## LIST OF CONTENTS

1. INTRODUCTION .............................................................................................................................................. 4
   1.1. BACKGROUND AND MOTIVATION ............................................................................................................. 4
   1.2. PROBLEM STATEMENT ............................................................................................................................... 4
   1.1. OBJECTIVES AND OUTPUT ....................................................................................................................... 4
   1.2. PROCEDURE AND METHODOLOGY ........................................................................................................ 5
   1.3. ADDRESSEES ............................................................................................................................................... 5

2. IT ARCHITECTURE ............................................................................................................................................ 5
   2.1. CURRENT SITUATION ............................................................................................................................... 5
   2.2. A GLIMPSE INTO OTHER DEPARTMENTS ............................................................................................... 6
   2.3. FUTURE APPLICATIONS ........................................................................................................................... 6
   2.4. IAM INTEGRATION ..................................................................................................................................... 7

3. PROPOSED SOLUTIONS .................................................................................................................................. 8
   3.1. THE NEVIS SOLUTION ............................................................................................................................... 8
   3.2. THE NEVIS MODULES ............................................................................................................................. 9
   3.3. E-SERVICES DATA FLOWS ..................................................................................................................... 11

4. TECHNICAL PRECONDITIONS FOR APPLICATIONS ......................................................................................... 12

5. REASONS FOR USING AN IAM ..................................................................................................................... 12

6. CONCLUSION .................................................................................................................................................. 13

LITERATURE ......................................................................................................................................................... 14
   6.1. BOOKS AND DOCUMENTATION .............................................................................................................. 14
   6.2. WEB LINKS ............................................................................................................................................... 14

List of figures
Figure 1: IAM integration [6, slide 6] ................................................................................................................... 7
Figure 2: NEVIS functionalities [3] .................................................................................................................... 8
Figure 3: The nevisProxy [3] ............................................................................................................................ 9
Figure 4: nevisIDM [3] ...................................................................................................................................... 10
Figure 5: nevisAuth [3] .................................................................................................................................... 10
Figure 6: E-Services data flows [6] .................................................................................................................. 11
<table>
<thead>
<tr>
<th>Abbreviation/Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fat Client</td>
<td>Fat clients have the classical view of applications and use text fields, buttons, check boxes etc. Not only is the user interface on the client but also the entire business logic with exception of the data which can be saved on a server.</td>
</tr>
<tr>
<td>GEVER (Elektronische Geschäftsverwaltung)</td>
<td>The German term for electronical business administration Software. It typically contains business control, work flows and document management systems.</td>
</tr>
<tr>
<td>Classical web-application</td>
<td>A classical web-application generally has a multi-page structure as well as the typical HTML look. The application is server-based. The entire business-logic and request/response communication goes through the server – the web-application is merely the surface of the received html. Desktop-elements such as drag and drop are missing. As a consequence, the usability suffers.</td>
</tr>
<tr>
<td>Rich internet application</td>
<td>According to Wikipedia, a Rich Internet Application (RIA) is a Web application that has many of the characteristics of desktop application software, typically delivered either by way of a site-specific browser, via a browser plug-in, independent sandboxes, extensive use of JavaScript, or virtual machines.</td>
</tr>
<tr>
<td>IAM</td>
<td>Identification und Access Management</td>
</tr>
<tr>
<td>User certificates</td>
<td>A possible authentication method</td>
</tr>
<tr>
<td>Challenge-response procedure</td>
<td>According to Wikipedia, in computer security, challenge-response authentication is a family of protocols in which one party presents a question (“challenge”) and another party must provide a valid answer (“response”) to be authenticated.</td>
</tr>
<tr>
<td>Suisse ID</td>
<td>According to suisseid.ch, it is the first standardised electronic proof of identity in Switzerland. It supports legal signatures as well as secure authentication.</td>
</tr>
<tr>
<td>Secure-Reverse-Proxy</td>
<td>According to Wikipedia, in computer networks, a reverse proxy is a type of proxy server that retrieves resources on behalf of a client from one or more servers.</td>
</tr>
<tr>
<td>Multi-tenant capable</td>
<td>According to Wikipedia, multitenancy refers to a principle in software architecture where a single instance of the software runs on a server, serving multiple client organizations (tenants). Multitenancy is contrasted with a multi-instance architecture where separate software instances (or hardware systems) are set up for different client organizations.</td>
</tr>
</tbody>
</table>

Table 1: List of terms and abbreviations
1. INTRODUCTION

1.1. Background and Motivation
This case study investigates the signification of a central Identity and Access Management (IAM) module in an IT-environment of a large organization. The showcase is the Swiss administration, namely the Federal Social Insurance Office. The IAM module that is subject of this case study is NEVIS from Adnovum Informatik AG.

The case study is partly an on-the-job analysis since the author of the document works in the Swiss administration. The projects he is working on are affected by whether or not his administration is going to use an IAM.

1.2. Problem statement
Administrations typically have historically grown structures and therefore a decentral administration of users. As a consequence, there can be several databases or directories with often redundant user data. More often than seldom, applications manage user identities and access rights separately.

In the historical context this made a lot of sense. However, as nowadays there is more and more demand for a comprehensive use of IT in organisations, it appears to be more useful to have one central module which takes care of certain functionality for a lot of applications. As an example: a module that is responsible for managing identities and authorisations.

Strategically this also seems like a sound advice: especially if the administration develops or buys new customized Software tools – the German term being “Individualsoftware”. In this case, the developers and suppliers do not have to develop an Identity or Access Management system from scratch, rather make the new Software fit to the requirements of the already existing and centrally available IAM.

1.1. Objectives and Output
The Federal Social Insurance Office is revising its strategy in terms of IT-architecture and application integration. In this context, the question comes up which modules would not only be usable by one application but serve in a cross-sectional manner.

A well-defined architecture paves the way for future individual applications. Suppliers and developers of the Federal Social Insurance Office could be given the architecture documentation to
let them make their applications fit into the architectural frame and furthermore make it able to cope with the modules that are thought for recurring and cross-sectional use.

This case study is to show such a cross-section use of a module, namely the Identity and Access Management. The objective and output is to understand the case and importance of IAM in the Federal Social Insurance Office.

The case study not only wants to show the overall significance of IAM, but also investigate more closely the example of NEVIS. It wants to answer questions like: what are the prerequisites towards the architecture – what are the requirements for applications to work with NEVIS – of what modules does NEVIS consist - how will IAM be embedded in the new architecture - what are the benefits of a central IAM.

1.2. Procedure and Methodology

The case study compares the present and future situation in the Federal Social Insurance Office in terms of its IT architecture. Furthermore, it looks at the NEVIS solution to understand how it works, how it is embedded in an IT architecture. This was done by collecting and studying available documentation – from internal (within the administration) and external sources. Also, the documentation set of the IAM solution NEVIS from Adnovum Informatik AG was analyzed more closely.

1.3. Adresssees

The following persons are addressed with this case study:
- Swiss Federal institutions
- IT strategy responsibles
- IT architecture responsibles
- IT security responsible
- Software suppliers
- People interested in e-business and e-government

2. IT ARCHITECTURE

2.1. Current situation

In 2011, the Swiss Federal Social Insurance Office has a large amount of Software solutions. While this was clear before, in the context of the system migration to Microsoft Windows 7, for the first time the Software is cleanly listed in a Software-portfolio. Now, IT responsible can get a good
overview. The analysis of the portfolio shows many independent tools for a lot of different tasks. What is missing?

Most applications are viewed as separate solutions. A clear strategy for the reuse of certain components is missing. The existing databases partly contain redundant data. If Software needs Identity and Access Management, it is developed from scratch.

Someone coined the term E-services. E-services can contain various functionalities such as address administration, as well as the mentioned Identity and Access Management. In terms of IT strategy, it seems sensible to use E-services for future applications in order not to reinvent the wheel each time.

**E-Services as described in [16]**

E-Access  This E-Service is responsible for access management. It makes it possible to access an application from within various network zones in an authorised way.

E-ID  This component provides a standardized an integrated user administration. It is for example possible for users to register themselves and to administrate their data online.

**Advantages of E-Services [16]:**

- Identity and Access Management can be reused for new applications
- The web-interface can be integrated in applications - for user registration, login, password changes, etc.
- Identities only have to be registered once
- Business and security mechanisms are separated
- A standardized user administration provides the same level of security for all users

### 2.2. A glimpse into other departments

By the date of submission of this paper, Adnovum’s IAM solution NEVIS is already used in the Swiss administration by

- the Department of Justice and Police (FDJP/EJPD): security and information portal (SSO)
- the Swiss Federal Administration, Department of Finance (FDF/EFD): access & identity management for an e-government solution

### 2.3. Future applications

The number of new applications in the next two years in the category ‘Individual-Software’ (excluding the GEVER-category) is estimated between five and ten. Some of the new applications
will be Rich Clients, with a fix installation on the user’s computer. Others are web-based solutions, either classical Web-applications or Rich Internet Applications.

What most of the applications have in common is a user authentication. According to [2, page 15], the concept consists of three-levels:

1. Lowest level: the current rights of an application, a session or a thread
2. Middle level: all supported roles, the types and numbers of rights
3. Highest level: all users and their roles for using the application

[2] explains the necessity of a common system for administrating the users and their roles.

2.4. IAM integration

Figure 1 shows how the IAM solution could be embedded into the IT landscape of the Federal Social Insurance Office. The schema displays the zones which varying level of security level and access right. It ranges from the public internet to the so-called ‘shared service zone’. The name is almost self-explaining, it is a zone where shared services are placed, meaning services used by several parties. The IAM solution ‘SSO NEVIS’ is situated in the SSZ. However, at the time of the submission of this case study, this schema is merely a draft and subject to many workshops and discussions between the concerned parties.

![Figure 1: IAM integration [6, slide 6]](image)

New applications as mentioned in 2.3 would be placed in the SSZ. One example is NA ALPS which is illustrated as a purple square in Figure 1. Users coming from the public internet zone as well as users in the restriced zones such as the BV-Netz which contains all users in the Swiss administration, will have to be registered in the IAM solution in order to gain access to NA ALPS.
This architecture allows to centrally administrating users, roles and access rights in all three levels (levels explained in 2.3). Applications to be developed later can also be placed into the SSZ and make use of the IAM.

3. PROPOSED SOLUTIONS

3.1. The NEVIS solution

According to [3], NEVIS provides Access- and Identity management which contains authentication and authorization, a web application firewall as well as various authentication methods and single sign-on (SSO). Furthermore, it has a Identity Management component which is responsible for the management and secure propagation of identities and permissions. Also it has Secure Integration of clients, applications, web services and backends and finally it provides a Central Administration for configuration, monitoring, alarming, auditing and reporting.

![NEVIS functionalities](image)

NEVIS offers a broad range of authentication variants:

- Username/Password
- Rasterkarte (letters and numbers in a table)
- User certificate
- OTP (one time password), Challenge/Response und Biometrie
- Kerberos (works on the basis of “tickets”)
Consequently, if in the future a set of applications will use ‘Suisse ID’, no big changes in the Software will be necessary.

### 3.2. The Nevis modules

**nevisProxy**
According to [3], the nevisProxy component acts as ‘single point of entry’ in the SSO-unit. If a client send an HTTP(S)-request to an application, the loadbalancer leads it to the secure-reverse-proxy (nevisProxy). nevisProxy holds the certificates and keys for the server authentication towards the client and takes – together with nevisAuth – the role as an application firewall. Therefore, it controls the user access and protects security-sensitive data, applications, services and systems against internal and external threats.

![nevisProxy](Image)

**Figure 3: The nevisProxy [3]**

**nevisIDM**
According to [3], the nevisIDM component is a multi-tenant capable identity management solution. It serves as a central administration unit for users, applications and access rights. It is possible to delegate the administration to superusers or to enable the users for self-administration.
nevisAuth

According to [3], the nevisAuth component grants strong user and system authentication in identity and access management solutions. It allows to securely executing multi step authentications including dynamic adaption of the authentication strength. It is possible to install various plug-ins to integrate more ways of authentication.
3.3. E-Services data flows

Figure 6: E-Services data flows [6]

Figure 6 illustrates how users can access Software with help of an IAM E-Service. It shows the order of steps in the procedure.

Steps of user authentication with E-Services as described in [6] page 4

1. The user calls the URL of the application he wants to use
2. If the user is not authenticated his request is transferred to E-Access
3. E-Access displays the login mask
4. The user types in his username and password (depends on the authentication method)
5. The data is transferred to E-Access Auth for authenticating
6. E-ID checks the credentials
7. E-Access Auth creates an identity token
8. The identity token is being transferred to the application server
9. The application checks the identity token for validity
10. The application finds the user and its roles
11. The application sets the user status to ‘logged-in’. The server response is displayed in the browser
4. TECHNICAL PRECONDITIONS FOR APPLICATIONS

There are certain technical preconditions for applications to easily integrate with the IAM solution. According to [8 page 7], those preconditions can be summarized with the term ‘proxy-awareness’.

Mainly, this means that

- relative URLs have to be used
- Web-applications have to be reachable under a self-contained URL (eg. https://somehost.ch/myappl/ not https://somehost.ch/).
- URLs which are called within the application also have to be relative (eg. ../pics/picture.gif instead of http://somehost.ch/myappl/pics/picture.gif).
- The HTML tag ‘base href’ must not be used (base href tells the browser that all relative links begin with a certain address)
- Coupling with other applications must go over the proxy
- URLs to external resources must be absolute
- The content type must be always be indicated (tells the browser whether the content is text, images, video, etc.)

5. REASONS FOR USING AN IAM

As mentioned in [1], a typical employee today works with a lot of different IT-systems. But also suppliers and clients increasingly have access to those systems. Identity Management defines the processes to give people fine-grained access rights to the necessary systems. The analogy of private internet users helps to illustrate the case: as pointed out in [1] page 2, nowadays most private internet users have numerous digital identities (eBay, Amazon, iTunes, etc.) which have to be administrated and protected.

According to [2], IAM is typically needed for all applications. It often occurs that users are granted access to several applications. In such cases IAM offers the following advantages:

- **Registration once**: The users only have to be registered once. This makes modifications (joiners, leavers, changers) much easier.
- **Single Sign on**: This means that users only have to authenticate once and afterwards will have access to all permitted applications. No further passwords need to be memorized.
- **Minimal security requirements are met**: An IAM allows the centralization of policies on one system. This means, the minimal password length, password complexity, frequency of password changes and so on only have to be defined once and not for each application.
- **Delegated user administration**: It is not so practical to only allow users to be registered or changed by a central instance. An IAM allows delegating the user administration. For each application specific administrators can be defined.
- **Consistency:** With an IAM the user administration automatically becomes consistent. The applications themselves don’t have to manage the role definitions.

- **Decoupling of the authentication method from the system:** IAM systems generally support various authentication methods. In Switzerland more and more the two-factor authentication is required (e.g. Suisse-ID). With the IAM a change of the authentication method is possible without extending the application.

[4] page 17 and [9] also list a number of reasons for the introduction of IAM:

- **Security-efficiency:** The number of subjects (users, systems) to be authenticated is growing. Therefore, the authentication process and the administration of authenticated subjects has to become more efficient.

- **Security-effectiveness:** Identities, claims, mechanisms and security levels have to be consistent in the entire IT-architecture

- **Agility and productivity:** The time to reaction to new or changed requirements is much shorter with an IAM. Furthermore, stuff can be appointed in a more optimal way (e.g. separation between user administration, access management and Software development) and the risk of fraud lowers as well.

### 6. CONCLUSION

To sum up, the wheel shall not be reinvented with every new Software acquisition. This means, Software modules which can be used by several applications should be purchased/developed only once. This is exemplarily shown in the case of NEVIS IAM.

In terms of e-government, an integrated application architecture has benefits for the customer; in our case the citizen of a country. Functionality like SSO (single sign on) allows the user to sign in once and use all other applications without further authentication. Various authentication methods such as Suisse ID, two-factor authentication, Biometric identification, etc. become possible for all applications ‘behind’ the IAM. This – in the end of the day - increases data security and also transparency to the citizen.
LITERATURE

6.1. Books and documentation

[5] IAM_20110616-v0.3.pptx (Bundesamt für Sozialversicherungen 2011)
[7] Demo_EESSI_PoC.pptx (Bundesamt für Sozialversicherungen 2011)

6.2. Web links