



“While the original motivation for introducing IT security measures has often been security enhancements, appropriate security solutions also offer substantial potential for cost savings and for accomplishing new opportunities, both for businesses and the public sector. Secure digital identification together with the management of identities play an essential role in this area and the deployment of various types of e-ID solutions is well underway.

This paper addresses key trends and current challenges in this area.”

Walter Fumy
Siemens AG, Healthcare Sector
Chairman ISO/IEC JTC 1/SC 27

Jörg Sauerbrey
Siemens AG, IT Solutions and Services

Key words: Interoperability, return on invest, compliance, data privacy, multi-factor authentication, identity and access management, standardisation.

1 INTRODUCTION

The global information society is strongly dependent on reliable and secure IT services, both in private life and in business. In this context, the ability to verify a person's identity plays a fundamental role. On the other hand, identity information is very sensitive and regularly regarded a privacy issue.

Protecting one's identity depends both on personal effort and on the practices, policies, and systems of the organisations to which one entrusts personal information. Individuals must exchange identity information and personal data almost daily with other individuals and with organisations. People constantly risk losing control of identity information and must rely on the entities that share the information to protect it.

In the area of e-ID solutions, many alternative technologies have been proposed, each presenting its own advantages. Nonetheless, physical access badges, biometric identification, one-time password tokens, corporate directories, identity management platforms, and the variety of password-enabled applications, are in many cases operating in isolation.

2 e-ID SOLUTIONS FOR THE ENTERPRISE

Managing identities in an enterprise is a challenge in today's business environment. Business relationships are growing more complex, blurring the line between internal and external business processes. They are also becoming more dynamic, requiring greater flexibility and responsiveness in the enterprise's business practices, policies and processes. Companies are under pressure to open up their IT infrastructure to an ever-increasing number of users, both inside and outside the company and to ensure the highest productivity and privacy for these users, all while controlling IT administrative costs and leveraging existing investments wherever possible.

Secure Digital Identification

In this context, the ability to verify a user's identity has become an essential foundation for trust in business relationships. Authentication solutions establish such trust by ensuring that a 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 identity management.

The two main use cases for e-ID solutions within an enterprise are physical and logical access.

- Enterprises need effective mechanisms for controlling access to networks, systems, and applications. e-ID solutions for securing logical access address off-site and on-site requirements and include controlling employee access to workstations, intranets, virtual private networks (VPNs), databases, and other logical information assets. A variety of options for authentication exist, including passwords, tokens, smart cards, digital certificates, and biometrics.
- Digital identification is also used as a means of restricting access to buildings and facilities. Card-based physical access technology has been deployed in a large number of enterprises.

In the past years, the market for enterprise e-ID solutions has been steadily evolving. Most notably, the following trends can be identified:

- Enterprises today tend to prefer deploying a converged authentication solution, whereby the digital identification is used for both logical and physical access.
- Single Sign-On (SSO) solutions have become aligned with strong authentication solutions. While SSO mainly addresses the problem of memorising passwords, it does not in itself address their inherent weaknesses. Strong authentication for SSO ensures that the first authentication prior to enabling SSO provides an appropriate level of security.
- Concerns about identity theft have become more prominent. This has consistently led to an increase in the use of multi-factor authentication, both in the consumer and the enterprise domain.

- Two-factor solutions (e.g., something you have and something you know) are ever more chosen for stronger authentication, in particular in the area of logical access. Also, the integration of digital certificates is emergent; these are additionally exploited for further security services, such as encipherment or digital signatures.
- One-time password (OTP) tokens have made two-factor authentication popular and still are a widely deployed strong authentication technology in the enterprise, particularly for VPN access. Today, there is a trend to consolidate credentials and to include OTP technology as an option into smart cards.

For many enterprises deploying e-ID solutions, the technology of smart cards as a secure and reliable means of electronic identification provides the favoured basis for authentication. Smart cards can securely store and process a variety of credentials that can be used to identify an individual, including static and dynamic passwords, private keys and digital certificates, and biometric templates.

Smart cards can be used to support multiple applications, enabling a consolidation of services on one token, which in turn promotes cost savings and efficiency. They also have clear advantages as element of a public key infrastructure (PKI) solution [1]. Moreover, smart cards can carry a photo and other information for visual identity verification, which makes them the preferred solution for converged logical and physical access.

Smart Card Standards

Smart card standards primarily specify physical properties, communication characteristics, and application interfaces.

- ISO 7816 [2] is the most important specification for smart cards. This multi-part standard defines the actual dimensions of the plastic card, connector layout, location of the chip, electrical specifications, and lower layer protocol formats.
- The dominant standard for the increasingly popular contactless smart cards is ISO/IEC 14443 [3]. This standard covers two types of contactless cards which allow for communications at distances up to 10cm.
- The most common way to access cryptographic smart card functions from an application is to make use of PKCS#11 [4], a cryptographic token interface standard developed by RSA laboratories. Alternatively, on Microsoft platforms the CSP API is being used.

HSPD-12 and FIPS 201

In 2004, the US Homeland Security Presidential Directive 12 (HSPD-12) was established which mandates all federal employees will have "a secure and reliable form of identification" and this credential to allow both "physical access to federally controlled facilities and logical access to federally controlled information systems."

Soon thereafter, the National Institute for Standards and Technology (NIST) issued FIPS 201 titled "Personal Identity Verification (PIV) of Federal Employees and Contractors" [5]. FIPS 201 and its associated Special Publications specify minimum requirements for PIV cards as well as for card management. The goals include to provide better access control, to reduce identity theft and ultimately establish a three-factor, biometric authentication system as the standard for the US government. The PIV card itself is essentially a dual interface - contact and contactless - smart card.

FIPS 201 consists of two parts which can be implemented sequentially:

- Part I describes the minimum requirements to meet the control and security objectives of HSPD-12, including personal identity proofing, registration, and credential issuance.
- Part II details the technical specifications required to support Part I as well as the interoperability aspects. It includes policies and minimal requirements for interoperable PIV credentials for both physical and logical access.

HSPD-12 requires federal government agencies to roll out secure smart-card ID credentials to all employees and contractors by October 2008. While NIST has delivered the necessary specifications quickly, agencies have had the unattractive task of replacing their existing physical and logical access infrastructures with the one required for PIV cards in a relatively short time frame. Experience shows that it is not the technology aspects, but the required integration and interoperability that takes time.

The impact of FIPS 201 is not restricted to the US government. The private sector is increasingly using similar technologies and controls, and enterprises that provide services to the government may find that a substantial part of their staff will need to be credentialed.

Identity and Access Management

In the conventional IT infrastructure used in most enterprises today, there is a one-to-one correspondence between a service or resource available to users and the IT application/system that provides that service. Consequently, user management, access management, password management and auditing are carried out on a per-IT system basis. IT personnel must administer users and their access rights on each IT system in the network, usually 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 de-provision users.
- 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.
- Decentralised auditing and monitoring makes it difficult to track changes to users and their access rights. There is no way to tell what a single user's total access rights are across the enterprise, which makes it difficult to audit for regulatory purposes.

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 best.

Identity and access management (IAM) technology has evolved to a well-defined market category and has reached the depth and breadth to offer an effective way to satisfy these requirements. Internal IT processes are optimised and standardised by means of self-service functions, delegated administration and request workflows. The creation of users in different systems and their assignment to roles and groups is controlled centrally and always carried out in the same way. Access decisions can be controlled and monitored centrally.

Together with the auditing and reporting services in an IAM solution, this creates the foundation for compliance, i.e. the clear and demonstrable observation of legal regulations, such as the Sarbanes-Oxley Act (SOX). An IAM solution can ensure that defined and stringent processes for managing identities and access permissions are implemented, and thus can help to guarantee that an enterprise always is able to answer the questions "Who is allowed to do what where?", "Who did what where?", and "Who has authorised it?".

Return on Investment

Decision makers are bound to measure their investments against financial criteria such as profits, costs and ROI. The business value of information security can be determined on the basis of risk reduction, as a decreasing cost of doing business and a return on investment via enhanced trust relationships and improved business opportunities [1]. In general, the cost to mitigate the damage from a successful attack is much higher than the cost to prevent an attack. Detailed studies have identified the potential financial returns that enterprise e-ID solutions can generate [6]. Areas for cost savings include:

- Substantial decrease in password-related help desk queries.
- General improvements to IT administration processes, in particular for conducting employee provisioning and for allocating roles and access privileges.
- Reductions in insurance costs by demonstrating a significantly reduced risk in terms of IT security breaches.
- Increased employee productivity by speeding up authentication processes and making them more reliable.
- Optional additional savings through the introduction of electronic workflows, typically enabled via PKI services.

On the other hand, in certain situations IT security solutions are not a question of financial returns, but an obligation due to regulatory requirements. This is because e-ID solutions play an essential role in assisting enterprises to achieve and sustain a compliance environment. Strong authentication based on smart cards or biometrics and digital signatures as well as identity and access management help to verify that the controls are in place and working.

3 e-ID SOLUTIONS FOR THE PUBLIC SECTOR

e-ID solutions are also being introduced in personal identification and entitlement schemes at national, regional, and international levels. Electronic passports, citizen cards, residence permits, drivers' licenses, and health insurance cards are rapidly becoming more widespread. The majority of these solutions are based on contactless smart card technology, for enhanced security a substantial fraction is integrating biometric authentication.

In many countries, capturing and storing biometric data is regarded a sensitive privacy issue. In the case of ID documents, legal frameworks often need to be amended, and regulations on the implementation need to be agreed upon well in time before a roll-out. International standardisation is fundamental for such e-ID solutions - a passport or driving license that does not guarantee international acceptance would be of little use.

Biometric Passports

The most prominent e-ID solution in this context is the biometric passport as standardised by the International Civil Aviation Organization (ICAO) [7], a combined paper and electronic identity document that uses biometrics to authenticate the passport holder. The passport design makes use of an embedded contactless chip, conforming to ISO/IEC 14443 [3], which is able to secure biometric and other data against unauthorised alteration and thus to guarantee the integrity of the passport.

The currently specified biometrics used for this e-ID solution are facial recognition (mandatory), fingerprint recognition, and iris recognition. The chip stores only the digital image of each biometric feature, matching of biometric features is performed externally by electronic border control systems.

European e-ID Programmes

Within Europe, a number of additional programmes for e-ID solutions are underway, including:

- **European Citizen Card (ECC)**
Several European countries have already launched national ID card programmes that support authentication for e-government and e-business services. The European Citizen Card (ECC) specification aims to harmonise national ID cards within Europe. The ECC contains a smart card chip that will hold personal data such as the holder's name, date of birth, height and eye colour, and in addition an electronic photo and two fingerprints. The sensitive biometric data is protected from unauthorised access and can only be read by authorised parties via a special authentication certificate. For e-government applications the ECC allows for additional authentication and electronic signature functionality.
- **Residence card for non-EU citizens**
Similar to the ECC, the new, harmonised EU resident permit will be a smart card-based document and will include two biometric identifiers, a facial image and two fingerprints. Depending on country-specific requirements, the dual interface chip can also incorporate other applications. Scheduled for introduction from 2010, the resident permit can act as a temporary entitlement to residence, as a permanent residency permit, or as a visa.

- **Electronic driving license**
Today there are more than 100 different driving license models used by European citizens alone, and all of them need to be mutually recognised. In a first step towards harmonisation, a number of countries have started deploying (man-readable) credit card format driving licenses. For a second step, ISO/IEC 18013 specifies a machine-readable, credit card-shaped driving license. Part 2 of ISO/IEC 18013 was published in 2008 and establishes guidelines for the content and formatting of data stored on the driving license [8]. It creates a common basis for the international use of such data without restricting individual authorities from applying their specific data policies.
- **Electronic European Health Insurance Card (eEHIC)**
To simplify the procedure for receiving medical care that might become necessary during a temporary stay in another country, it is planned to introduce an electronic European Health Insurance Card. The eEHIC will be a smart card which can be electronically read in the premises of healthcare providers and whose validity can be verified on-line. While standardisation of the eEHIC architecture has just started, it is recognised that in the short and mid term it will be necessary to support the existing national or regional cards to some extent.
- **Registered Traveler Program (RTP)**
Still under study is the introduction of a European registered traveller scheme that enhances the customer experience and accelerates passengers clearance without lowering the levels of security. This is anticipated through a combination of technology, process and people-related advances accessed by registered passengers who are judged as 'not high risk'.

While these and additional programmes contribute to an impressive list of e-ID activities underway, it should be noted that there are severe challenges regarding the progress and adoption of related standardisation activities. In the case of the e-ID card for instance, eight European countries have already implemented solutions - e-ID cards which are not interoperable at all.

4 CONCLUSIONS

During the last 25 years smart card technology has emerged as the preferred e-ID solution, by offering mature technology, quality and an excellent performance/price ratio. The technology platform of smart cards allows for securely hosting and managing logical and physical identity credentials, well suited for both enterprise and government environments, including e-ID programmes on a nationwide scale.

The trend towards deploying a holistic identity and access management system suggests that there will be an increased demand to merge VPN, physical access and desktop security. The need for consolidation of credentials is becoming more evident, and smart cards represent the ideal identifier for consolidating credentials.

Identity and access management (IAM) plays a significant role in helping maintain the integrity of an enterprise's reporting process. While IAM is just one element of the overall compliance processes, it can help make these processes significantly easier to implement, maintain and audit.

A large variety of e-ID solutions for the public sector is currently being designed or implemented. To take the benefit of existing standards, existing infrastructure, and existing experience, a common framework for these e-ID solutions should be adopted - as it is already the case for travelling documents, electronic passports, and electronic identity cards.

5 REFERENCES

- [1] Fumy, W.; Sauerbrey, J.: Enterprise Security, Publicis Corporate Publishing, Erlangen, 2006.
- [2] ISO/IEC 7816: Identification cards - Integrated circuit cards (Parts 1 to 6).
- [3] ISO/IEC 14443: Identification cards - Contact-less integrated circuit cards - Proximity cards (Parts 1 to 4).
- [4] RSA Laboratories: PKCS #11: Cryptographic Token Interface Standard, v2.20, June 2004.
- [5] FIPS Publication 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors, 2006.
- [6] Datamonitor White Paper: A New Look at the ROI for Enterprise Smart Cards, 2008.
- [7] ICAO Document 9303, Part 1, Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability, 6th edition 2006.
- [8] ISO/IEC 18013: Information technology - Personal identification - ISO-compliant driving licence (2 Parts).