FIDIS

Future of Identity in the Information Society

Title:	"D14.7: Analysis of contemporary security techniques with respect to identification in business processes"
Author:	WP14
Editors:	Rani Husseiki, Dennis Gessner (SIRRIX, Germany)
Reviewers:	Rainer Böhme (TUD), Jozef Vyskoc (VAF)
Identifier:	D14.7
Type:	[Deliverable]
Version:	1.0
Date:	Monday, 10 August 2009
Status:	[Final]
Class:	[Public]
File:	fidis_wp14_d14.7_v1.0_final.doc

Summary

In this deliverable, we give an overview of widely used identification and authentication techniques, namely, password-based authentication, smartcards, digital certificates and biometrics.

Then, we lay down the requirements for identification schemes from the perspective of enterprises, business collaborators, and legal and standardization institutions.

Afterwards, we shed light on the different properties of contemporary identification schemes that are mostly considered for business processes. Particularly, we focus on scalability and flexibility, trustworthiness across domains, robustness, anonymity, usability, efficient identity management, and legal grounds.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

PLEASE NOTE: This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. ***Tilburg University***[1]	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Centre Technique de la Gendarmerie Nationale (CTGN)	France
19. ***Netherlands Forensic Institute (NFI)***[2]	Netherlands
20. ***Virtual Identity and Privacy Research Center (VIP)***[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

[1] Legal name: Stichting Katholieke Universiteit Brabant

[2] Legal name: Ministerie Van Justitie

[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
1.0		• Initial Release

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 (Introduction)	Rani Husseiki (Sirrix AG)
2 (Digital Identities)	Rani Husseiki (Sirrix AG)
3 (End-user Identification Techniques)	Dennis Gessner (Sirrix AG)
4 (Identification Requirements in Businesses)	Rani Husseiki (Sirrix AG)
5 (Properties of Contemporary Identification Schemes)	Rani Husseiki (Sirrix AG)
6 (Conclusion)	Rani Husseiki (Sirrix AG)

Table of Contents

1 Executive Summary

Digital identities have become a ubiquitous means for identification of users to different computing systems and services. Even if they represent a single subject (e.g. human), these identities might be different depending on the context in which there are used. However, a digital identity is only meaningful if its attributes can be verified to be authentic. For this reason, authentication and identification techniques are used in order to verify that a human is truly the subject represented by the claimed digital identity.

In this deliverable, we shed some light on four categories of end-user identification techniques: the "Authentication by knowledge" (e.g. passwords), the "Authentication by possession of hardware" (e.g. smartcards), "Authentication by measurement of biometric features", and "Authentication by possession of electronic document" (e.g. public key certificate).

While these techniques have been widely used in different contexts, the deliverable focused on their usability and application in business processes. For that, we laid down the requirements of identification schemes in enterprise environment.

Scalability and flexibility are important for addressing the needs of identification in a business process including a large number of collaborators in a wide enterprise environment. Trustworthiness across identity domains is also relevant when the business process crosses the boundaries of the organization to include collaborators from other enterprises. Robustness, mainly dependent on the security and reliability of the identification system is important when considering the sensibility of the information being handled in the scope of the business process, as is the case with internet banking. The usability aspect is also a critical factor that should be considered by an enterprise before deploying an identification or authentication scheme, and is mostly dependent on user satisfaction. Efficient identity management can play an important role in the success of an identification scheme, since collaborators identification information are expected to be revoked on a regular basis. Last but not least, the authentication standards and regulations defined and enforced by public and private organizations play a crucial role in the choice of a suitable identification scheme.

A subsequent analysis of contemporary identification and authentication techniques was performed.

It showed that security and reliability, which we see as the metrics for robustness of a certain identification systems, are subject to trade-offs. However, we can conclude that while biometrics seems to be the most secure, their combination with smartcard technology can achieve a higher security level. Therefore, enterprises which are still adopting the password-based identification schemes should start moving out of this arena which has become acknowledged to be the least secure. A shift towards smartcard infrastructures might be suitable. On the other hand, since identification techniques seem to share an almost equivalent level of reliability, which is considerably high, this reliability level should be maintained in future developments in existing technologies.

Generally speaking, the scalability requirement is currently addressed by deploying identification schemes supported by hierarchical trust models or decentralized trust models, such as in PKI schemes based on digital certificates. Interoperability seems to be a stressing factor, although enterprises and organizations in many fields still lack this property in their identification schemes. These institutions would rather be on the safe side when choosing an identification scheme by complying with common and widely deployed standards. Trustworthiness across domains is also still in its early stages, since enabling technologies such as Trusted Computing are not widely deployed in enterprises. Nevertheless, scalable PKIs are being used for this purpose, although they might not fulfil the exact security requirements. Efficient identity management is also becoming more and more considered by enterprises, especially with deployment of federated identity management schemes.

It can be also said that anonymity is not widely addressed in current identification systems, though research in the area if anonymous authentication is quite advanced and many schemes have been specified. Deployment of these schemes is however not perceivable. Considering the anonymity requirements by employees stated in the previous chapter, business processes are increasingly facing this requirement, which means that enterprises and service providers should start considering state of the art technologies addressing this issue.

Finally, both the identification standards defined by official institutions, or legal agreements in the form of SLAs are becoming widely considered by enterprises for this business processes. However, an enterprise might have to choose between complying to a certain standard in the context of identification, or having its proprietary identification scheme and adhering to an agreement with the peer business partner or customer. This is a choice that needs to be wisely done by the enterprise considering many technical, legal and management overhead factors.

2 Introduction

Business processes rely on the strong collaboration of partners, customers and employees. The identification and authentication of these collaborators is indispensable in most of the cases. In a digital environment, these collaborators are represented using their digital identity. Therefore, digital identification techniques have become sophisticated enough to account for a reliable authentication of collaborators.

Enterprises are therefore interested in deploying identification schemes in their IT infrastructure that meet their expectations in many respects. Basically, enterprises as well as peer collaborators want to establish trust in the claim of identity by a peer collaborator to the business process.

Identification and authentication schemes range from simple username and password combination to sophisticated smartcard technology or digital certificates. Each of these schemes has advantages and disadvantages with respect to the other, and is deployed according to a set of requirements.

In fact, the requirements that govern the choice of an identification and authentication system can be categorized into business requirements, employees' and customers' requirements as well as legal and standardization requirements.

Suitable technologies, models, and metrics are typically defined by entities concerned in choosing an identification system. Research and development has achieved quite a lot in terms of fulfillment of requirements.

In this deliverable, we start by stating the definition of a *digital identity* in chapter 2, and we explain its relevance to enterprises in the context of authentication.

In chapter 3, we give an overview of widely used identification and authentication techniques, namely, password-based authentication, smartcards, digital certificates and biometrics

Then, in chapter 4, we attempt to define the requirements for identification schemes from the perspective of enterprises, business collaborators, and legal and standardization institutions. Particularly, we focus on scalability and flexibility, trustworthiness across domains, robustness, anonymity, usability, efficient identity management, and legal grounds.

Afterwards, in light of these requirements, chapter 5 sheds light on the different properties of contemporary identification schemes that are mostly considered for business processes.

The requirements listed in chapter 4 are generic requirements that should be – at least partially – fulfilled by any deployed solution, whereas the properties of identification techniques described in chapter 5 reflect the current status of these techniques with respect to the requirements of chapter 4.

3 Digital Identities

Kim Cameron defined *digital identity* as “the digital representation of a set of claims made by one digital subject about itself or another digital subject” [Cameron, 2005]. While digital subjects can represent either humans or non-humans (device, computers, digital resources…), the value of a digital identity pertains only in the context in which it is used: a digital identity used for identification in an enterprise’s network could be irrelevant for identification of an email account, for performing a digital signature on a document, or for accessing a private place. Hence, for a single entity, its digital identity does not need to be unified across different contexts, but can rather be unique in each domain of application.

However, any digital identity is meaningful only if the attributes it associates to the corresponding digital subject are authentic. Therefore, authentication mechanisms are crucial to ensure correct identification and to prevent identity theft. Authentication mechanisms used for correctly authenticating a digital identity are mainly implemented in software and hardware, but can sometimes rely on physical authentication techniques such as iris scanning for human unique identification instead of relying on the possession of hardware id-token.

A digital identity can be presented by several means. In many cases, the authenticity of a digital identity is crucial to its value. This is why a username is associated to a password, a Public Certificate is signed by a Certificate Authority’s private key, a bankcard is associated to a PIN, a digital signature is associated to a private key… passwords, private keys, PINs are secrets known only to the corresponding digital subject. Their confidentiality to the digital subject is necessary to ensure prevention of identity theft. Since a digital identity is only relevant if its authenticity can be proven, it is crucial how the corresponding secret is protected. In some cases, the secret can be memorized (in the case of a PIN or the answer to a challenge-question), but in other cases it needs to be stored in digital form, mainly on hardware devices such as hard disks or smartcards. In most cases, the secret has to be provided to other hardware or software in order to be processed for authenticating the digital identity.

For this reason, encryption schemes are widely used nowadays to protect the secret corresponding to digital identities. Authentication mechanisms rely heavily on those encryption schemes to ensure secure authentication of digital identity. The encryption schemes are used to protect the secret both in storage and during communication for authentication purposes. In other cases, the digital identity is preserved thanks to the uniqueness of identification information associated to a certain person, such as in the case of biometrics.

In any case, in a digital context, it is always hard to tie a certain physical person with a certain digital identity. This is the reason why (identity) fraud can take place, and attacks can be launched against the identity of users.

In this context, the ability to verify a user’s identity has become an essential foundation for trust in business relationships.

Authentication solutions help to establish trust in the identity of the authenticating person, by ensuring that the person is who she/he claims to be. They serve as a basis for critical security mechanisms such as granting the right people the right access to the right resources at the right time. Most enterprises have implemented policies that specify the relationships between authenticated users and resources through the control of access to networks, services and applications. Authentication and access control are both integral to what today is commonly termed as (corporate) identity management.

The two main use cases for digital identities within an enterprise are physical and logical access.

- Digital identification is used as a means for restricting access to buildings and facilities. Card-based physical access technology has been deployed in a large number of enterprises.
- Enterprises also need effective mechanisms for controlling access to networks, systems, and applications. An authorization system based on digital identities allows securing logical access to resources by controlling employee access to workstations, intranets, virtual private networks (VPNs), databases, services and other logical information assets.

To summarize, digital identities constitute a cornerstone in the identification techniques that are deployed in businesses in the scope of authentication and authorization systems. Linking the attributes of the digital identity of a business collaborator (a digital subject) to their corresponding authentication information is crucial for establishing trust in the identity of the collaborator (user) before granting him access to resources.

4 End-user Identification Techniques

Different types of end-user identification techniques are used within business environments depending on the trust model, the required security and practicality levels (among other requirements). In this chapter, we give an explanation of different authentication methods used in IT systems nowadays, which are detailed in [Eckert, 2004].

4.1 Authentication by knowledge

Currently the mostly used methods are based on a piece of knowledge exclusive to the authenticating user. Generally, a technique is used where a user or guest has to authenticate himself with the knowledge of a special secret. Therefore so-called challenge-response-techniques (3.1.2) can be used. In practice, the mostly used methods of these authentication methods are probably password-based methods, which are described in the following.

4.1.1 Password based

With the aid of password-based methods, a subject (in case of operating systems, usually the subject is the user) authenticates himself by the fact that he can prove the knowledge of a predefined secret. This method is currently used in many authentication schemes across many systems and service providers. The system has to store the passwords in a way that no unauthorized access to these passwords is possible. Therefore, usually cryptographic methods (more precisely: cryptographic hash functions) are used, which give the possibility to ensure the secrecy of the stored passwords. In general, it is not the password itself which is stored on the system, but rather a cryptographic hash-value of the password in combination with further information which characterizes the user. Thanks to the one-way-functionality of hash-functions, it is guaranteed that no one can get access to the password unless he accepts a huge effort to calculate it (or a hash collision) out of the sole knowledge of its stored hash-value. This leads to the fact that the security of the password, among others, strongly depends on the strength of the hash-method. In some cases it is also problematic that the password-file with its sensible data inside is open for read-access, which gives an attacker the possibility to use chosen-plaintext-attacks. A person who already has access to the system can choose a password for himself, and observe the corresponding encrypted form of the password in the password-file. Repeating that with a large number of chosen passwords, he can start deriving information about the encryption algorithm used for passwords. Eventually, he would be able to retrieve the passwords of other users. These kinds of attacks are known as “password cracking” and might come in different forms, such as dictionary attacks (guessing the password based on likely possibilities) or rainbow tables (lookup tables offering a time-memory trade-off in recovering the plaintext password). There are a lot of freely accessible programs which try to break the stored passwords with a systematic use of dictionaries.

Not less problematic is the fact that the security of this authentication method strongly depends on how wisely the password itself is chosen and how it is handled outside the technical system. A highly secure password does not guarantee any security to the authentication process if an attacker is able to get it just by asking the right questions in the right situations. This kind of attacks falls in the category of so-called “social engineering”.

Here an attacker tempts his victim to give away his secret password asking some clever questions.

The choice of the password is a critical issue since it affects its robustness against dictionary attacks. Guidelines have been proposed to help users define such secure passwords, e.g.:

- The password or parts of it should not contain the user's first or second name.
- The password should not contain any word that could be consulted out of a dictionary. Also it should be at least eight symbols long.
- There should be at least one special sign.
- It should not be constructed from a simple combination taken from the keyboard (like "qwert").
- The password should contain preferably many different numbers and letters.
- It should be changed in regular time intervals, although a controversy exists around frequent password changing. An enterprise's policy requiring frequent password changing might lead users to chose easier-to-guess passwords, e.g., by using a series of simple passwords ending with an incrementing number (pass01, pass02, etc…).
- The system should check automatically if the user violates one or more predefined password-rules.

Nevertheless, passwords which are defined according to these guidelines are generally hard to remember, which incites users to write them down on papers instead of memorizing them. This has serious security implications since it increases the risk of password disclosure.

Moreover, the system should only allow a predefined low number of unsuccessful attempts to enter the login-information. After this, the system should lock the account. (This might give the opportunity for attackers to launch denial-of-service attacks, but is still necessary to defend against brute-force attacks).

4.1.1.1 One-time password

As an alternative to the classical password-based identification methods, one-time-passwords (OTP) could be used. As the name indicates, these passwords are used only once – one per authentication process. Thus it can be proven that the knowledge of the password does not give an attacker the possibility of a successful sniffing attack[4]. In fact, an opportunity to eavesdrop the login procedure gives an attacker no advantage, as the OTP used there (and possibly sniffed) will not be valid for subsequent logins. That means that OTP are appropriate for scenarios where one cannot rule out eavesdropping of the communication between user and a system (e.g., remote login over untrusted and unencrypted channels).

Such a method is often used inside external systems, where no other established security-technology like Kerberos or Secure Shell is available.

[4] Password sniffing includes collection of the first several characters of a user session requiring entry of a password, with a reasonable assumption that the user name and password are contained in these characters.

The question here is how such a one-time password should be created, in order to avoid burden on the user as much as possible and without giving the attacker the chance to guess a “not yet used” one-time password correctly. A possible solution can be to use a oneway-function. A conception of such a scheme was firstly defined in 1981 by Lesli Lamport [Lamport, 1981]. Later his concept was implemented with a method called S/Key [Haller, 1994] and was spread in the Unix/Linux-world. The following gives a short description of this method.

S/Key-method

Originally the S/Key-method was developed to solve problems regarding password-sniffing-programs in client-server-based communicating systems. Later, based on the S/Key-method, some other OTP-methods were developed as specified in RFC2289 [RFC2289].

- The method starts with a secret password *s*, which is predefined between the user and its client-PC. What is special about *s* is that the server does not know anything about it. This makes it unnecessary to transmit the value of *s* between client and server.
- With the use of cryptographic hash-functions as one-way-function *f,* the secret *s*, and a seed-value *k*, the client calculates a sequence of one-time-usable passwords. This also means that there is no need to send the password *s* from the client to the server.
- To initialize the process, the client sends the last password of the sequence with the seed-value *k* to the server. *[over a secure channel / in a secure environment?!]*
- The server stores the last used sequence-number *i+1* and the corresponding one-time-password.
- When the user logs in again, he is shown the sequence number *i*
- Based on this sequence number *i* (a number between 1 and 100), a server defines how often a hash-function has to be used upon the secret password to get the right one-time-password.
- The client gets this number in combination with the seed-value *k*, and calculates the *i*-th password in the following way:

  $$p_i = f^{\,i}(s \mid k)$$

  The seed is unique for the server and gives the user the possibility to use the same password for different PCs. Thus the seed gets a similar functionality as the salt[5] value of the common Unix login.
- The system gives the user the possibility to create a sequence of one-time-passwords, which would make it possible for him to log in via an insecure computer. Therefore he

[5] A set of random bits used as input to the hash function applied over passwords in order to complicate dictionary attacks. Since salt values associated to a password are stored separately, obtaining the hash value of the password would not be enough for an attacker to perform dictionary attacks (trying common passwords).

has to save the fore-created passwords on an external storage and has to enter them manually later.[6] (A sheet of paper can serve as storage in the simplest case).

The S/Key system design includes a sophisticated method to transform generated password (usually incomprehensible and hard to remember) into more easily remembered sequence of short words. Therefore, the robustness of the password is lower compared to normal passwords chosen according to the guidelines listed above. It is just that the generated sequence is easier to remember by the user, which helps keeping him from writing the password down instead of memorizing it.

OTP-Token

An often used system for authentication with one-time-passwords is the RSA SecurID [RSA]. The authentication of a user against the server (the RSA ACE Server), is done as a two-factor-authentication where a user has to prove his identity on one the hand with the knowledge of the PIN and on the other hand with the ownership of the token. Initially, the user receives this token – a physical device with display – from a system administrator. It has a unique serial number which is also known by the server. Also the token has an implemented 64-bit symmetric key, the seed, which is also known by the server. Finally the user has an identification that is combined with the serial number of the token and the seed inside the server.

Compared with the S/Key-method, a token-based method is based on a time-synchronized method, where server and token have a synchronized clock inside. The token creates a so-called token-code every 60 seconds, which is displayed on the display of the token. Normally AES is used as hash-function[7] that is used for hashing the combination of the serial number of the token, the seed, and the current time.

An example for one of these token-generators is the key fob, a very small token that calculates a new password every 60 seconds. For authentication with the server, the user has to identify himself with his identification, the PIN and the one-time-password that was displayed on the display of the token. This method might be problematic when considering synchronization of token clock with server clock.

Similar products are the SecureID Card and the PIN-Pad Card where the user has to enter a 10 symbol password to activate the card itself.

4.1.2 Challenge-response based techniques

Challenge-Response based techniques are a generalisation of authentication mechanisms based on knowledge. The idea behind this mechanism is similar to one-time passwords, where the secret does not have to be transferred to the login PC multiple times, but a new password

[6] It has to be noted that the number *i* must be decreased after each login to provide a sequence of one-time passwords in such a way that if an eavesdropper obtains a number of one-time passwords used in past logins it is impossible (assuming one-way function *f* is used) to calculate the correct password used in the next login.

[7] AES-hash is largely derivative of Davies-Meyer and its padding is derived from other hashing functions [Cohen, 2001].

is generated for each login. This is achieved by pre-appointing questions and answers with the host system.

4.1.2.1 Mechanisms with symmetric cryptography

Authentication with symmetric cryptography requires both parties to possess the same encryption algorithm E, as well as a shared key. Let CN (Card Number) be a number uniquely identifying a chipcard. Further, let K_r be the key used to communicate with the chipcard CN and which is stored locally in a database. If the card is authentic, then K_CN = K_r. The following example explains this in more detail:

At login, a user inserts his chipcard into a reader connected to his computer. The PC reads the CN out of the chipcard and queries its database for the according key K_r. If a database entry exists, the PC sends a challenge to the chipcard by generating a new random number RND. The chipcard will now encrypt the received RND with its internal key K_{CN} to $C = E_{Kcn}$ (RND) and sends the result back to the PC.

The PC itself verifies the received result by calculating $C' = E_{Kr}$ (RND). The chipcard (and therefore the user) is authenticated, if C = C'.

Another possibility is mutual authentication, where the client also generates a challenge for the PC, who has to provide the correct result.

Challenge-response protocols with crypto systems can nowadays be found in many fields of mobile communication, such as the authentication of mobile phones in GSM networks or in wireless LAN authentication.

One advantage of this procedure is that an attacker cannot re-use the calculated encrypted authentication credential, because the random number RND is generated fresh each time[8] (similar to the one-time password scenario). However, if the attacker controls the communication channel between client and server, it is possible to perform known-plaintext attacks, if the exchanged messages are transmitted unencrypted. This attack tries to gain knowledge of the used encryption key by observing the encrypted response calculated with the RND, which was transmitted in plaintext. Additionally, it is possible to perform dictionary attacks, where the attacker tries to guess the secret key used by encrypting the RND and comparing it to the transmitted ciphertext. One variant of this attack was for example successfully executed against version 4 of the Kerberos protocol. However, this problem can easily be solved by either encrypting the RND value before transmitting or by using approaches based on zero-knowledge techniques (3.1.3).

4.1.2.2 Mechanisms with asymmetric cryptography

In contrast to symmetric cryptography, a PC using asymmetric cryptography only needs the public key K_E^{CN} of the chipcard CN. After a login request, the PC generates a random number RND, which he sends as a challenge to the chipcard. The card will sign it with its private key K_D^{CN} returning the digital signature Sig = D(RND, K_D^{CN}) as response. The PC will verify the signature with the known public key of the chipcard and check whether the signed RND value

[8] Assuming that it is picked randomly from a large enough space of possible values.

matches the previously transferred RND. One advantage of this method is that – in contrast to symmetric cryptography – PC and chipcard do not need to share a secret. Therefore, there is no need for an initial protocol to generate a shared secret. However, the public key of the chipcard needs to be authentic, which requires a trusted public key infrastructure (PKI).

Alternatively, the PC can request a valid client certificate signed by a trusted third party upon each login request. This variant is for example used in the SSL protocol family.

One requirement for the usage of both methods is a secure (pseudo) random number generator, which produces high-entropy random numbers with ideally no period. This shall hinder an attacker to collect challenge- and response tuples and wait until a random number is chosen again, such that he can replay the previously collected response. Also, missing mutual authentication could allow an attacker to spoof a server and use the client as an encryption oracle.

4.2 Authentication by possession / ownership of hardware

In contrast to knowledge-based authentication-techniques, chipcards are typically used in ownership-based techniques. Possible alternatives like USB tokens will not be described in more detail, since in most cases their underlying concepts are the same.

Today's chipcards are plastic cards of different types. Simple ones only have EEPROM-memory of some hundred up to 8Kbyte size. These cards are very cheap to produce, but do not offer any intelligent hardware inside the cards. Such cards were often used as health insurance cards. Among simple cards, one can find more intelligent cards, equipped with additional security hardware. Their area of application is for example PIN-storage or PIN check. If there is an additional microcontroller inside the card, it is called a "smartcard". An example of such a smartcard is the "Geldkarte" used in Germany for micro-payments. A short overview of the architecture, operating systems and area of application of smartcards is given in a book by Rankl and Effing [Effing et al., 1999].

4.2.1 Architecture

Predefined requirements of card dimensions, the order of the card contacts, supported signals and voltage levels, and transmission protocols are specified in the ISO 7816 standard. Contact-based smartcards communicate with eight contacts C1-C8, contactless smartcards use radio frequency communication based on the ISO/IEC 14443 standard.

In principle one can differentiate between three different types of card sizes, type ID-1, ID-000 and ID-00. The standard size is type ID-1 and has the size of a normal credit card. Central device of the chipcard is the microcontroller, which is located directly below the contacts of the card. On the one hand there are simple chips with 8-bit or 16-bit processors. High-end microcontroller offer 32-bit processors with up to 320 Kbyte of ROM. This kind of ROM-memory is mask-programmed and normally contains the card operating system or cryptographic software for encryption, signing or the calculation of hash values. Moreover, smartcards offer up to 16 Kbyte RAM- and up to 400 Kbyte EEPROM-memory.

Most smartcards use symmetric techniques for encryption, since these methods consume less memory than asymmetric techniques. Also the encryption itself is much faster with symmetric techniques.

In the case of smartcards based on asymmetric techniques, the generation of RSA keys (which is very time consuming) is often done outside the card. As the computing time of the RSA-encryption strongly depends on the employed key length, often keys with the length of 512, 768 or 1024 bits were used. Especially the first two lengths do not satisfy the current high-security requirements. To solve this problem, modern smartcards often use additional components, the Additional Units (AU). These components could be a Memory Management Unit (MMU) or co-processors, which speed up the RSA encryption.

4.2.2 Security

Smartcards are considered to be a strong authentication and identification technology. The reason is that it is somewhat tamper-resistant and implements cryptographic protocols that allow only authorized access to the secret data stored on the card based on a correctly supplied PIN. Nevertheless, smartcards might be subject to side-channels attacks, such as differential power analysis (measuring the exact time and electric power required for performing a certain cryptographic operation on the card) [Messerges et al., 1999], or physical disassembly (using acids and abrasives to disassemble the chip and get direct access to the on-board microprocessor) [Kömmerling et al., 1999].

However, most attacks today are considered not to be efficient, which means that either the costs associated to break the system are far more than the cost of the system itself, or that the attacker has to spend several or hundred years of computing power to break into a single transaction [Surendran, 1999]. Smartcard technology has been developing substantially ahead of cracker methods, which made it robust against many vulnerabilities that can be exploited. Nevertheless, the latest smartcard technologies need to be deployed as soon as they are standardized in order to cope with the developing cracking methods. Otherwise, old smartcard-based infrastructures would be vulnerable to new attacks.

4.3 Authentication by measurement of biometric features

4.3.1 Biometric techniques

In [D3.2, p. 62], an overview of biometric techniques was given, which included:

- **Face**: analyses facial human characteristics
- **Voice**: analyses the tone, pitch, cadence and frequency of a person’s voice
- **Fingerprint**: analyses an individual’s unique fingerprints
- **Hand geometry**: analyses the shape of the hand and the length of the fingers
- **Iris**: analyses the coloured ring surrounding the pupil of the eye
- **Retina**: analyses the capillary vessels at the back of the eye

- **Vein**: analyses the patterns of veins, traces and shapes in the back of the hand and the wrist using infra-red light
- **Signature**: analysis of the way in which a person signs their name
- **Keystroke dynamics**: analysis of the way a person types

4.3.2 Biometrical authentication

According to [D3.2], a biometric system is used either to *identify* or *verify* a person. *Identification* is the process of comparing a biometric data sample against all those enrolled in the database with their respective biometric data (reference template) in order to find the identity of the person trying to access the system. *Verification* however involves the process of comparing a biometric data sample against a single reference template of a particular enrolled individual in order to confirm a claim of identity of that person. When a biometric system correctly identifies a person, then the result of the identification process is a *true positive*, whereas if the system correctly rejects a person as not matching the person, the result is a *true negative*.

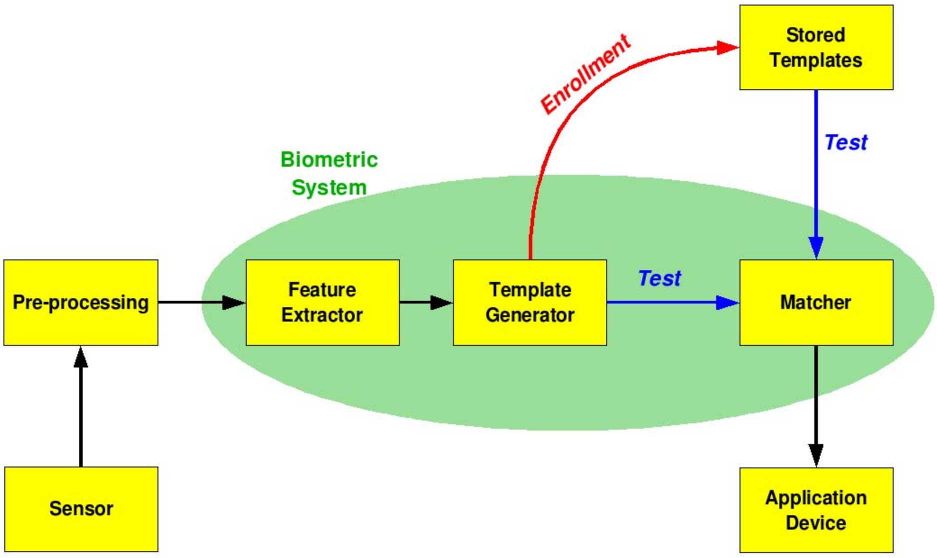


Fig.1: Biometric system diagram [Damato, 2007]

The Sensor is the interface between the human and the system which receives all the input from the human organ, e.g., through an optical scan. The pre-processing stage includes removing undesirable artifacts from the obtained image. Then, the sought feature is extracted from the image, and is used to create a template, which is a synthesis of relevant characteristics of the source that are only relevant to this particular biometric system. In the case of enrollment, the template is stored (e.g. first time). If it is an authentication procedure, the template is compared to the stored template of the corresponding human by the Matcher. The result of the comparison is returned to the Application Device, to be used as input to the decision making in the authentication procedure.

4.3.3 Security of biometric techniques

Biometrics have been considered as an effective means for reliable and secure identification of individuals. For example, fingerprints have some advantages over other authentication schemes (whether passwords or id-tokens) since they reflect a piece of information that can hardly be leaked to – or stolen by – an attacker.

Nevertheless, biometric techniques for identification still have some margin for failure, just like any other authentication scheme. In particular, biometric identification solutions might suffer from False Accept Rate (FAR) and False Reject Rate (FRR). Moreover, fingerprints can be faked, e.g. by taking the traces on a glass that has been touched, and developing real "fingerprints" out of them. Forensic studies take this possibility into consideration during investigations.

Using biometric data in combination with other authentication means such as a smartcard can greatly enhance the overall security and reliability of the system, as will be shown later.

4.4 Authentication by possession of electronic document

Authentication can also be performed based on the possession of a certified electronic document. This electronic document comes in the form of an attachment to the message being sent during the authentication process, and includes information about the digital subject which are previously certified by a certification authority. A common type of electronic documents used in this category of authentication schemes is *digital certificates* also known as *public key certificates*.

In [Arturo, 2004] an overview of digital certificates is given. Since digital certificates can be easily attached to a message in a protocol, they can be used also to perform digital signatures of the message to which they are attached, therefore proving the authenticity of the sender.

Digital signatures are extraordinary important mechanism. In their presentation paper on public key cryptography, Diffie and Hellman [Maurer and Wolf, 1999] proposed the creation of public directories where public keys could be registered by their owners (similar to a universal telephone directory). However, the problems involved in having such huge directories soon prompted a search for a more viable solution. Kohnfelder was the first to propose the idea of public key certificates, or digital identity certificates.

3.4.1 Digital certificates

Briefly, a public key certificate or a digital identity certificate is an electronic document digitally signed by an authority, usually called a Certification Authority (hereinafter CA). The CA guarantees the association between a public key and a particular person identified by their name or any other information, which permits their unique identification. Hence, individuals wishing to obtain a certificate must be identified and authenticated by a CA, more or less rigorously depending on the use the certificate is to be put to.

Thus authentication could range from requiring no personal appearance to requiring personal appearance of the candidate, authenticated by an accrediting document (such as a passport).

Evidently, in the case of the former type of authentication, messages signed with such a public key will lack trustworthiness.

Digital certificates – authenticating either identity or attributes – can be stored in a file with the private key or, more securely, in a cryptographic smart card which can execute the signing operation. This means that the private key must never leave the chip. This prevents it from being be captured by a malicious terminal. Consequently, a user B wishing to verify the authorship and integrity of a signed message from A, must follow the following steps to obtain A's public key:

1. Obtain a digital identity certificate from A (which will usually accompany the message)

2. Extract the public key from A's digital identity certificate.

3. Verify the public key by checking the CA's signature on the certificate.

If everything matches, the public key is guaranteed by a CA which is trusted by B.

Technically, the digital certificates currently in use are standardized by the ITU-T and the ISO/IEC in recommendation X.509v.3. An X.509v3 certificate includes a set of data fields, some of which are mandatory and others optional. Among the mandatory fields are certificate number, signature algorithm identification, CA signer name, validity period, name of the holder, public key and signature algorithm to be used.

As for the optional fields, the most important extensions are those which provide additional information about users or other specific data about organizations. Extensions can be used to define more precisely the purpose of a public key (key encryption, data encryption, authentication, key negotiation, electronic signature, etc.), the policy of the CA, its purpose, etc.

3.4.2 Attribute certificates

Recently, another type of certificate has begun to be deployed. It does not certify the association between a public key and its holder (in fact no public key is included), but includes other information that is sometimes needed to guarantee that the certificate holder is empowered to act: for example, whether the holder is authorized to sign a certain type of document, whether there is a limit to the amount of money transacted, if more than one signature is needed, etc.

This information could be included in a digital identity certificate – by using the extensions described above – but, although the association between individual and key pair is usually long lasting, signing rights are usually short-lived.

Also, if a certificate is intended to be used for a number of different purposes, there will need to be a large number of extensions; one for each function. For these reasons, it would seem more reasonable to separate identity from the information authorising or restricting the use of keys for certain functions or tasks, relegating those to another short-lived certificate – without a public key. Such other certificates are known as attribute certificates and always need to be accompanied by a digital identity certificate.

3.4.3 Certification authorities

CAs are trusted, independent entities which supervise the entire life cycle of the certificates they sign. Thus they generate, publish, cancel, revoke and renew certificates (usually regenerating a certificate with the same public key and an extended expiry date).

They also often register and identify the applicants for certificates and they are sometimes responsible for generating public and private keys (although the latter is a very bad practice). From this its is eveident that the overall security ultimately depends on the security of the CA. For this reason, security measures at CAs should be very strict, both in physical terms and also in terms of the technical and managerial aspects involved. It is particularly critical to the security of the system to ensure the maximum possible confidentiality of the private key the CA uses to sign the certificates it generates. There is one very important document which all CAs offering services to the general public should make readily available to any interested party: the Certification Practices Statement (CPS). This document contains the set of standards, rules and procedures that govern the life cycle of their certificates. It should also include the responsibilities the CA has towards the users of their certificates and vice versa, and the extent of liability.

5 Identification Requirements for Businesses

A business process or business method is a collection of related, structured activities or tasks that produce a specific service or product for a particular customer. Therefore, a business process typically involves a set of activities performed by different individuals whose corresponding identities are critical to the overall process. Particularly when security is a focus, the identities of the contributors to a business process affect the decision on the disclosure of certain business data to them.

The requirements for a general identification scheme for business processes should take into consideration three categories: business requirements, employee and customer requirements, as well as standardisation or legal requirements. In the following, we try to lay down these different kinds of requirements.

5.1 Business requirements

5.1.1 Robustness

The sensibility of digital information processed nowadays within business processes has led to an increasing need for strong identification and authentication techniques in enterprise environments. This is due to the high risk associated with confidentiality breaches when a failure of the authentication system occurs. Strong, multi-factor authentication schemes are becoming widely deployed across financial, governmental and healthcare institutions. In fact, the username/password schemes are considered to be prone to failures, for obvious reasons such as customers' or employees' choice of weak passwords that can be guessed by attackers, or writing passwords down on a paper, thus exposing them to the risk of disclosure.

In high-value business-to-customer services, enterprises as well as customers cannot afford a high rate of unauthenticated access to the services, e.g. by attackers. For example, if authentication credentials used for online banking are leaked to an unauthorized user, or if the authentication system is weak enough to be cracked, this can lead to unauthorized high-value transactions by attackers.

Therefore, in 2007 a research report by Gartner [Allan, 2007] has advised organizations to "look to use stronger authentication in high-risk situations such as remote access now, and consider wider use of stronger authentication by the end of 2007 and plan for deployment during the following two to three years."

Hence, organizations are faced with a strict requirement – for their credibility, assurance of their businesses, as well as their customer's satisfaction – to implement robust and secure authentication systems that rely on reliable identification techniques. Multi-factor authentication is considered to be a good approach in this regard. It is based on user (employee or customer) credentials that require more than one piece of information from the user, part of which can be inherent to them (e.g. biometrics, fingerprints). This permits reliable identification of collaborators to a business process.

In fact, relying on a single type of information for secure and reliable identification might not always result in a robust authentication system. For example, if biometrics are used for identification alone, the process might be compromised by sophisticated attacks on the computing device receiving the biometric information, such as spyware, Trojan horses or phishing attacks. This constitutes a security risk especially when the biometric information is supplied via proprietary computing devices (e.g. fingerprint scanner built in a proprietary notebook with no secure operating system). Therefore, an identification system combining biometrics with, e.g., a PIN (authentication through knowledge) might be more robust against several types of attacks (excluding Trojan horses).

5.1.2 Scalability and flexibility

The scalability and flexibility of the identity management system (IMS)[9] is a key requirement for businesses. In fact, the procedure for identification of collaborators to a certain business process should not present an inhibiting factor or overhead for the business.

Business need to account for customers or employees accessing their networks and services, often in a widely distributed environment (e.g. international organizations with a distributed IT infrastructure). This entails the need for a scalable identity management system that can handle identification information corresponding to a large number of collaborators to the business process. This means that administration of the identity management system should be scalable enough to account for the geographically and even functionally distributed suppliers, customers and partners. This scalability can be achieved by several means, such as distributed administration roles, and hierarchical trust models (e.g. a public key infrastructure).

There is, however, a flexibility requirement that also needs to be accounted for: when creating, revoking, and modifying identification information for the sake of authentication and authorization to a certain service, these procedures must not introduce complications to the business itself, and must be as transparent as possible to collaborators. As discussed in the literature [Zheng, 2003] [Boneh, 2001], fast and flexible identity revocation is an essential requirement. An administrator should be able to revoke a collaborator credentials with little if any need for introducing any changes to the credentials of authorized users. Moreover, he should be able to revoke parts of the identification information that no longer hold true, or are not possible to verify. Therefore, the validity of parts of the identification information should be possible to revoke.

5.2 Employee and customer requirements

5.2.1 Anonymity

Anonymity is becoming an issue when identification to authenticate to a certain service is required. In fact, there is no need for every authentication session to require identification

[9] A system intended to streamline the management of user objects on one or more systems or directories. It operates on user objects, identity attributes and security privileges.

information, since the identity of the business customer or employee is sometimes not relevant when authenticating his rights. Indeed, the rights are often not connected to the identity of the collaborator, but rather to his role. This is for example the case of so-called Role-Based Access Control (RBAC) security models where identities are grouped into roles and authorization rights are associated to these roles [Sandhu et al., 1996],. These schemes assume that although identification information are usually required for authorization to a certain service, there is no absolute need for validation of the identity. Therefore, anonymity can be an important requirement by employees and customers who are afraid to be monitored in their use of the system.

5.2.2 Simplicity and Usability

Simplicity of the identification mechanisms that collaborators to a certain business process require is of high importance too. In fact, the complexity of such mechanisms can lead to either a reluctance to use the service – which might cause harm to the business – or finding simplification ways by the customer or employee, which can lead to security problems in the long run. For example, if an enterprise infrastructure requires a different set of usernames and passwords for each of the services it provides to its employees, the latter would have the tendency to set a single password for many – if not all – of his accounts, which means that a leakage of one account to another employee would let him access all the other accounts. Hence, making the identification process based on a single account for several services - whether in a single-sign-on scheme, or with a repeated password - adds simplicity for the user, but leads to a single point-of-failure.

Alternatively, the employee might tend to write down his passwords on a sheet of paper in order to remember them, which makes them more prone to disclosure. Therefore, the authentication procedures should be as transparent and simple as possible to the employee in order to avoid this kind of situations.

In this scenario, a smartcard-based identification scheme might be suitable since it requires a combination of a token owned by the user (the smartcard) and a 4-digit PIN: even if the PIN is disclosed, or the card is lost, this would not be enough for an attacker to impersonate the user. Moreover, since the PIN is small, it can be easily memorized by the user no matter how complicated it is, which helps keeping the user from writing the PIN . Hence, if this smartcard system is used for identification for more than one service of the enterprise, it would provide a suitable compromise between simplicity (a bit more cumbersome than using passwords) and security (two-factor authentication).

Therefore, the simplicity of the identification method is essential in order to guarantee ease of use, but also avoid security pitfalls that can make the authentication process subject to social engineering attacks.

5.3 Legal requirements

5.3.1 Standards and Regulations

Legal requirements for identification in business processes stem from the fact that many standards are being defined and enforced by concerned institutions. These regulations and standards defined in the scope of strong identification and authentication techniques cover a wide range of fields.

For example, in the healthcare industry, privacy of patient data is essential, which incites standardization bodies to define "Acts" or standards to be abided by healthcare institutions in order to implement strict control on data access based on strong identification and authentication schemes. Financial institutions also have their own regulations to comply with, especially with the use of Internet banking, which requires strong authentication schemes. Authentication and identification in federal government agencies are also subject to standards defined by public or governmental institutions.

This kind of standards and regulations add a set of requirements on the choice of the authentication system to be considered for a business process. In the following, we list few relevant standards:

Standard	**Field**	**Title**
ISO/IEC 11131	Banking	*Financial Institution Sign-On Authentication*
ISO/IEC 9798	General	*Entity Authentication*
ISO/IEC/JTC1/SC17	General	WG4: *Smart Cards: ISO/IEC 7816 Personal verification through biometrics*
ANSI/NIST X9.84:	Banking	*Biometrics Management and Security for the Financial Services Industry*
CEN EN 1387:	Healthcare	*Machine readable cards- Health care applications – Cards: general Characteristics*
CR 13643	Healthcare	*Machine-readable cards – Healthcare applications – Logical data structures and concepts for different card technologies for use by patients in health applications*

5.3.2 B2B or B2C agreements

Customers or business partners are nowadays demanding legal agreements with regard to the confidentiality of certain data typically exchanged within the process, as well as agreements that can enforce strict rules with regards to privacy of information handed over to a business entity. These agreements (e.g. Service Level Agreements, section 5.7.2) entail deployment of sophisticated techniques by enterprises in order to guarantee as much as possible abidance by the agreement rules. The reason is that a failure to comply with legal rules can lead to a breach in the confidentiality or privacy of sensitive information, which eventually leads to legal problems with partners or. These problems entail costs for courts, and cause huge harm to the reputation of the enterprise.

6 Properties of Contemporary Identification Schemes

In the following sections, we give a closer look at the properties of identification schemes as currently considered in enterprises and business processes. We explain how the requirements discussed in chapter 4 are generally addressed with contemporary identification schemes.

6.1 Robustness

6.1.1 Security

Robustness of identification schemes is mostly defined by the strength of the authentication capability they can provide. Multiple solutions are usually deployed to meet different kind of requirements, each with advantages and disadvantages. Security management solutions are usually used to mix different kinds of authentication schemes in a single IT infrastructure. Basically, authentication schemes can be categorized according to the following properties:

Information known only by the user:

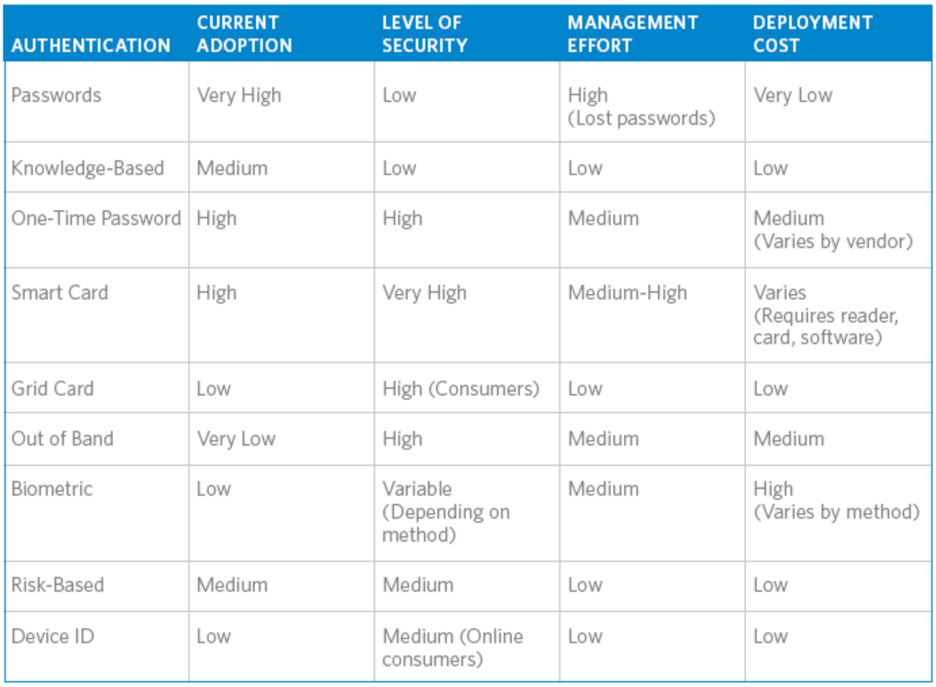
- **Passwords**: as explained in 3.1.1, a password or PIN is one of the most widely used form of authentication, but is never considered as a strong means for authentication no matter how long or complex it is.
- **Challenge-response:** this kind of schemes require the authenticating user to provide an answer to a certain question (challenge) which supposedly should only be know by him. This is also a form of authentication that is not considered as a secure one since the answer can sometimes be easily guessed.
- **One-time-passwords:** mentioned in 3.1.1.1, these id-tokens are generally considered to be secure, but they have disadvantages such as the need for users to carry the token with him which is prone to be lost or damaged.
- **Digital certificates:** represent an authentication mean that is widely adopted due to the high security it provides, coupled with a scalability aspect (PKI), as well as the ability to embed a certificate, e.g., in a smartcard, or any computing device or USB token.

Above are some of the authentication techniques that fall in this category. In terms of robustness as well as practicality, digital certificates are considered the best authentication means in this category.

Information which is part of the user:

- **Biometrics:** including fingerprint readers, iris scans, this type of authentication technique is considered to be very secure due to the fact that the identification information is very hard to fake or leak, so the authentication system is unlikely to be spoofed by an attacker. However, when using biometrics, identification cannot realise anonymity since the identification information provided link directly to the identity of the user and not to his role (for example). It is therefore useful in the case where anonymous authentication in meaningless, such as with e-passport[10].

In [CA, 2007], a comparison is given between the different levels of security corresponding to each authentication technique.



AUTHENTICATION	CURRENT ADOPTION	LEVEL OF SECURITY	MANAGEMENT EFFORT	DEPLOYMENT COST
Passwords	Very High	Low	High (Lost passwords)	Very Low
Knowledge-Based	Medium	Low	Low	Low
One-Time Password	High	High	Medium	Medium (Varies by vendor)
Smart Card	High	Very High	Medium-High	Varies (Requires reader, card, software)
Grid Card	Low	High (Consumers)	Low	Low
Out of Band	Very Low	High	Medium	Medium
Biometric	Low	Variable (Depending on method)	Medium	High (Varies by method)
Risk-Based	Medium	Medium	Low	Low
Device ID	Low	Medium (Online consumers)	Low	Low

Table 1: Comparison between different identification techniques [CA, 2007]

As can be seen in the results shown in Table1, the use of simple passwords for authentication has the least security level, whereas the use of smartcards has the highest security level. Moreover, passwords seem to require the highest level of management effort, if lost passwords are taken into consideration. While this looks to be a somehow expected result, it is important to mention that combinations of these techniques are also possible for enhancing authentication and identification processes, and can lead to even higher security levels. For example, using biometrics in order to enhance smartcard authentication is possible and has been discussed in [Bechelli et al. 2002] and [Bistarelli et al. 2003].

In his master thesis, Sollie [Sollie, 2005] conducted a subjective evaluation of the different combinations of authentication methods (Username and password; Smart card with PIN; Fingerprint; Password and smart card with PIN; Username, password and fingerprint; Fingerprint and smart card with PIN). This evaluation and subsequent comparison of the systems were made according to certain pre-defined metrics. The security metrics (SM) were as follows:

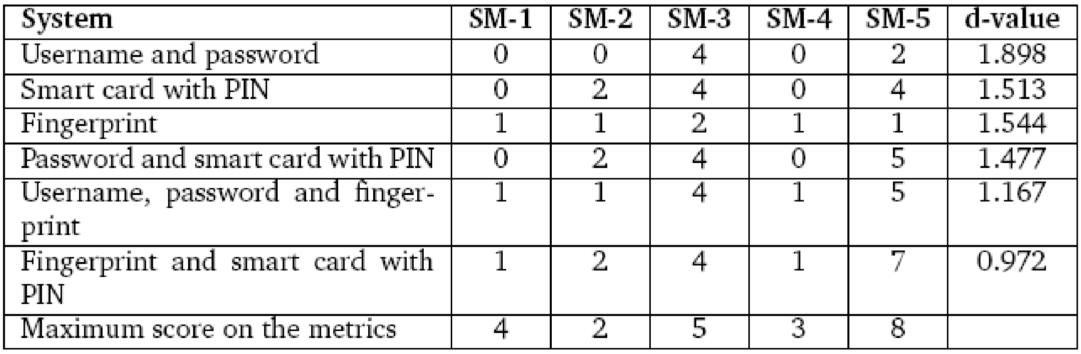
- **SM-1: Liveness testing:** indicates the usage of a human physiological and/or behavioural feature, such as biometrics, for unique identification.

[10] Also known as “biometric passport”, is a combined paper and electronic passport that uses biometrics to verify the identity of the holder.

- **SM-2: Tamper resistance:** includes protection against side channel attacks such as probing attacks, fault induction attacks, timing attacks, power analysis attacks, and electromagnetic analysis attacks.
- **SM-3: Secure communication:** indicates the level of protection (encryption, integrity) of the data communicated between modules of the authentication system over an insecure line.
- **SM-4: Traditional authentication:** indicates the use of a piece of information (PIN, password, etc…) or a token (Key-fob, smartcard, etc…) which only the user knows or has.
- **SM-5: Multiple authentication:** indicates the use of multi-factor authentication based on both piece of information and id-token.

The measurements of the metrics for each system were done according to an evaluation of the corresponding aspect of the system performed by the author based on personal research.

The results are shown below, a lower *d*-value indicating a higher overall security level.



System	SM-1	SM-2	SM-3	SM-4	SM-5	d-value
Username and password	0	0	4	0	2	1.898
Smart card with PIN	0	2	4	0	4	1.513
Fingerprint	1	1	2	1	1	1.544
Password and smart card with PIN	0	2	4	0	5	1.477
Username, password and fingerprint	1	1	4	1	5	1.167
Fingerprint and smart card with PIN	1	2	4	1	7	0.972
Maximum score on the metrics	4	2	5	3	8	

Table 2: Security of authentication schemes based on security metrics [Sollie, 2005]

The results suggest that "Fingerprint and smartcard with PIN" scheme is the most secure, and the simple "Username/Password" scheme is the least secure among the considered schemes, and according to the metrics above.

One observation to be made here is that the multi-factor authentication aspect is crucial for the security of the authentication system. Especially when different kinds of these factors are needed, namely biometric information, knowledge of a piece of information, and possession of a token, the system scored the highest level of security.

Nevertheless, it is important to note that the evaluation of the schemes with respect to the defined metrics was based on underlying technical assumptions that might be changed over the time by developing technologies. For example, the Fingerprint scheme has been subject to development over the past few years, where a scan of four full fingers is done, instead of the top of the thumb. Therefore, the authentication methods depend on the overall system whose improvements might lead to a change in the evaluation with respect to a certain metric.

6.1.2 Reliability

Reliability of the identification scheme can be looked upon as measurement of its robustness. In addition to the level of security an identification system should provide, it should be reliable, in the sense that no errors by the system itself (such as authorizing an unauthorized user, or even denying an authorized user) can occur. In [Sollie, 2005], this factor is defined as a metric for usability of the identification system, and is defined by the rate of errors by an authentication system should be very low, if not zero. Especially when high-value businesses are in question, it is necessary to avoid any failures by the authentication system in order to ensure effectiveness of the business. The determination of the error rate can only be done if the system is implemented and tried by users. This is often very time consuming and costly.

It can be concluded that security and reliability, which we see as the metrics for robustness of a certain identification systems, are subject to trade-offs. However, we can conclude that while biometrics seems to be the most secure, their combination with smartcard technology can achieve a higher security level. Therefore, enterprises which are still adopting the password-based identification schemes should start moving out of this arena which has become acknowledged to be the least secure. A shift towards smartcard infrastructures might be suitable. On the other hand, since identification techniques seem to share an almost equivalent level of reliability, which is considerably high, this reliability level should be maintained in future developments in existing technologies.

6.2 Scalability and flexibility

6.2.1 Hierarchy and decentralization

The deployment of an identification scheme based on digital certificates allows establishment of a hierarchical trust model that is scalable and flexible.

The hierarchical trust model requires all creation of certificates and their verification to be coordinated by the certificate authority. It is required to trust in the CA to function correctly. This is the reason for the hard security requirements that are expected from CAs, who issue electronic signature certificates that are legally binding in the European Union according to its signature legislation.

The CA issues signed certificates, thus establishing a trust relationship with the owner of the certificate. Usually the hierarchical approach is used for centralized systems and reflects an organizational hierarchy. All members that seek to verify trust in a certificate holder verify whether they get presented a valid certificate from their CA. Trust can be propagated in this model by introducing sub-CAs who are allowed to create certificates for entities (e.g., a department could issue its own certificates). The sub-CA will have a signed certificate from the central CA, thus establishing a trust relationship to the central CA. A certificate from the sub-CA can be linked to the sub-CA and, by using the sub-CA's certificate, indirectly to the CA.

One open problem remains: How does the verifier know that there exists a sub-CA, and how can he verify the link to the central CA? For this purpose, CAs have a directory of certificates that is used to look up certificates. If a verifier gets a certificate with an unknown CA signature, he can look up in the directory and will find whether this is a sub-CA known to his central CA. If so, he can also look up the certificate that establishes the trust relationship between the sub-CA and the CA.

One last important topic is certificate revocation. To cancel a trust relationship, i.e., to indicate that a sub-CA certificate is not valid and not trusted anymore, it is marked as "revoked" in the directory.

6.2.2 Interoperability

Interoperability is also a basic property of a scalable and flexible identity management system. It gives companies and customers the ability to resolve trust requirements when carrying out business processes across organizations (or even within a single organization) with distinct identity management systems. However, interoperability is often subject to constraints by enterprises with specific commercial interests. In fact, interoperability problems might arise even if enterprises adopt digital certificates for identification since the representation standards for technologies underlying the scheme might differ [IDWG, 2006]. Therefore, common and consistent representation of certificates would allow a person from one organization to participate in a process under a different identity management system.

However, the realization of interoperability is still far from reach in many fields and organizations. For example, health information exchange in the American health care system falls short from achieving this goal. Even if interoperability on a data sharing level is available, building trust in the identity of authenticating users is still not always possible. [Holt Anderson et al., 2007], an expert panel report on “Interoperable Digital Identity Management in the Electronic Exchange of Health Information” in America, suggests that “without a common means to assure identity and thereby control authentication and access, the ability to exchange data will be severely limited”. This implies that interoperability between identification techniques of different health care institutions has become a necessity.

Research in the European community around the same problem is underway, with a focus on an identification system that allows interoperable identification of patients to facilitate the creation of a European electronic health records database [Quantin et al., 2007].

Interoperable identification systems are also a concern for e-government in the EU, especially that the EU Commission has set the interoperable authentication and authorization systems for e-government access as a priority target for 2010 [Pimenidis, 2007].

Therefore, different industries face the challenge of interoperable identification technologies. Pilot projects and schemes are aiming at this target. For example, interoperability of identity and identification systems has been discussed in FIDIS workpackage 4, such as in D4.2 [Backhouse et al., 2005] and D4.9 [Backhouse et al., 2007].

6.2.3 Trustworthiness across domains

Establishing trust in identities across domains is crucial in many enterprise scenarios where business processes need to be carried out by many partner organizations. The reason is that interoperability is not enough for enterprises to trust each others in terms of identification techniques. In fact, even if interoperability between identification credentials of different organization is achieved, the trust in the identification mechanisms at the peer organization requires further investigation.

Trustworthiness in identification across domains can greatly enhance business processes, and is therefore addressed in different identity management solutions. For example, in [D3.9, 9], we gave a scenario where identity credentials from a certain service provider are used for accessing a service in the domain of another service provider.

An architecture proposed in [Fichtinger et al., 2007] shows how Trusted Computing functionalities and protocols can be used to establish trust in identification credentials across identifier domains. It integrates the role of "Privacy-CA"[11], i.e., a certification authority defined by the Trusted Computing Group (TCG) that can certify pseudonymous machine credentials. This architecture defines a set of protocols that allow a service provider residing in identifier domain B to be able to accept identity credentials issued by identity providers in identifier domain A, and that is based on the trust in the Privacy-CA, and the integration of TPM[12] hardware and functionalities. This scheme claims to achieve interoperability and trustworthiness for the identification credentials.

Other initiatives also provide PKI schemes that can be used for trustworthy identification of users across domains, such as the work in [Patel, 2004]. This work is done in the scope of the Keystone project with the aim to develop a scalable and robust PKI architecture for cross-domain operations. The reference model is based on the notion of Trusted Third Parties (TTP), which have interfaces to both single users and users within organizations in order to endorse their certificates. TTPs have interfaces among themselves which allows validation of certificates, e.g., across organizations.

[11] The Privacy CA is a role defined by the TCG. It is responsible for management of pseudonyms which are associated to identifying machine credentials. The integration of this role in the Trusted Computing protocols allows hiding the identity of the machine (and consequently the end-user), which helps preserving privacy.

[12] A TPM (Trusted Platform Module) is a tamper-resistant security chip specified by the TCG which implements smartcard-like functionality, such as registers and cryptographic functions, and is typically built in computing devices to securely and persistently store hash measurements of the software stack for later verification.

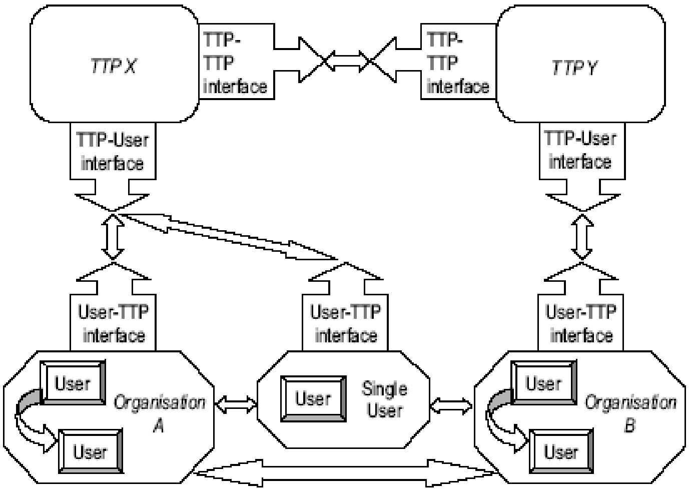


Fig.2: PKI Reference model for cross-domain use of certificates [Patel, 2004]

Other cross-domain identification schemes are based on the “Pretty Good Privacy” (PGP) scheme, which follows the OpenPGP standard [RFC2440] . The PGP scheme does not require any third party CA. It allows the distribution of public keys that are trusted by peer users. This trust is established if the receiver of a message can contact the sender to verify whether the fingerprint of the signature is valid. However, this procedure is not considered as practical in a larger community, since senders cannot be easily accessible for receivers who need to verify signature key fingerprints. Therefore, the PGP scheme allows users to sign each other’s public keys.

All these approaches allow establishment of trust in identification credentials across domains or organizations.

6.2.4 Efficient identity management

The management of identification information is crucial for any identification scheme. Therefore, efficient identity management is a priority when deploying an identification scheme for a certain business.

Without corporate identity management systems, IT personnel must administer users and their access rights on each IT system in the network, often by manual administration. Users get accounts and passwords for each IT system they need to use. Each IT system has its own audit or monitoring function to track changes to users and their access rights on that system. Such a setting has a number of shortcomings:

- Decentralised user management and provisioning means that identity and access data is duplicated across IT systems and usually becomes inconsistent over time, making it difficult to find correct and up-to-date information, and to revoke users’ rights.
- Many identification techniques might be suitable for one enterprise but not another. For example, if password-based authentication is considered for authorization to different applications, one password per IT application means that users must remember many

different sets of login credentials, or they use the same credential for each application which in turn reduces security. Password proliferation leads to more help desk calls, lost productivity as users wait for password resets and increased IT administration costs. Therefore, it might be suitable to employ, e.g., federated identity management in this case (see 5.6.1).

- Auditing and monitoring requires identification of a collaborator to a business process in order to identify who has done what on the system. Therefore, it is necessary to determine the total access rights of a certain user across the enterprise, which requires an efficient and centralized identity management system. However, this identification is conflicting with the anonymity requirement that many employees might raise. Therefore, the trade-off between anonymity and auditing should be handled by the identity management system according to the policy of the enterprise, or the business process.

Overcoming these limitations requires an enterprise-wide, cross-platform, centralised and automated user management, provisioning and access management system, which controls access to IT resources based on business roles, policies and processes. The system must provide ways to align itself with business processes and off-load routine administrative functions and decisions from IT staff to users and their managers so that decisions about what users really need are made by the people who know it best.

Identity and access management (IAM) technology has greatly evolved in order to efficiently address the business and users requirements, and supporting standards are being defined. *[Ref. to standard or standardization effort]*

6.2.4.1 Federated identity management systems

Federated identity management (FIM) systems represent one way to administer and manage the identification information of users within a business process.

While interoperability in identity management is essential to allow different enterprises to carry a business process across their boundaries by making the identification schemes homogenous among the partner enterprise, FIM leverages this capability and extends it to allow identification information supplied at different enterprises to be federated. This in turn allows services such as single-sign-on to be implemented.

FIM systems usually allow single-sign-on in order to make the services provided within different context accessible to the collaborators in an easier way. Federation of identity is performed based on a federation framework that includes an infrastructure for establishing communication between participating organizations. The main aim of identity federation is to enable users of one “security domain” to access services of another domain. For that purpose, protocols are employed to broker information on identities, identity attributes and authentication credentials as well as sharing federation metadata including security token exchange between Requestors, Identity Providers (IP) and Security Token Services (STC) [Federated, 2008].

Although many federation standards exist, each with different capabilities, they all share common security requirements. We list here Shibboleth, Security Assertion Markup Language (SAML, by OASIS), Liberty ID-FF (by Liberty Alliance) and WS-* efforts for web services (mainly WS-Security, WS-Trust and WS-Federation by IBM, Microsoft, and partners) [IBM, 2005].

There are many aspects in those standardized protocols that can directly or indirectly affect the security of the federation framework. Basically, the authentication and authorization in the federation framework depends on a general security model.

Security model

The security model of a federation framework relies on the notion of security tokens, which represent a collection of claims that a user have with regard to authorization to certain services. Security tokens constitute one of the core means for securing the process of authorization of a certain user to a specific service. Typically, security tokens that are initially provided by one Security Token Service (STS) that corresponds to one IP in a domain are used to access web services in another domain, for example, by:

- Getting certified by STS corresponding to the second domain, or
- obtaining new local security tokens that are valid for authorization to the web service from STS in the second domain, or
- getting validated by the resource provider's STS.

The usage of security tokens depends on the established trust model. However, it is necessary to exchange these tokens between participating parties by means of adequate communication protocols, which entail the requirement of secure communication.

Trust model

Federated trust can be based on different trust models. A trust model typically depends on the different parties and entities contributing to the federation process, namely the STS, the IP, the requestor, and the resource itself. The following figure illustrates the different entities/parties, and the established trust between them.

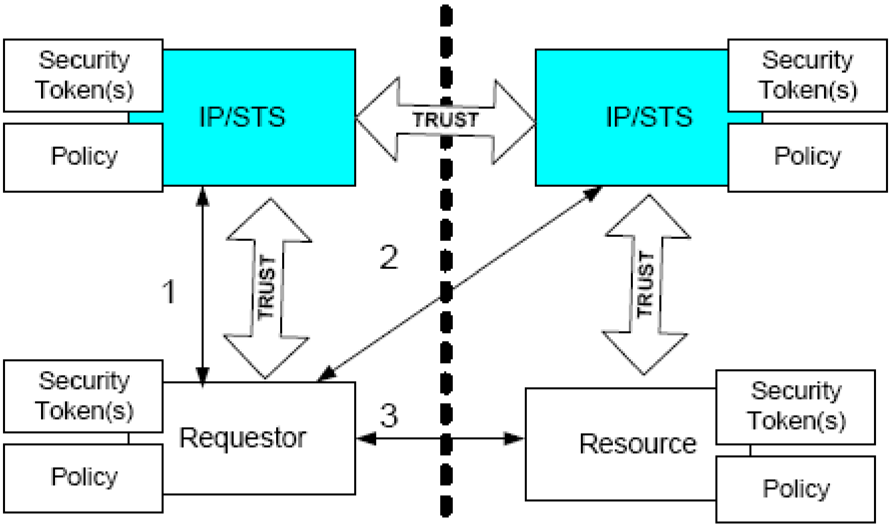


Fig.3: Federation and trust model [WS-Federation, 2006]

The requestor trusts the IP/STS of its own realm, and same does the resource with its IP/STS in the second realm. The IP/STS in the different realms trust each other.

Based on this model, different trust topologies can be derived. Basically, they differ in the way security tokens are issued, validated and exchanged by the different entities involved in the process. For example, one approach (shown in the figure) requires the requestor to obtain a token from the IP/STS in its own realm, provide it to the IP/STS in the second realm, which then check its validity and exchange it with a token that is valid in this second realm. Using this token, the requestor would be able to directly access the resource. Another approach would require the requestor to obtain a token from its IP/STS, supply it to the resource, which then validates the token at its own IP/STS before granting access to the requestor.

Security of communication

The requirement of secure communication between participating parties is important, especially across different domains. The security of communication protocols is crucial to the security and reliability of the overall FIM system since any malicious or involuntary breach of those protocols could have several consequences such as the user obtaining access to a certain service to which she is not authorized, or a user denied access to a service which she is supposedly authorized to access.

Therefore, message exchanged between services should be integrity protected by including the body of the message as well as the headers in the signature. Moreover, encrypted communication is needed (e.g., using transport security protocols) [WS-Federation, 2006].

Moreover, certain parameters used in the protocols need to undergo a strict verification due to their sensitive nature. For example, in an HTTP protocol used by a Web Requestor, the *wreply* parameter, including the URL to which responses are directed, can be spoofed.

Attribute service information is usually privacy critical, and should therefore be handled with care: Pseudonym service information can include passwords and similar secret information. Therefore, both require encryption during communication.

Security tokens must either have an embedded signature for integrity protection or be included in message supporting integrity check mechanisms [WS-Federation, 2006].

Generally speaking, the scalability requirement is currently addressed by deploying identification schemes supported by hierarchical trust models or decentralized trust models, such as in PKI schemes based on digital certificates. Interoperability seems to be a stressing factor, although enterprises and organizations in many fields still lack this property in their identification schemes. These institutions would rather be on the safe side when choosing an identification scheme by complying with common and widely deployed standards. Trustworthiness across domains is also still in its early stages, since enabling technologies such as Trusted Computing are not widely deployed in enterprises. Nevertheless, scalable PKIs are being used for this purpose, although they might not fulfil the exact security requirements. Efficient identity management is also becoming more and more considered by enterprises, especially with deployment of federated identity management schemes.

6.3 Anonymity

As mentioned earlier, anonymity might be of interest to many employees or customers when authentication to a certain service is needed.

Few authorization schemes emphasize on preserving the privacy of the service user. As explained in [D3.9, 8.6], Trusted Computing generally provides a means for authorizing a certain device to access a certain service based on TPM platform certificates that can be used to verify the trustworthiness of the device. Privacy-CAs, as well as the Direct Anonymous Attestation (DAA) protocol allows to provide a verification of trustworthiness without disclosure of any identifying information (only to Privacy-CA in case no DAA is used).

However, the problem persists if a user wants to get authenticated based on personal rights (and not device trustworthiness) without revealing his identity. This seems to be a paradoxical notion. However, it has been addressed in the literature, e.g. in [Kilian et al. 1998, Schechter et al., 1999, Boneh et al., 1999], naming it *anonymous authentication.* In [Lindell, 2007], an anonymous authentication protocol is defined as one that allows:

1. Secure authentication: no unauthorized user should be able to fool the server into granting him access (except with negligible probability).
2. Anonymity: the server should not know which user he is interacting with.

The work in [Lindell, 2007] gives an overview of a few techniques that are used to achieve anonymous authentication over Internet connections. They can be called “Anonymous routing mechanisms” (“Mix nets”, “Onion routing”, “Dining cryptographers” and “Crowds”).

It can be said that anonymity is not widely addressed in current identification systems, though research in the area if anonymous authentication is quite advanced and many schemes have been specified. Deployment of these schemes is however not perceivable. Considering the anonymity requirements by employees stated in the previous chapter, business processes are increasingly facing this requirement, which means that enterprises and service providers should start considering state of the art technologies addressing this issue.

6.4 Simplicity and usability

Simplicity and usability are important aspects of identification credentials employed by users in a business process. In [Sollie, 2005], a number of usability metrics have been defined and assessed on different authentication mechanisms.

Sollie conducted an experimental evaluation of the security of identification and authentication systems. In the scope of the experiment, which had 61 participants with different levels of computer skills, an application was developed which allowed a user to chose a combination of authentication methods The experiment required from each participant to select an authentication method out of the list, and perform a registration to the system (enrolment) and an authentication using the developed test application (along with smartcards and fingerprint scanners). Then a questionnaire is given for the participant in order to collect information on perceived security and usability.

Rate of errors by users: many employees tend to forget their passwords which makes them dependent on system administrators for retrieving their passwords, or incites them to use very simple passwords which are easier to crack. It might also be the case that the requirements for a PIN or password by the system are too complicated for the user to choose a relatively simple password that he can memorize.

Time to learn: the time needed for users to get used to the authentication mechanisms is important. If the learning requires a lot of time and effort, user are likely to be reluctant to use the system.

Subjective satisfaction: this is in fact the most important aspect when usability needs to be assessed, since the usability and simplicity of the authentication system is measured from the user's perspective whose satisfaction is the main goal.

6.5 Standards and regulations

Standards defined by several kinds of institutions of different fields can be encountered.

While there exists a large number of standardization bodies which have more than one standard addressing the identification and authentication related issues, we list a few relevant standards:

- CEN/ISSS – EN 726: Identification Card Systems – Telecommunications Integrated circuit cards and terminals.
- CEN/ISSS – CR 13644: Machine-readable cards – Healthcare Applications

In addition, a CEN/ISSS Workshop was held for discussion around European Electronic Authentication, to cover a functional architecture and required Identification, Authentication and electronic Signature (IAS) characteristics for the purpose of a European Public Identity using smartcards, or other multi-application cards.

Another workshop by the CEN on "Cyber Identity: unique identification systems for organizations and parts thereof (CEN/ISSS WS/CyberID) was started on April 11th, 2008 and is expected to come up with a CWA standard by August 2009.

In [CA, 2007], the following three examples are given in the scope of US standards:

- The Health Insurance Portability and Accountability Act (HIPAA), which mandates strict controls over privacy of patient data. That, in turn, forces healthcare companies - and indeed any organization that holds potentially sensitive data on employee health – to ensure that only authorized people can access patient data.
- The Federal Financial Institutions Examination Council (FFIEC) guidelines on "Authentication in an Internet Banking Environment," which — like earlier Federal Deposit Insurance corporation (FDIC) guidelines — say that user ID and password alone should not be resumed to be a sufficient form of authentication for online banking.
- NIST Special Publication 800-63, which provides electronic authentication guidelines for federal government agencies; some levels require two-factor authentication.

6.6 Service level agreements

Identification of business collaborators across enterprises or even in business-to-customer scenario can not only rely on the trustworthiness of the identification system. It can also require a sort of legal agreement regarding the reliability and security of the identification scheme. If the identification scheme fails in achieving its claimed goals, the responsible legal entities are held accountable according to the terms of the agreement. This kind of agreements falls in the category of so-called "Service Level Agreements" (SLA).

In fact, a general trend in the market is its evolution towards services. Within this context and given the great competition in the business domains with a wide range of services provided and a great number of Service Providers (SPs) offering them, customers seek for services of specific quality at an affordable price. The International Telecommunication Union (ITUT) defines Quality of Service as "the collective effect of service performances, which determine the degree of satisfaction of a user of the service. The quality of service is characterized by the combined aspects of service support performance, service operability performance, service integrity, and other factors specific to each service" [ITUT, 2009].

In order to enable trust between the different parties, both in Business to Business (B2B) and Business to Customer (B2C) interactions, a contract – the Service Level Agreement – is signed between the entities involved prior to service provision. According to the TeleManagement Forum, an SLA is defined as "a formal negotiated agreement between two parties, sometimes called a service level guarantee. It is a contract (or part of one) that exists between the service provider and the customer, designed to create a common understanding about services, priorities, responsibilities, etc." [TeleManagement Forum, 2009].

Hence, the SLA contains :

- the legal description of the parties involved,
- provided and requested quality of service (QoS), including availability requirements, service performance in a normal state, acceptable deviations,
- expected usage of the resources,
- the SLA lifetime,
- reporting on the quality of the services delivered to the customer,
- problem response time and resolution, which specifies the time after which a reported problem will be solved,
- compensations and penalties for not meeting agreed upon service quality levels,
- customer and SP responsibilities,
- service pricing and discounting policies
- SLA exclusions, including the conditions under which the SLA will not be valid, such as earthquake, general power failure, flood and so on.

In other words, the SLA facilitates the increase of the customers' confidence in the robustness, security and performance of the provided services and, in the meanwhile, the operation of these services on the SPs' behalf in an efficient and ultimately profitable manner. A well-designed and well-chosen SLA forms the basis for the establishment of the SP's credibility acting as a means for customer attraction in the competitive business environment through the establishment of a trusted customer-provider business relationship. In fact, according to Mitchell and Mckee (2006), the SLA has various roles in the business processes:

1. Management of the customer expectations: The SLA includes a clear and unambiguous description of the service through which problems may be avoided. The customer has a clear view of costs, the availability of reports, and the scale of any associated penalties.
2. Support for product differentiation and assistance in consumer choice: particularly important in a dynamic market place.
3. New customers attraction and existing customers retention
4. SP Advertising: an SLA is indicative of a supplier's confidence in their ability to deliver services effectively, and may be used as part of the discovery and selection method together as a mechanism for establishing trust between providers and consumers.
5. Assistance in customers' evaluation of their contracted service.
6. Reduced risk when provided service is composed by services offered by various SPs. The SLA may aggregate risk for the consumer, service providers may incorporate the services of other providers in their product offerings. The principle supplier will in that case have subordinate SLAs with the subcontractors, and will have to make appropriate assumptions regarding the degree of risk they are happy to assume in guaranteeing the composite service.

The SLA lifecyle

The struggle of the SPs to increase their market share and profits, the intensified request of services of improved quality by the customers and the cooperation of multiple SPs for the final service provision lead to a constantly increasing complexity of the SLAs. Hence, in order to maintain the value of the SLAs as contractual agreements between SPs and customers for the agreed-upon service provision, their efficient management is strongly required. Although various versions related to the steps of the SLA establishment and execution process exist, the complete lifecycle of an SLA includes six distinct phases [TeleManagement Forum, 2005]:

- Development of service and SLA templates
- Discovery and negotiation of an SLA
- Service provisioning and deployment
- Execution of the service
- Assessment and corrective actions during execution (parallel phase to execution of the service)
- Termination and decommission of the service

Hence, initially customer needs and service capabilities are identified based on which the SLA templates are formed. Through these templates the provider's service offering is advertised to the customer. At this point, a service broker may act as a service marketplace, enabling consumers to find and use providers. The SLA initiator either selects a suitable SP and starts the negotiation process with the latter or negotiates with multiple potential SPs in order to choose the best service according to their needs (performance, performance vs cost, availability and so on). After the successful negotiation, the service is available to the customer for use under the terms of the agreed upon SLA. In the meanwhile, the SLA monitoring process takes place during which the metrics related to the terms of the SLA are monitored and evaluated based on the Quality of Service parameters agreed between the two sides. The SLA monitoring and evaluation processes are responsible for guarding the execution of the provided services by verifying whether the latter is in line with the SLA.

Generally, both the identification standards defined by official institutions, or legal agreements in the form of SLAs are becoming widely considered by enterprises for this business processes. However, an enterprise might have to choose between complying to a certain standard in the context of identification, or having its proprietary identification scheme and adhering to an agreement with the peer business partner or customer. This is a choice that needs to be wisely done by the enterprise considering many technical, legal and management overhead factors.

7 Conclusion

In this deliverable, an overview of the widely used identification and authentication techniques is given. These techniques are typically deployed in enterprises and organizations in order to provide secure and reliable identification of collaborators to a certain business process. Each of these techniques has its advantages and disadvantages, and several metrics should be considered by an enterprise in order to assess the best identification scheme to fit its needs these of its customer or peer enterprise.

The identification techniques addressed in this deliverable are knowledge-based authentication (such as password-based authentication, or challenge-response authentication), possesion-based authentication, biometrical authentication schemes and digital certificates. For each of these schemes, a description is given, along with an overview of its security properties.

The general identification requirements are then listed, categorized according to business requirements, employees' and customers' requirements as well as legal requirements.

An enterprise managing a business process needs a suitable identification scheme for the collaborators to the process. The robustness and security of the identification scheme is essential to an enterprise since a failure in the identification system might cause considerable damage to the business value as is the case with an unauthorized access to an online banking account. The reputation of the enterprise can also be affected if such breaches occur, which requires it to consider a suitable level of security when deploying a certain identification system. On the other hand, the scalability of the identification system is also important to the enterprise since it defines the boundaries of the identification system in terms of coverage of geographical as well as function areas. Flexibility is also relevant when a business process requires a frequent alteration of identification information of collaborators, or revoking collaborators credentials.

Employees and customers are interested in high level of security in the identification system within a business environment, but might also have specific requirements such as anonymity and simplicity. Anonymity and authentication of a certain collaborator might look contradictory requirements, but anonymous authentication has been addressed in the literature so as to allow authentication of granted rights without revealing the identity of the user. This requirement is relevant for collaborators who do not want their actions to be monitored. Moreover, collaborators are generally interested in the simplicity of the authentication system since complexity can either add a burden, or lead them to breaching social engineering guidelines.

Requirements imposed on identification systems also stem from the growing amount of standards and regulations defined by legal entities. Governmental agencies might have strict legal requirements to be considered when an enterprise deploys a certain identification system, especially for achieving a certain security level in high-value public services. On the other hand, enterprises might have to abide by legal agreements made with business partners and customers, which dictates the kind of identification system to be used.

In chapter 5, we discussed the properties of contemporary identification techniques. The scalability requirement is currently addressed by deploying identification schemes supported by hierarchical trust models or decentralized trust models. PKI schemes support the use of digital certificates and allow a certain level of scalability and flexibility of the identification system. Interoperability of identification schemes is also considered in enterprises by complying to common standards and technologies with peer enterprises in the field. This enhances the scalability and flexibility of identification.

Trustworthiness across domains is also a relevant property addressed in many business scenarios. Typically, scalable PKIs are designed for this purpose, and Trusted Computing technologies help achieving the needed trust in the peer identification scheme.

Anonymity is not widely addressed in current identification systems, though research in the area if anonymous authentication is quite advanced and many schemes have been specified. Deployment of these schemes is however not perceivable.

Security and reliability, which we see as the metrics for robustness of a certain identification systems, are subject to trade-offs. Many studies have assessed different identification techniques in terms of the level of security they can achieve. Biometrics seems to be the most secure, but is generally coupled with smartcard technology – which also has a high-security level – for practical business scenarios. It has generally become widely acknowledged that passwords-based authentication can be a weak identification technique in many high-value business processes. Reliability of an identification system is usually measured by the rate of errors the system suffers from after deployment. Experiments have shown that the identification techniques discussed in this deliverable all share an almost equivalent level of reliability, which is considerably high.

Efficiency of identity management, a crucial property for identification schemes, depends on different factors, such as the extent of centralization of the trust model, the rate of revoking of identity credentials during the business process, the complexity of the authentication policy required by the enterprise or business process, and the relevance of anonymous authentication to collaborators. Federated Identity Management, with single-sign-on support, might be a suitable identity management concept that coherently addresses most of these requirements.

Legal grounds currently considered in governing the choice of identification schemes and systems come in the form of either standards defined by official institutions in the corresponding fields, or legal agreements, e.g., service level agreements made between partner businesses or between an enterprise and its customers.

8 Bibliography

[D3.9] Ammar Alkassar and Rani Husseiki (Eds.). FIDIS deliverable D3.9 “Study on the Impact of Trusted Computing on Identity and Identity Management”. FIDIS NoE Consortium – EC Contract No. 507512. 6th Framework Application of European Commission. 2007.

[D3.2] Mark Gasson, Martin Meints, Kevin Warwick (Eds.) FIDIS deliverable D3.2 “A study on PKI and biometrics”. FIDIS NoE Consortium – EC Contract No. 507512. 6th Framework Application of European Commission. 2005.

[Andersson et al., 2005] F. Andersson, S. Hagström. Dynamic identities for flexible access control. Master's Thesis. *School of Engineering Blekinge Institute of Technology*, Sweden, 2005.

[IDWG, 2006] IDWG–Technologies. Technologies for Identity Infrastructures. *Twist*, 2006.

[Holt Anderson et al., 2007] Holt Anderson et al.,"Interoperable Digital Identity Management in the Electronic Exchange of Health Information." An Expert Panel Report, 2007.

[Patel, 2004] Ahmed Patel. "Creating a Cross-Domain Public Key Infrastructure: The Keystone Project". *Electronic Signature & Digital Identity*, 2004.

[Lindell, 2007] A. Lindell. “Anonymous Authentication”, *Black Hat USA*, 2007.

[CA, 2007] CA. "Managing Strong Authentication: A Guide to Creating an Effective Management System". Technology Brief: Identity and Access Managmement, 2007

[Mitchell and Mckee, 2006] Mitchell, B., Mckee, P. SLAs: A Key Commercial Tool, Innovation and the Knowledge Economy: Issues, Applications, Case Studies, Paul Cunningham and Miriam Cunningham (Eds), 2005 IOS Press Amsterdam, ISBN: 1-58603-563-0, 2006.

[ITUT, 2009] International Telecommunication Union (ITUT), http://www.itu.int/ITUT/, accessed on 22nd April, 2009.

[TeleManagement Forum, 2005] TeleManagement Forum, SLA Management Handbook - vol. 2 - Concepts and Principles, 2005.

[TeleManagement Forum, 2009] TeleManagement Forum, http://www.tmforum.org, accessed on 22nd April,2009.

[Arturo, 2004] Arturo Ribagorda-Garnacho, Electronic Signature at the Heart of Information Security Development: An Overview, Upgrade - the European Journal for Informatics Professionals, June, 2004.

[Sollie, 2005] Roar S. Sollie, Security and usability assessment of several authentication technologies, Masters Thesis, Gjøvik University College, 2005

[Fichtinger et al., 2007] Barbara Fichtinger, Eckehard Hermann, Nicolai Kuntze, Andreas Schmidt: Trusted Infrastructures for Identities, Koblenz 2007, http://www.virtualgoods.org/2007/10_VG07_Fichtinger_Hermann_Kuntze_Schmidt.pdf

[Kilian et al. 1998] J.Kilian and E.Petrank. Identity Escrow. In Advances in Cryptology CRYPTO '98

[Schechter et al., 1999] Stuart Schechter 1 , Todd Parnell, A.J. Hartemink Anonymous Authentication of Membership in Dynamic Groups. In 3rd Financial Cryptography, Springer-Verlag (1999)

[Boneh et al., 1999] D. Boneh and M. Franklin. Anonymous authentication with subset queries. In proceedings of the *6th ACM conference on Computer and Communications Security*, pp. 113--119, 1999

[Bechelli et al. 2002] L. Bechelli, S. Bistarelli, and A. Vaccarelli. Biometrics authentication with smartcard, 2002. http://citeseer.ist.psu.edu/bechelli02biometrics.html.

[Bistarelli et al. 2003] Stefano Bistarelli Giampaolo Bella and Fabio Martinelli. Biometrics to enchance smartcard security. http://www.sci.unich.it/\~bista/papers/ papers-download/mocviatocfinal.pdf, 2003.

[Federated, 2008] Federated Identity – Wikipedia (2008) http://en.wikipedia.org/wiki/Federated_identity

[IBM, 2005] Federated Identity Management and Web Services Security, IBM, 2005 http://www.redbooks.ibm.com/redbooks/pdfs/sg246394.pdf

[WS-Federation, 2006] Web Services Federation Language (WS-Federation) http://specs.xmlsoap.org/ws/2006/12/federation/ws-federation.pdf

[Noel, 2004] V. Noel. Security Using Digital Identification Methods for Use within "Federated, Secure Trust Networks for Distributed Healthcare IT Services". Bachelor Thesis, University of Virginia, 2004.

[Eckert, 2004] C. Eckert, IT-Sicherheit. *Oldenburg Verlag München*. Wien, 2004

[Lamport, 1981] Leslie Lamport. Password authentication with insecure communication. *CACM, 24(11):770-772*, November 1981

[Haller, 1994] N. Haller. The S/Key one-time-password system. In Dan Nesset (General Chair) and Robj Shirey (Program Chair), editors, *Symposiom on Network and Distributed Systems Security, San Diego,* California, February 1994.

[RFC2289] Internet Society. RFC2289. http://tools.ietf.org/html/rfc2289

[Effing et al., 1999] W. Effing, W. Rankl. Handbuch der Chipkarten. *Carl Hanser Verlag*, 1999.

[Cameron, 2005] Cameron, K., *Laws of Identity*, version of 5/12/2005. See at www.identityblog.com.

[RSA, 2009] RSA, RSA SecurID, http://www.rsa.com/node.aspx?id=1156, 2009

[Cohen, 2001] Cohen, B., Laurie, B., AES-hash, 2001, http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/aes-hash/aeshash.pdf

[Allan, 2007] Allan, A., "The Twilight of Passwords: A Timetable for Migrating to Stronger Authentication," Gartner, Inc., 2007.

[RFC2440] Callas, J. et al., "OpenPGP Message Format" (RFC2440), The Internet Society, 1998, http://www.ietf.org/rfc/rfc2440.txt

[Quantin et al., 2007] Quantin, C. Allaert, F.A. Fassa, M. Avillach, P. Fieschi, M. Cohen, O. Dijon Univ. Hospital, Dijon; Interoperability Issues regarding Patient Identification in Europe. Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE, 2007

[Pimenidis, 2007] Pimenidis, Elias and Savvas, Ioannis, "E-identification technologies for e-government interoperability in the EU", International Journal of Electronic Security and Digital Forensics, 2007

[Backhouse et al., 2005] Backhouse, J. and Vanfleteren, M. (ed.), FIDIS deliverable "D4.2: Set of requirements for interoperability of Identity Management Systems". FIDIS NoE Consortium – EC Contract No. 507512. 6th Framework Application of European Commission. 2005.

[Backhouse et al., 2007] Backhouse, J. and Dyer, B. (ed.), FIDIS deliverable "D4.9: An application of the management method to interoperability within e-Health". FIDIS NoE Consortium – EC Contract No. 507512. 6th Framework Application of European Commission. 2007.

[Zheng, 2003] Zheng, P. 2003. "Tradeoffs in certificate revocation schemes". *SIGCOMM Comput. Commun. Rev.* 33, 2 (Apr. 2003), 103-112.

[Boneh, 2001] Boneh, D., Ding X., Tsudik, G., and Wong, C. "A Method for Fast Revocation of Public Key Certificates and Security Capabilites". In The 10th USENIX Security Symposium, 2001

[Sandhu et al., 1996] Sandhu, R., Coyne, E., Feinstein, H., Youman, C., "Role-Based Access Control Models", IEEE Computer, 1996

[Messerges et al., 1999] Messerges, T. S., Dabbish, E. A., and Sloan, R. H. 1999. "Investigations of power analysis attacks on smartcards". In *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology*, 1999

[Kömmerling et al., 1999] Kömmerling, O. and Kuhn, M. G. 1999. "Design principles for tamper-resistant smartcard processors". In *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology*, 1999

[Surendran, 1999] Surendran, D., "Smart Card Technology and Security", http://people.cs.uchicago.edu/ ~dinoj/smartcard/security.html

[Damato, 2007] Damato, A., "Biometric system diagram", Biometrics, Wikipedia, http://en.wikipedia.org/wiki/File:Biometric_system_diagram.png, 2007

[Maurer and Wolf, 1999] Maurer, U., and Wolf, S., "The Diffie-Hellman Protocol" , Designs, Codes, and Cryptography, 1999