or announced e-Identity means in Switzerland.

<table>
<thead>
<tr>
<th>Product (alphabetical order)</th>
<th>Provider</th>
<th>Ownership</th>
<th>Functional Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>eID Zug</td>
<td>Zug, using Consensys uPort</td>
<td>Public</td>
<td>I x x x - -</td>
</tr>
<tr>
<td>Schaffhauser eID+</td>
<td>Schaffhausen, using Procivis eID+</td>
<td>Public</td>
<td>x x x -</td>
</tr>
<tr>
<td>SwissID</td>
<td>SwissSign AG</td>
<td>Private</td>
<td>x x x x x</td>
</tr>
</tbody>
</table>

*Table 3: Overview e-Identity-Initiatives and -systems in Switzerland / as of January 2018*

The reasons for the failure of the SuisseID e-identity solution launched in 2010 as part of a public-private partnership are various. For example, the high initial costs and the lack of modern technical realization using an USB stick or smart card and reader were too high a hurdle for the small number of available applications. However, this situation is set to improve by an alliance from a number of large corporations. In line with the German verimi approach, nine groups of companies joined forces at the end of last year to turn the sluggish SuisseID into a successful SwissID. A decentralized e-identity approach is now to be used. Several providers are to be connected to the system, each of which, as an e-identity provider, has its own databases containing the personal data of its customers. Customers can also be registered with several e-identity providers. Whereas originally only private companies were designated as e-identity providers, the concept paper of the Swiss Data Alliance created as a compromise now includes public offices as e-identity providers. In addition, the ID broker, who is connected between the e-identity providers and the relying parties, should ensure the anonymization of the inquiries, so that the e-identity providers do not gain knowledge about the specifically used Relying partners or their services. The joint venture Swiss Sign Group is to act as intermediary to the individual e-identity providers. By the summer of 2018, the Federal Council will present a bill with clear rules for a state-approved electronic proof of identity for private e-identity providers. The concrete design is thus still open in detail.
Parallel to this discussion, two Swiss municipalities have already provided their own e-identity means on a blockchain basis at the local level. The city of Zug has been offering an Ethereum Blockchain-based solution since fall 2017 using Zug ID (based on uPort from Consensys). The ID data is stored here in the digital locker of the user’s app, the city checks and confirms only the identity of the person. For verification, the user of the Zug ID must be personally present in the townhouse once. The output of the e-ID’s is already done, but the use cases are only gradually created. The canton of Schaffhausen piloted the e-Identity Schaffhäuser eID+ in December last year. This uses the solution eID+ from Procivis, which is blockchain-based as well. Both initiatives will initially run until at least the spring of 2018.

At the regional as well as the national level, the listed initiatives in Switzerland offer approaches for the development of e-identity systems, which will be further developed in the short term. In particular, the establishment of the first use cases becomes exciting here, whereby Swiss ID can draw on a portfolio of previous activities of individual initiators.

**Conclusion**

We looked at the European e-identity landscape with the aim of getting a sense of which country is most successful in establishing an e-identity ecosystem and what can be considered the success factors. In total, we analyzed 30 countries with a total of 94 e-identity systems and initiatives.

On a cross-cutting basis, a lot is happening: state solutions are developing slowly but steadily across countries. The focus is mainly on the provision of digitally readable and online usable e-identity means for eGovernment use cases as well as digital signatures. The eIDAS will provide an impetus for Europe-wide use of national solutions. At the same time, private-sector approaches exist which provide their own means of identification and/or integrate the available state resources, in particular for higher-value use cases. The most well-known and successful example of this are the bank-driven initiatives in the Scandinavian countries. These cooperative approaches - in which several parties have joined forces - are characterized by high acceptance and relevance in their markets. The examples bankID (Norway), BankID (Sweden) and TUPAS (Finland) as a cooperation solution of the respective leading national banks as well as NEM ID from Denmark as cooperation between the state and a specialized IT provider of the banks with the common and consistent focus on the digitization of all official and economic communication processes are to be emphasized positively. The willingness to cooperate has inevitable advantages at this point: The famous hen egg problem can be solved and/or additional costs through mutual competition can be avoided.
In addition to openness to collaborations, the focus on dedicated use cases proves necessary in the establishment of e-identity systems. Both comparable regulatory requirements and the combination of use cases that provide additional services to the established products play an important role. In particular, the challenge is to use diversity as an enrichment and driving force for the further development and dissemination of common e-identity systems, rather than constraining them by competition.
Sources

tandbanking.com/fintech-podcast-136-payment-in-den-nordics

2. Bundesministerium für Digitalisierung und Wirtschaftsstandort Wien, Digital
Roadmap Austria, downloaded on 30.01.2018, https://www.digitalroadmap.gv.at/

3. derStandard.at, Mia: Österreichische Ausweis-App macht Daten ohne Speichern
zugänglich, 29.04.2016, downloaded on 30.01.2018, https://derstand-
ard.at/2000035996259

4. Österreichische Staatsdruckerei, MIA, downloaded on 30.01.2018,
https://www.mia.at/

5. STUZZA, e-Identifikation, downloaded on 30.01.2018, http://eserv-
ice.stuzza.at/de/kundenservice/e-identifikation-e-id.html

6. A-SIT Zentrum für sichere Informationstechnologie, Handy-Signatur und Bür-
gerkarte, downloaded on 30.01.2018, https://www.buergerkarte.at/

7. Handelsblatt, verimi-Chefin Donata Hopfen im Interview, 26.01.2018, downloaded

8. Neue Zürcher Zeitung, Neun Schweizer Grosskonzerne preschen bei der el-
ektronischen Identität voran, 21.11.2017, downloaded on 30.01.2018,
https://www.nzz.ch/id.1331019

9. Eidgenössisches Justiz- und Polizeidepartement EJPD, Eine staatlich anerkannte
digitale Identität: Bundesrat bringt Gesetz bis Sommer 2018, 15.11.2017, down-
loaded on 30.01.2018, https://www.ejpde.admin.ch/ejpde/de/home/ak-

10. Business-on.de, Interview mit FinTech-Pionier WebID und Geschäftsführer Frank
Stefan Jorga, downloaded on 30.01.2018, http://www.business-on.de/ber-
lin/_id27376.html

11. Vorstellung YES auf der NOA London https://www.noah-conference.com/vi-
edos/7/show/LAL.9Fia8Pfzo5fyb

12. Blockchain Helix Pressemeldung zu Helix Alpha
https://www.openpr.de/news/985780

13. Jolocom, Präsentation zur Smart Wallet https://www.slideshare.net/jolocom-
com/jolocom-revolutionizing-identity

14. Swiss Data Alliance, Konzeptpapier zur Swiss ID, https://www.swissdataalli-
ance.ch/aktuelles-content/konzept-für-die-digitale-identität-in-der-schweiz-
vorgestellt
IT-Finanzmagazin, Konkurrenz zu YES, Verimi und CAS? idento.one will Identitäten per Smart-Contracts (Blockchain) verwalten, https://www.it-finanzmagazin.de/?p=62446


Giropay, Online ausweisen mit Giropay-ID, https://www.giropay.de/kaeufer/online-ausweisen/


Idento.one, Personal Data Banking Provider, http://idento.one/

Ralf Keuper @ Bankstil, PSD2 und DSGVO: Datenschutz auf unterschiedlichem Niveau?, https://bankstil.de/psd2-und-dsgvo-datenschutz-auf-unterschiedlichen-niveau

Deutsche Post AG, POSTID - Ihr Ausweis im Internet, https://www.deutschepost.de/de/p/postid.html

verimi Website, https://verimi.de/

Stadt Zug, Blockchain-Identität für alle Einwohner, http://www.stadtzug.ch/de/ueberzug/ueberzugrubrik/aktuelles/aktuellesinformationen/?action=showinfo&info_id=383355

Paul Kohlhaas, Zug ID: Exploring the First Publicly Verified Blockchain Identity, https://medium.com/uport/38bd0ee3702

Kanton Schaffhausen, Schaffhauser eID+, https://www.sh.ch/Schaffhauser-eID.5016.0.html
Authors

Andrea Müller disposes of many years of experience in the design of digitization and transformation processes in both the banking and financial sector as well as the manufacturing industry. As an IT business engineer and economist in foreign trade she has acted in responsible positions in industrial and consulting firms.

Dr. Andreas Windisch is Managing Director at asquared. As a certified computer scientist and with a doctorate in engineering, he acted in leading positions in automotive, technology and consulting firms and disposes of many years of experience in the field of IT transformation management – especially in the banking and financial services sector.

About asquared

Asquared is a Berlin-based consulting firm. Our work focuses on developing practical solutions for the regulatory, technologically and/or socially induced change, associated with direct application and confirmation in an industrial environment.

Our attention is focused on business and technology and their interaction. Reaching from the reorientation of strategies, over the (re)design of products and services to the operationalization – our work focuses on shaping change. On all levels.

We present selected insights of our theoretic and practical research work to a broader audience in the form of publications and lectures.