Bring Your Own Identity - Case Study from the Swiss Government

Gion Sialm[1] and Silvia Knittl[2(✉)]

[1] Federal Office of Information Technology,
Systems and Telecommunication FOITT, Bern, Switzerland
[2] CSC Deutschland Consulting GmbH, Wiesbaden, Germany
sknittl@csc.com

Abstract. Imagine that you are a citizen or a company and you are able to file your tax declaration or exchange governmental information by using your favourite existing electronic identity (eID), such as your bank or consumer account. At present, citizens and companies quite often have to create an individual account for almost every government application to share or exchange information. Enabling "bring your own identity" (ByoID) for eGovernment means that access management (AM) will gradually converge to create a single, user-friendly approach in the future. From a technical point of view, many of the necessary features and protocols already exist but have not yet been widely implemented in eGovernment environments. This poses a very complex challenge, both from an operational point of view and from an IT governance and compliance perspective. The only way to solve this is close collaboration among citizens, the private sector and the government. The basis will be an identity and access management (IAM) system that can be adapted to the comprehensive requirements resulting from the aforementioned collaboration. In this article, we describe the path the Swiss government has taken for establishing such a flexible IAM system from the IT providers' perspective while respecting security and privacy requirements.

1 IAM and Data Protection

The process of digitisation makes daily work easier by providing the possibility to do things such as shopping at any time from home or elsewhere in the world. The result for the user is a list with dozens of accounts and passwords. Hence, the efficient use of digital offerings still lacks an uniform identity and access management (IAM). People are very understanding when it comes to log-in to different companies' applications. However, when it comes to interactions with the government, people are not as understanding as with the private sector, since they see the government as one single "company". Therefore, they want to be able to log-in to all eGovernment applications with a single account or even reuse an existing account. Moreover, governments increasingly want to motivate people to use their electronic offerings in order to save money, as banks are doing with online banking. This means that such a transformation will have an impact on all levels, such as social, economic and political. On the governmental level, the government will gradually become an IT service provider. According to the

S. Schiffner et al. (Eds.): APF 2016, LNCS 9857, pp. 38–47, 2016.
DOI: 10.1007/978-3-319-44760-5_3

study prepared for the European Commission in [17], the prerequisites for the increased future use of eGovernment services are both trust and accessibility.

IAM is the core building block to implement trust and accessibility and to enable "bring your own identity" (ByoID). Holistic IAM provides the technical means to ensure protection against unauthorised processing while providing good usability for users. The basic function blocks of IAM are identity management (IM), access management (AM) and access governance (AG). IM covers the tasks involved with creating and maintaining an (electronic) identity. AM relies on IM and deals with authentication and authorization of electronic identities. This sounds very easy. But establishing an electronic identity (eID) that is accepted both by the government and the private sector is a huge challenge. However, this means that the IAM building block has to be very flexible while also providing high security. That is why strong AG will be essential in the future. AG is the functionality within the IAM discipline that is responsible for ensuring, inter alia, that:

- Policies and regulations are applied correctly
- Access to IT resources is managed according to their risk profile
- User access is documented for valid reasons and separation-of-duty conflicts are prevented
- Accountability, manageability and reporting to both business and IT owners is deployed

Figure 1 illustrates a simplified view of IAM from an IT-provider perspective. Depending on the type of data the IT resources are processing (personal data, health records, critical business information, etc.), they are subject to different kinds of compliance requirements. Examples are the Information Protection Ordinance [9], Data Protection Law [8] or Electronic Health Record Law [3]. One aspect of ensuring the data's privacy is to control who has access to the IT resources. The Swiss Data Protection Law states that "personal data must be protected against unauthorised processing through adequate technical and organisational measures" (Art. 7 in [8]). We will outline the complexity of this task from an IT provider's perspective and introduce the necessary IT components, such as a broker infrastructure in the following.

Switzerland is a federal republic, and the federal administration consists of seven federal departments and the Federal Chancellery. Each department consists of several federal offices or agencies (approximately 90) and about 40,000 employees. We will focus here mainly on IAM for the Swiss federal administration's applications as described in [12]. Outcomes of the Identity Network Switzerland [20] programme - which takes into account the confederation, the cantons, and the communes - will be considered where appropriate. A thorough analysis of the establishment of an eID that could be used nationally and internationally is part of a strategic project [14] and summarised in [22].

In the following, we delineate on the basis of the development steps, starting from an isolated approach in Sect. 2.1 and moving on to a modern microservice architecture in Sect. 2.4, how loosely coupled IAM microservices better support the implementation of legal requirements imposed by data privacy and other

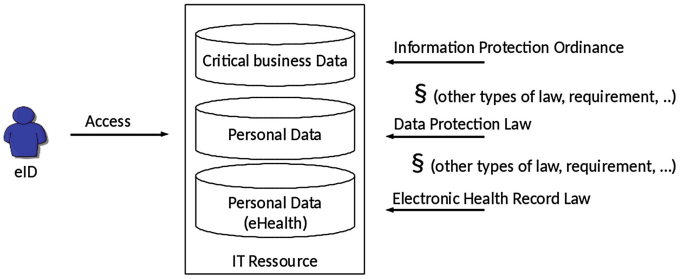

Fig. 1. Controlled access to IT resources

laws. Further, we outline in Sect. 2.3 that the need for delivering eGovernment services, beside legal requirements, was an additional strong driver for this development. While we demonstrate from the technical perspective that IAM could be implemented to address the various compliance aspects, we describe in Sect. 2.4 the challenges from the IT governance and management point of view.

2 IAM - from Silo to Services

2.1 Past IAM - Monolithic Silos

In the past, direct interactions, such as business-to-business, were the core business of most companies. Client-server architectures helped to address this business. In this architecture, IAM was directly integrated into each application, because at that time each application provided mostly only name and password as an authentication method. Moreover, the application was usually connected to an identity directory such as the Active directory[1] from Microsoft. The separation of applications was even seen as a unique selling proposition against competitors, because separation provided high security.

A simplified outline of our environment following this architecture pattern is illustrated in Fig. 2. The Swiss government consists of seven departments, which are further divided into agencies. Every agency is supposed to serve its dedicated mission according its legislative basis. In order to fulfil their mission, purposive applications, such as tax processing applications for the tax office or data warehouse applications for the statistical office, had to be developed, installed and operated for the agencies. Every application had its own inbuilt IAM functionality.

Users, such as internal staff, staff from other agencies, citizens or people at companies needed to be registered and maintained on an individual application basis. Application owners were responsible for both administration and governance. Hence, every application owner was responsible for addressing compliance issues, such as identifying the laws and legal requirements that had to be followed according to the federal administration's IT processes [13]. From an IT

[1] https://msdn.microsoft.com/en-us/library/bb742424.aspx.

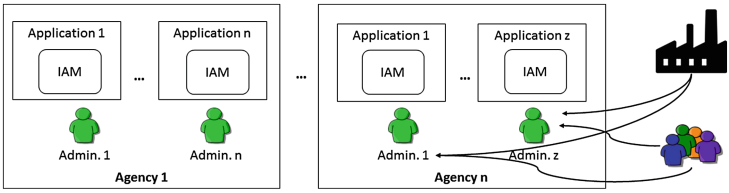

Fig. 2. IAM integrated in each application

governance perspective, the main drawbacks of this monolithic IAM set-up were poor scalability, high maintenance costs and a lack of a comprehensive overview concerning compliance. Questions, such as "who has access to what" or "what kind of access" individuals have at agency, department or even government level could only be answered by asking every application owner separately.

As consumer orientation (business-to-customer) became the main driver for business, Web application became the main key architecture. However, as the number of Web applications grew, users started to complain about the fact that they had to maintain a list of passwords to access applications. Therefore, organisations started to integrate all of their applications into a single personalised portal. This approach was tedious and expensive. For that reason, other solutions were required. By this time, a new approach for IAM appeared.

2.2 Near Past IAM - Service Orientation

A few years ago, IAM solutions were developed that were still monolithic but could be separated completely from Web applications. The advantages of this approach are obvious. There was no need to introduce a separate identity directory for each Web application. As a result IAM governance became easier by centralising the AM infrastructure while still giving the full freedom of AM to the agencies. Figure 3 shows the fact that IAM is provided as a dedicated service for the agencies. The increasing level of centralisation induced the necessity of having a formalised legal basis for providing IAM and other IT services by dedicated IT providers. Therefore, the relevant enactments came into effect delivering clear guidance on the roles and responsibilities of IT governance and management, such as [4,5]. IT management functions were partly consolidated and transformed to one dedicated agency.

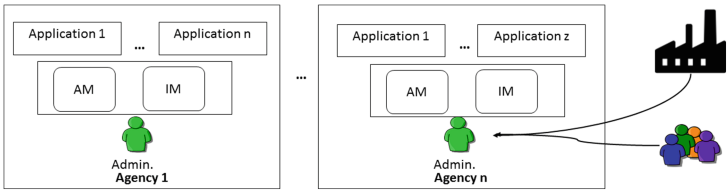

Fig. 3. IAM as a Service per Agency

But still, several drawbacks have to be tackled, such as the focus on internal staff and the poor support of governance requirements [16]. Externally hosted applications and commonly used platforms, such as Sharepoint or content management systems, require better integration support. This can be achieved by managing each site as a "normal" application within a tenant of an agency. This saves money, as only one license per platform is required and allows each agency to manage one or more sites. There is a strong need for supporting a centralised IM with decentralised AM structures. This enables citizens to register themselves just once for all Swiss government applications while allowing AM to remain on the agency side. Quite often, users already have (external) eIDs. Therefore, they demand to re-use these to simplify log-in and AM. This requires the possibility of linking different identities. In the next section, we describe how additional eGovernment requirements foster the need for a new approach to IAM.

2.3 eGovernment: New Requirements for IAM

As competition grew increasingly fierce on the market, close collaboration between companies became more and more important. Centralised AM was no longer an appropriate solution, as each company or organisational unit, rather than a centralised AM department, knew better who should have access to an application. Moreover, centralised AM also required centralised IM. As a consequence, sharing applications among different companies meant that employees again had to manage a list of passwords. A similar development could be observed in government infrastructures.

To cope with this, an IAM programme was launched [12], and requirements for future IAM were broadly gathered from the relevant stakeholders. An initial overview of the results is shown in [15]. The structuring of the requirements was aligned with the business attribute taxonomy according to the SABSA framework [18]. Of course, the attributes "access control" and "accessible" were requested most frequently by the interview partners, both from the technical as well as business side, in the context of an IAM programme. But "business enabled", "continuous" and "compliant" were also concerns voiced by many of the stakeholders.

The meaning of every illustrated business attribute is derived directly from the SABSA framework and adapted to the own context as needed. For example, in our context the requirement "business enabled" means support for seamless and smart eGovernment as defined in [17] and includes, inter alia, the following aspects:

- Government-to-government: support secure interactions between government agencies on the same federal level, but also between government agencies on different levels (international, national, federal, community)
- Government-to-business: support secure interactions of people at companies that have to interact with government agencies, e.g. for tax affairs, social security aspects, and many other government-to-business applications
- Government-to-citizens: support secure interactions between citizens and government agencies

The attribute "compliant" comprises both the needs to define the adequate legal foundations for IAM in the context of eGovernment and to ensure compliance of the IAM solution with the relevant laws. The requirement "continuous" includes the continuity of the technical systems and the related business processes. The more eGovernment applications are operational and accessible, the higher the need for the operation of the IAM solution around the clock. This is even more important for critical infrastructures, such as police applications, road control systems, etc. - and impacts the IT organisation of the provider for running IAM. Finally, easy-to-use interfaces and applications are a feature most stakeholders are asking for in their interaction with online government services. In the next section, we will outline our architecture to implement these requirements.

2.4 Present and Future IAM - Microservice Architecture

Figure 4 shows the current IAM architecture. It is a microservice architecture consisting of small decoupled services such as a reverse proxy, trust broker, identity provider, IM system and identity directories (for details, see also [19]). This architecture offers standardised application programming interfaces (APIs), meaning that the integration of all existing IAM components with the IAM broker could be accomplished quite easily. The usage of a dedicated API component makes it possible both to integrate existing directories and to seamlessly migrate from old applications on the mainframe to modern architectures such as Web applications and, ultimately, the commonly used SuisseID for citizens [21]. This broker architecture relies heavily on trust. Hence, a thorough IT governance is needed to maintain a high level of security. Explicitly managing trust is therefore essential in such a system.

Federation and ID Linking Services. In future, the IAM system will be even more strictly developed according to the standards defined for the so called SuisseTrustIAM (STIAM [7]). The STIAM-related standards are designed to provide generic IAM services for eGovernment, eHealth, eEducation and eEconomy in a standardised way across Switzerland. The most important service will be a broker infrastructure that allows the verification of attributes derived

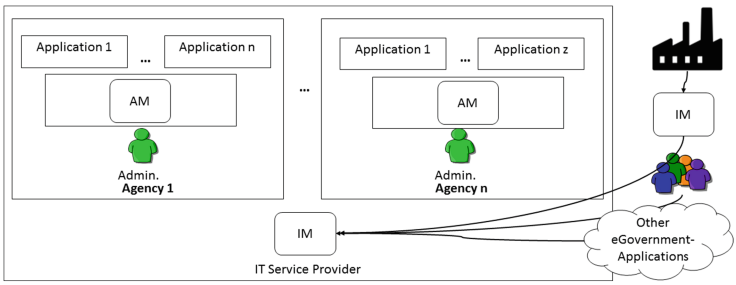

Fig. 4. IAM as a modular Service Application

from registers or directories for any subject that has been authenticated via its eID. Traceability to support compliance will also be a part of the STIAM functionality.

Subjects are able to re-use their already issued eID in the sense of ByoID. The issuers of such IDs need to be assigned an appropriate trust level according to the related eCH-standard (see eCH-0170: eID Qualitätsmodell). The criteria for defining the trust level are the identification procedure (physical presence, quality and validation of assertions), the credential-issuing process or the security of the authentication mechanism. The Swiss standardisation working group developed the STIAM standards with an eye to being compliant with the relevant European and international standards.

By implementing this modular IAM, the following improvements are achieved: easier access via a self-service portal for all types of users; users are able to customise individual configurations for fine granular access as requested in [3] and link their existing external accounts (e.g. bank account) to agencies' accounts and vice versa. Additionally, the administrators' work is also simplified by linking accounts and by managing internal staff and external users in the same way. Moreover, it is even possible to integrate applications from the private sector into government processes or vice-versa, resulting in lower costs for the government and the private sector.

IAM: Future Work. In the sections above, we described how the functional development of IAM has evolved from a silo approach to modular open architecture. Widespread technical standards are available and have been the main drivers of this development. The ongoing concentration, consolidation and migration of the former IAM silos to open architecture on the one hand, while opening interactions for eGovernment across the boundaries of own organisations on the other hand, imposes new challenges on the steering and management of IAM services.

The implementation of such trust and federation services is supported by technical standards that are already in place and incorporated in many off-the-shelf products. Further, the Swiss government funded participation in the pilot environments of the STORK project [1]. The aim of this project was to establish an European eID interoperability platform that will allow citizens to establish new e-relations across borders, just by presenting their national eIDs. One of this project's outcomes was an essential contribution to the eIDAS Regulation [6]. A statement in the final report, "STORK 2.0 für die Schweiz", is the recommendation of Swiss participation in mutual eID recognition as part of the eIDAS regulation. Therefore, a process has to be started that is estimated to last about two years. There will be a need of interim arrangements until this process is implemented

Having the legal enactments in place is a vital premise for such eGovernment services. In the initiation phase of a project, the mandatory project management method HERMES prescribes that risks and the operational risks have to be determined and the legal framework and the protection needs have to

be analysed [10]. This method covers various scenarios, such as procurement of standard software or dedicated software development, but not IT operation. Therefore, the legal basis for providing and operating the described STIAM services has to be adjusted, and a dedicated IAM enactment is already under development. The continuity of centrally provided IAM services was named frequently in the above cited requirements from the stakeholders interviewed. To build the legal foundation, the Swiss Federal Council has opened the consultation phase for what will be known as the Informationssicherheitsgesetz (Information Assurance Law [2]).

Besides legal considerations, it is also fundamental to have the organisational structures aligned. To do so, the current design of boards, responsibilities and processes in the management and steering domain will be reconsidered. The Swiss government is responsible for granting what is known as the "Marktmodell" [5] for all services that are operated as standardised services for the federal administration. This model contains the future IAM service model, including the required resources for its operation and future development. The revised Marktmodell is an outcome of the IAM programme [12] and will be presented to the Swiss government in the near future.

3 Conclusion - IAM as a Service is by Far More Flexible but also Needs More Governance

In recent decades, the in-house production depth within manufacturing has decreased gradually by focusing on assembly. The same development can be seen in IT environments. Compared to the highly integrated IT systems of the past, functional decomposition is now considered state of the art. In this paper, we have illustrated this aspect of the IAM function and showed the development from monolithic IAM to loosely coupled IAM consisting of microservices, where users are able to bring their own identity (ByoID). ByoID can help to overcome inhibitions related to eGovernment and may promote the collaboration between the government and the private sector. This development will make easier some aspects of IAM governance, such as AM, as stated in various laws. On the other hand, ByoID is a challenging task for IAM governance in its mission to maintain the same security as in the past. To master these challenges, the Swiss government recently published specific actions in its IT strategy for the years 2016 to 2019 as:

- Strengthening the IT management system of the federal administration with concise assignments of tasks, competences and responsibilities
- Regularisation of the governance of IT architecture
- Further developing strategic IT controlling
- Consolidating the IT default documents across all levels

The goals of these strategic aims are to steadily strengthen IT steering, to reliably deliver a sound basis for decisions and to gradually increase the maturity of the IT [11]. The next big challenge in IAM is to consider and integrate the identity

of things as the Internet of things grows. Governments' IAM will have to follow this development, and policy makers will have to address this issue by providing the relevant legal framework.

References

1. Bern University of Applied Science: STORK 2.0 für die Schweiz. Projektabschlussbericht, State Secretariat for Economic Affairs (SECO) (2016). http://www.seco.admin.ch/themen/05116/05118/05315/05329
2. Bundesversammlung der Schweizerischen Eidgenossenschaft: Bundesgesetz über die Informationssicherheit (ISG). Web, March 2014. http://www.news.admin.ch/NSBSubscriber/message/attachments/34224.pdf, draft. Accessed 25 May 2016
3. Bundesversammlung der Schweizerischen Eidgenossenschaft: 2011 - Bundesgesetz über das elektronische Patientendossier (EPDG). Web (2016). http://www.bag.admin.ch/themen/gesundheitspolitik/10357/index.html?lang=de. Accessed 9 Mar 2016
4. Der Schweizerische Bundesrat: Verordnung über die vom BIT betriebenen Verzeichnisdienste des Bundes. Web (2014). https://www.admin.ch/opc/de/classified-compilation/20132589/index.html. Accessed 6 Mar 2016
5. Der Schweizerische Bundesrat: Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung. Web (2016). https://www.admin.ch/opc/de/classified-compilation/20081009/index.html. Accessed 6 Mar 2016
6. European Commission: Trust Services and eID. Web (2015), https://ec.europa.eu/digital-single-market/trust-services-and-eid. Accessed 10 Mar 2016
7. Fachgruppe Identity und Access Management: SuisseTrustIAM Rahmenkonzept. Standard eCH-0167, Verein eCH - E-Government-Standards, June 2014. http://www.ech.ch/
8. Federal Assembly of the Swiss Confederation: Federal Act on Data Protection (FADP). Web (2014). https://www.admin.ch/opc/en/classified-compilation/19920153/index.html. Accessed 9 Mar 2016
9. Federal Assembly of the Swiss Confederation: Ordinance on the Protection of Federal Information (Information Protection Ordinance, IPO). Web (2015). https://www.admin.ch/opc/en/classified-compilation/20070574/index.html. Accessed 9 Mar 2016
10. Federal IT Steering Unit: HERMES 5.1. Federal IT Steering Uni, 5.1 edn. (2015). http://www.hermes.admin.ch/onlinepublikation/index.xhtml
11. Federal IT Steering Unit: IKT-Strategie des Bundes 2016–2019. Web, December 2015. https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sb000-ikt-strategie-des-bundes.html. Accessed 20 May 2016
12. Federal IT Steering Unit: Programme IAM of the confederation. Web (2015). https://www.isb.admin.ch/isb/de/home/themen/programme_projekte.html. Accessed 25 May 2016
13. Federal IT Steering Unit (FITSU): P000 - federal administration's IT processes. Web, September 2015. https://www.isb.admin.ch/isb/en/home/ikt-vorgaben/prozesse-methoden/p000-informatikprozesse_in_der_bundesverwaltung.html. Accessed 25 May 2016
14. Federal Office of Police (fedpol): Establishment of an electronic identity (eid) that is valid nationally and internationally. Web (2016). https://www.egovernment.ch/en/umsetzung/schwerpunktplan/elektronische-identitat/. Accessed 25 May 2016

15. Hoernes, P.: Ein IAM Grossprojekt aus der Perspektive des Enterprise Architekten - Erfahrungen aus der Schweizer Bundesverwaltung. Web (2014). https://rg-muenchen.gi.de/node/1291, presentation at the EAM working group of the Gesellschaft für Informatik. Accessed 8 Mar 2016
16. Knittl, S., Wiedmer, H.U.: Dienste und IT-Governance in der Bundesverwaltung - Bedarf, Nutzen und Potenzial. eGov Präsenz (2015)
17. Lörincz, B., Tinholt, D., van der Linden, N., Oudmaijer, S., Jacquet, L., Kerschot, H., Steyaert, J., Cattaneo, G., Lifonti, R., Schindler, R., Millard, J., Carpenter, G.: eGovernment Benchmark Framework 2012–2015. Web (2012). http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1929. Accessed 9 Mar 2016
18. Open Group TOGAF-SABSA Integration Working Group: TOGAF-SABSA Integration WG: TOGAF and SABSA Integration. Whitepaper, The Open Group and The SABSA Institute (2011)
19. Sialm, G.: eIAM: Neue Möglichkeiten dank offener Architektur. Eisbrecher (54), June 2014. http://www.bit.admin.ch/dokumentation/00090/00156/index.html?lang=de
20. State Secretariat for Economic Affairs SECO: Identity network Switzerland. Web (2016). https://www.egovernment.ch/en/umsetzung/schwerpunktplan/identitatsverbund-schweiz/. Accessed 25 May 2016
21. Trägerverein SuisseID: SuisseID - Die SuisseID ist der Schweizer Standard für sichere Authentifikation und elektronische Signatur. Web (2016). http://suisseid.ch/de. Accessed 30 May 2016
22. Weber, C., Bernold, R., Brian, O., Brugger, J., Dungga Winterleitner, A., Fraefel, M., Hosang, R., Riedl, R., Selzam, T., Walser, K., Weissenfeld, K.: eID-Ökosystem Modell. Technical report Version 1.1, Fachhochschule Bern, June 2015. https://www.wirtschaft.bfh.ch/uploads/tx_frppublikationen/eID-OEkosystem_V1_2.pdf