Identity Management Lifecycle - Exemplifying the Need for Holistic Identity Assurance Frameworks

Jostein Jensen

Identity Management Lifecycle - Exemplifying the Need for Holistic Identity Assurance Frameworks

Jostein Jensen

Norwegian University of Science and Technology, Department of Computer and Information Science, Norway,
jostein.jensen@idi.ntnu.no

Abstract. Many governments around the world have a strategy to make electronic communication the primacy choice for interaction between the citizens and public services. Identity management makes the foundation for secure and trusted communication, and government frameworks for authentication and identity assurance are therefore developed to support the strategies. This paper examines three existing authentication and identity assurance frameworks, and is a good example to show the importance of specifying assurance frameworks that takes a holistic view of the identity management lifecycle and related threats.

1 Introduction

A (digital) identity is *the information used to represent an entity in an ICT system* [4]. In the context of this paper we think of entity as a human being, meaning that we think of identity as a digital representation of a physical person. A digital identity consist of three key elements [6]: 1) an *identifier* used to identify the owner of the identity 2) *attributes*, which describes different characteristics of, or related to, the identity owner 3) *credentials* which is evidence/data that is used by the identity owner to establish confidence that the person using the identity in the digital world corresponds to the claimed person. There must be processes in place to create, use, update, and revoke digital identities, and policies must exist to govern each of these activities. This is called Identity Management (IdM), and the IdM lifecycle is illustrated in Figure 1. The rigor and quality of all steps of the IdM process can vary substantially between different organizations, and this affects the level of trust that can be associated with a digital identity. Dishonest individuals can exploit weaknesses in any of the identity management lifecycle steps to gain unauthorized access to resources, and as such threaten confidentiality, integrity and availability of assets.

Security requirements can be specified for each phase and each activity in the IdM lifecycle to mitigate threats towards it. The purpose of defining security requirements in relation to identity management is to increase the confidence in the identity establishment phase, and increase the confidence that the individual who uses a digital identity is the individual to whom it was issued [7].

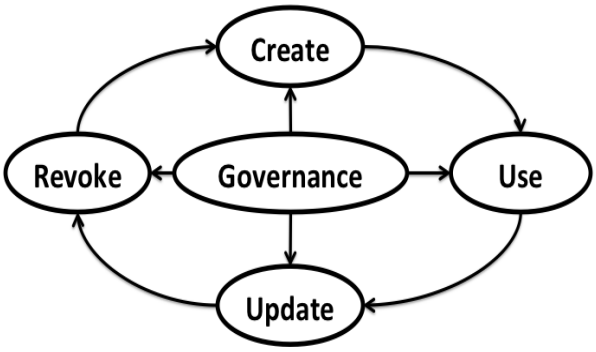

Fig. 1. Identity Management Lifecycle. Adapted from [6]

Requirements for each lifecycle activity can be bundled to form identity assurance levels, where a low assurance level specifies IdM requirements for systems with limited risk levels and high assurance levels define IdM protection strategies in high-risk environments. Examples of assurance levels with associated requirements targeted at the activities in the IdM lifecycle can be found in Identity Assurance Frameworks, such as those defined by the Norwegian government [1], the Australian government [2], and the US government [7].

In this paper we will look at each step of the identity management lifecycle, and identify relevant threats to each lifecycle phase (section 2). The government frameworks mentioned above [1] [2] [7] are examined to determine whether they specify security requirements that can mitigate the identified threats, and they are used in this paper to illustrate the need for holistic identity assurance frameworks that cover all phases of the IdM lifecycle (section 3). Then we provide a discussion of our findings in section 4, and conclude the paper in section 5.

2 Identity management lifecycle and threats towards it

Identity management life cycles have been presented in different shapes, for instance in by International Standards Organization [4], Baldwin et. al [5] and Bertino and Takahashi [6]. Even though the lifecycle presentations vary between these, they treat the same concepts. The following structure, which is illustrated in Figure 1 is inspired by Bertino and Takahashi. More information about threats towards IdM can be found in [7] and [5], while more technical insight to most threats can be found in the CAPEC database[1].

[1] CAPEC, Common Attack Pattern Enumeration and Classification, http://capec.mitre.org/

2.1 Creation

The first phase in the IdM lifecycle is identity creation. Identity attributes will be collected and registered, credentials will be defined, and finally issued to the user during this process. Identity proofing including screening and vetting of users [4] can be part of these activities. The creation process is the foundation for all subsequent use of digital identities, and as such rigor in this phase is of utmost importance for systems that require a high to moderate security level.

Threats to the creation process There are numerous motives for attackers to somehow manipulate the identity creation process, and where one example is to assume the identity of another person during the establishment of a digital identity. This can e.g. be done by presenting forged identity information (e.g. false passport) during the identity proofing process, or exploit the fact that identity proofing is not operationalized in the creation process. University enrollment under a fake alias, establishment of credit cards or establishment of phone subscriptions in another persons name are examples of this threat. The consequence of this is that the attacker obtains full access to resources by means of a valid user identity. Further, invalid attributes can be inserted in the user database, attributes can be modified by unauthorized entities or valid, and false attributes can be registered during the attribute registration if proper countermeasures against these threats are not in place. These threats can have serious consequences knowing that attributes can be used to determine access level e.g. based on group memberships/roles in role based access control (RBAC) schemes or possibly any other attribute in attribute-based access control (ABAC) schemes. Also the credential registration process must be protected so that attackers cannot steal or copy credentials, such as username password pairs. If attackers get access to valid credentials, they can impersonate valid users to obtain protected information. These challenges also exist during delivery of digital identities. Attackers can obtain access to digital identities, which can be used in subsequent malign activities by intercepting the communication channel used to deliver the credentials, such as mail or e-mail.

2.2 Usage

Once a digital identity is created and issued, it is time to start using it in electronic transactions. Digital identities are often being associated with the authentication process. The issued credentials are being used for this purpose. It is also becoming more and more common that electronic services provide personalized content based on identity attributes, and even to base access control decisions on certain identity attributes. The use of digital identities can vary from use on one separate service, to use on multiple services. Single-sign-on (SSO) is a concept where users obtain a security assertion after a successful authentication, and where this assertion is used as authentication evidence towards the subsequent services the user visits. SSO is commonly used in enterprise networks

where employees' authentication provides them a security assertion (e.g. Kerberos tickets in Microsoft environments) that can be used to access their e-mail, file shares, intranet and so on. Federated single-sign-on is an extension of the SSO concept, where organizations can cooperate on technology, processes and policies for identity management. Federated SSO allows security tokens to be used to achieve single-sign-on across organizational borders.

Threats to the use phase There are many threats towards the use of digital identities. Access credentials can be lost, stolen or cracked so that attackers can authenticate, and thereby impersonate, valid users. There are many attack vectors used to obtain valid credentials. Communication lines can be intercepted to copy plaintext data, password files can be stolen and decrypted, social engineering can be used to trick users into giving away their credentials, and so on. The introduction of SSO and federated SSO has added to this complexity in that security assertions are issued based upon a successful authentication. This security assertion is stored by the client and used as proof of identity in subsequent service request. This means that an attacker can copy assertions and add them to malign service requests, or replay previously sent messages. If the receiving service trusts the assertions it will provide information as requested. Since authentication data (assertions) are shared across services in SSO and across services within different trust domains in federated SSO, the attack surface in weakly designed systems is highly increased compared to having separate systems. As already mentioned, RBAC- and ABAC-models allow taking access control decisions based on identity attributes. If attackers can modify attributes during transmission, they can be allowed to elevate their privileges by manipulating attributes. Another scenario is that attackers modify e.g. shipping address so that one user orders and pays the goods, which are then sent to the attacker's destination. The disclosure of identity attributes may also violate users privacy, or reveal company internal information.

2.3 Update

While some identity attributes are static, such as date of birth, eye color and hight, others can change over time. Employees' role in a company can change, people can move and change address, and credit cards, digital certificates and so on can expire. The identity management process must therefore include good procedures to keep identity attributes up to date to ensure their correctness. Identity adjustment, reactivation, maintenance, archive and restore are activities part of the identity update process [4].

Threats to the update phase The threats related to the update phase are similar to those presented in the creation phase. Credentials can be copied or stolen and false attributes can be provided. In operative environments one can experience that the responsibility for identity creation and identity update are

placed at different levels in the organization. While the human resource department may be responsible for creation of user identities e.g. in relation with a new employment, the responsibility for updating user profiles may lie at the IT-support department. Consequently, attackers can approach different parts of an organization to achieve the same goals. Attackers can also exploit weaknesses specific to the update procedures. Delays in the update procedure can allow users to access content based on old but still valid access credentials and attributes, and attacks towards update management interfaces can allow unauthorized reactivation of user accounts.

2.4 Revocation

Identities, including credentials should be revoked if they become obsolete and/or invalid [6]. Revocation can be separated into identity attribute suspension and identity deletion [4]. The former means that some or all identity attributes are made unavailable so that access rights associated with these attributes are made temporarily unavailable to the user. An example of this can be that the association between a user and a certain group membership is removed to reduce a user's access rights. Another is the deactivation of all access rights associated with a user. Identity deletion means the complete removal of registered identity information. Information about revocation should be distributed to all relevant stakeholders to ensure that access is not given based on invalid credentials.

Threats to the revocation phase Suspension and deletion of identity information can primarily be misused to block authorized users from accessing resources. Additionally, insufficient distribution of revocation lists to distributed services can allow attackers to use stolen identities even after the access rights have been formally revoked.

2.5 Governance

There is a need to have policies in place and govern all steps of the identity management lifecycle. Regarding creation of identities, for instance, there should be policies in place that regulate e.g. who can create identities, how they are created, how the quality of attributes can be assured, how credentials are issued and so on. Identity management governance is closely related to identity assurance and identity assurance levels, where requirements for all phases are specified.

Threats to identity management governance Password policies are among the policies that affect all phases of the identity management lifecycle, so we continue to use this as an example to illustrate the lack of, or weak, policies. Password policies should include requirements for password length, complexity and validity period. Non-existent or weak policies will allow users to associate their digital identities with insecure passwords. Weak passwords are easily being hacked e.g. through brute force attacks or guessing attacks. Insufficient password

policies therefore lead to concerns whether an identity can be trusted or not. Non-existent or poor requirements for password change (update) and revocation also affect the trustworthiness of credentials. With infinite password lifetime, attackers can exploit compromised credentials as long as the user account is active. Policy incompliance means that policies exist, but that they are not being followed to e.g. due to lack of policy enforcement. It does not help to have password length and complexity requirements if the technical platform still allows users to select shorter and weaker passwords. Further, many users will continue to reuse their passwords after expiry, despite a policy stating that passwords are valid for 90 days and that reuse is not allowed. Lack of policies in other IdM areas will similarly lead to weaknesses that can be exploited.

3 Identity assurance frameworks

The previous section introduced the steps of the IdM lifecycle and threats that are relevant to each of these. Baldwin et al. [5] state that identity assurance is *concerned with the proper management of risks associated with identity management.* Identity assurance contributes to ensure *confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and confidence that the individual who uses the credential is the individual to whom the credential was issued* [7]. Identity assurance frameworks consider the threats associated with each IdM lifecycle phase, and specify security requirements to mitigate them.

Many governments around the world, including the Norwegian, the Australian and the US, have developed government strategies to provide online services to their citizens, and to make electronic communication between citizens and the public services a primary choice. There are several legal requirements that regulate such communication, and proper identity management and proper management of identity assurance levels are essential to fulfill them. Consequently, each of these governments have developed identity assurance frameworks: The Norwegian Framework for Authentication and Non-repudiation with and within the Public Sector (FANR) [1], the Australian National e-Authentication Framework (NeAF) [2] and the US National Institute of Standards and Technology (NIST) Electronic Authentication Guideline [7].

Security requirements for each IdM lifecycle phase are bundled to form identity assurance levels; the higher the assurance level, the stricter requirements. Assurance levels can be seen as the levels of trust associated with a credential [9], and information about the assurance level of a digital identity can be used by service providers to determine whether they trust the identity presented to them or not. The US government, for instance, defines four identity assurance levels [3]:

- Level 1: Little or no confidence in the asserted identity's validity
- Level 2: Some confidence in the asserted identity's validity
- Level 3: High confidence in the asserted identity's validity

– Level 4: Very high confidence in the asserted identity's validity

Identities that fulfill requirements at level 1 can be used to access content that has limited concerns regarding confidentiality, integrity and availability, while identities fulfilling level 4 requirements can be used to access assets at the highest classification level. This will balance needs for usability and security.

In Table 1 we provide a summary of the IdM lifecycle phases and activities we presented in section 2, and a third column to illustrate which of the lifecycle phases and activities each assurance framework cover[2]. Our claim is that identity assurance frameworks should cover all phases, and all important activities of the IdM lifecycle to establish trustworthy IdM. Non-existence of requirements may lead to situations where identity risks are not being properly managed.

Table 1. IdM Lifecycle and assurance framework coverage

IdM Lifecycle Phase	**Lifecycle activity**	**Framework coverage**		
		FANR	NeAF	NIST
Create	Credential delivery	x	x	x
	Identity proofing		x	x
	Attribute registration			x
Use	Authentication	x	x	x
	Use of assertions (SSO/federated SSO)			x
	Attribute sharing			
Update	Renew credential		x	x
	Update attributes			
	Reactivate user account		x	x
Revoke	Suspend attributes		x	
	Delete identity		x	x
	Distribute revocation lists		x	x

4 Discussion

As Table 1 illustrates, the most extensive assurance framework of the three we have investigated is the NIST Electronic Authentication Guideline. Both the Australian and the Norwegian frameworks have shortage of requirements for several of the IdM lifecycle activities. Madsen and Itoh [8] state that if there are factors in one lifecycle activity causing low assurance, then this will determine the total assurance level, even if other areas are fully covered at higher assurance levels. In practice this means that even if services offered e.g. by the Norwegian

[2] An x indicates that the framework includes requirements for the given activity, however, the completeness and quality of the requirements are not considered.

government use authentication mechanisms that satisfy assurance level 4, the full service should be considered to satisfy assurance level 1 at best, since there are no requirements for use of SSO assertions (online services offered by the Norwegian government use federated single-sign-on). We will primarily use the Norwegian framework [1] as example in the following discussion.

The Norwegian framework specifies requirements for the creation phase only targeted at credential delivery. Consequently, threats towards the other activities in the creation phase will not be mitigated unless the identity providers implement security controls specified outside the scope of the framework. There are theoretical possibilities that false identity attributes can be registered for a person, and that identities are created for persons with false aliases and so on since there are no common rules for identity proofing and attribute registration. One can also question the quality of created credentials if there are no further specifications regarding credential generation, including key lengths, password strengths and the like.

For the use phase there are requirements targeted at authentication activity. In isolation, the authentication requirements in the Norwegian framework seems to be sufficient in that the quality of the authentication mechanisms shall improve with increasing assurance levels. However, since the identity proofing and other credential quality requirements during the creation phase are not in place there is still a risk that credentials in use are of low quality, and therefore exposed to guessing attacks or brute force attacks. Further, the framework does not specify any protection requirements for use of assertions. If the assertions in SSO and federated SSO environments are not properly protected, an attacker can intercept the communication between a user and a public service, copy the assertion, and craft his own service requests with valid assertions included. In this way an attacker can impersonate a user without a need to know access credentials. None of the three investigated identity assurance frameworks specify requirements for the attribute sharing activity. Thomas and Meinel [10] claim that *a verification of an attribute might not be desired as long as a user is not involved in transactions that require it.* As such, the lack of attribute sharing requirements may indicate that there is only a very limited set of attributes being shared in the government systems and that attributes are not being used as source for authorization decisions. If this is not true, however, Thomas and Meinel's advice to implement mechanisms to verify the quality and integrity of shared identity attributes should be followed [10].

Both the Australian (NeAF) and US (NIST) frameworks cover important aspects of the identity update and revocation phases, except that they do not specify requirements on updating and suspending attributes. The reason for omitting such requirements may be similar to what we identified for attribute sharing in the use phase. The Norwegian framework, on the other hand, fails to target the update and revocation phases at large. Users of the Norwegian framework must therefore on an individual basis define security controls to mitigate the threats against the update and revocation phases.

All the government frameworks are developed to facilitate common identity management practices throughout government agencies, and reuse of authentication services or access credentials across online services offered by the governments. Based on the discussion above one can argue that this goal can be fulfilled by following NeAF and NIST guidelines. The Norwegian identity assurance framework [1], on the other hand, has considerable limitations. The Norwegian framework states that *"the factors used to separate between security levels* [read: assurance levels] *are not exhaustive."*. This understatement is consistent with our analysis that shows there are many factors that are not considered at all. The consequence is that service providers independently need to fill in the gaps where the framework is incomplete. The probability that two independent organizations solves this task completely different is high. There are at least two challenges related to this:

- Specifications, policies and technical solutions will likely be inconsistent. This will result in lack of interoperability between systems, and thus prevent reuse of solutions.
- Each organization will specify different requirements and policies for each assurance level. It will be difficult to assess the assurance level against trustworthiness of the digital identities if there are no common definitions of what each assurance level include.

Madsen and Itoh [8] took at technical view to explain challenges related to identity assurance, and related technical interoperability issues. Our results show that challenges with identity assurance can be elevated to a higher level if identity assurance frameworks are not developed with an holistic view on the identity management lifecycle, i.e. it must be developed to include security requirements that mitigate current threats towards each lifecycle phase. The trust an entity will associate with a digital identity will depend on *all the processes, technologies, and protections followed by the identity provider and on which the digital identity were based* [8]. That being said, the Norwegian Government and public administrations have had success with implementation of a common authentication service for the public sector. The main reason for this is that one common entity, the Agency for Public Management and eGovernment (Difi)[3], has been responsible for realization of a public authentication service (MinID/ID-porten). Norwegian public administrations can integrate their online services with this common authentication portal. The chance of having interoperable, federated SSO enabled, authentication services without this model would have been low without considerable efforts to improve the common Norwegian identity assurance framework, or without substantial coordination activities between the public services.

5 Conlcusion

The essence of information security is to protect confidentiality, integrity and availability of assets. To achieve this we need to know whether the entity re-

[3] www.difi.no

questing an asset is authorized or not, and consequently we need to determine the identity of the requestor. Identity management defines the processes and policies to create, use, update and revoke digital identities. IdM is as such essential to ensure information security. Identity assurance frameworks specify requirements targeting the different phases of the identity management lifecycle, and are intended to specify and determine the trustworthiness of digital identities.

In this paper we studied the Norwegian Framework for Authentication and Non-repudiation in Electronic Communication with and within the Public sector, the Australian National e-Authentication framework, and the US Electronic Authentication Guideline as examples of existing identity assurance frameworks. We saw that these frameworks have considerable deviations in coverage when it comes to targeting security requirements towards the identity management lifecycle phases and activities. The paper illustrates the importance of specifying assurance frameworks that takes a holistic view of the identity management lifecycle and related threats.

References

1. Framework for autehntication and non-repudiation in electronic communication with and within the public sector (norwegian title: Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. Tech. rep., Det kongelige fornyings og administrasjonsdepartementet, Norwegian Government (2008)
2. National e-authentication framework. Tech. rep., Australian Government, Department of Finance and Deregulation (2009)
3. E-authentication guidance for federal agencies. Tech. Rep. OMB Memorandum M-04-04 (2011)
4. Information technology - security techniques - a framework for identity management - part 1: Terminology and concepts. Tech. Rep. ISO/IEC 24760-1, ISO/IEC (2011)
5. Baldwin, A., Mont, M.C., Shiu, S.: On identity assurance in the presence of federated identity management systems. In: Proceedings of the 2007 ACM workshop on Digital identity management. DIM '07 (2007)
6. Bertino, E., Takahashi, K.: Identity Management - Concepts, Technologies and Systems. Artech House (2011)
7. Burr, W.E., Dodson, D.F., Newton, E.M., Perlner, R.A., Polk, W.T., Gupta, S., Nabbus, E.A.: Electronic authentication guideline. Tech. Rep. Special Publication 800-63-1, National Institute of Standards and Technology (2011)
8. Madsen, P., Itoh, H.: Challenges to supporting federated assurance. Computer 42(5), 42 –49 (may 2009)
9. Soutar, C., Brenan, J.: Identity assurance framework: Overview. Tech. rep., Kantara initiative (2010)
10. Thomas, I., Meinel, C.: An attribute assurance framework to define and match trust in identity attributes. In: Web Services (ICWS), 2011 IEEE International Conference on. pp. 580 –587 (july 2011)