



Corporate Badge

Raising security and usability with a multi-purpose company card

The number of plastic cards we carry around in our wallets is constantly increasing. There are credit and debit cards from financial institutes, loyalty program cards from shops, airlines and clubs. But not every plastic card is the same. Some plastic cards are equipped with a magnetic strip that holds information about the owner. Other plastic cards – so-called smart cards – have a chip that processes data and supports Radio Frequency IDentification (RFID) and cryptographic functions.

THIS PAPER IS ABOUT THE SMART CARDS that are used for identification and access control by companies and organizations: corporate badges. Optical identification, physical access at doors, logical access to systems and even cryptography (encryption and digital signing) can be combined in one card. The same mechanisms used for authentication at a cash point can be used to protect the facilities and data of an organization from unauthorized access. Having just one advanced card promises lower costs, higher security and higher user satisfaction.

The choice of appropriate cards and software, as well as the integration of badge management with the organization's processes, is not easy. This paper outlines the numerous aspects that an organization needs to consider to make the correct choice of technology and to ensure successful integration and deployment.

The Corporate Badge

The concept of a corporate badge implies that one card can be used for multiple purposes. Every employee will receive one card to deal with all physical and logical access mechanisms within the corporate boundaries. The use of two-factor authentication (2FA) for logical access to IT systems is enabled through Public Key Infrastructure (PKI) technology, which does not need



to come at the cost of user convenience. And, if the relevant aspects have been carefully considered beforehand, card production and subsequent card life-cycle management will be cost-efficient.

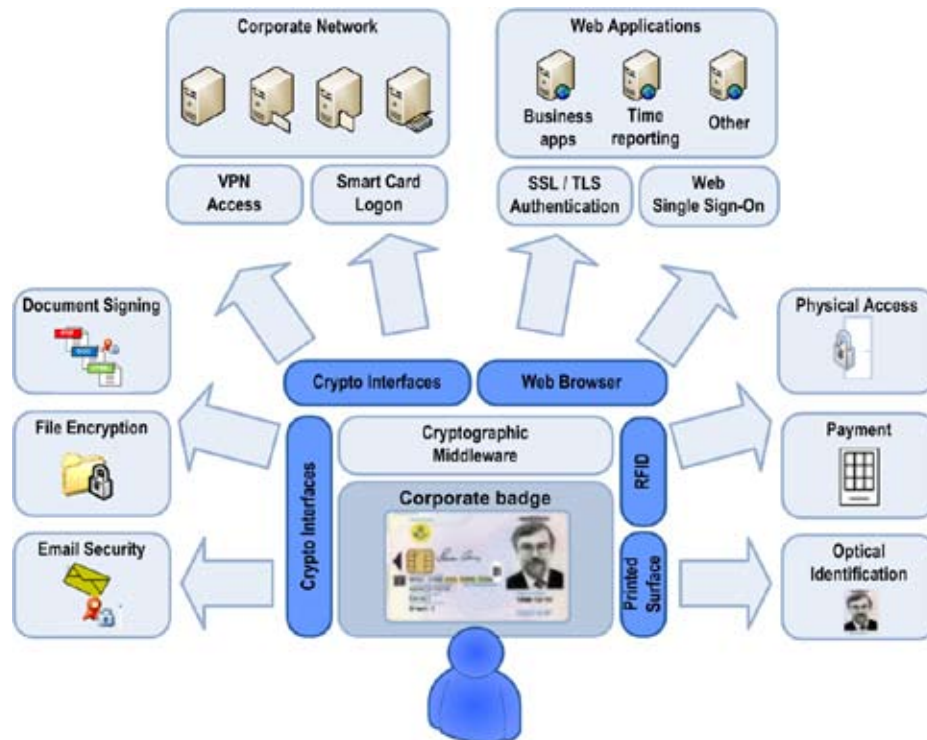
The same mechanisms used for authentication at a cash point can be used to protect an organization's facilities and data from unauthorized access.

The corporate badge unifies all identification and access functions within the organization. The badge opens doors, lets you pay in the canteen, logs you in to computers and IT services, and enables you to sign travel expenses requests. It accompanies you throughout your work.





WHITE PAPER



The functions

A corporate badge is three different ID cards in one:

1. An ID card for visual identification – a graphically printed plastic card, often with a photograph of the owner together with other information tying the owner to an organization, a specific department or role in the company.
2. A key card for physical access – a plastic card equipped with a magnetic strip or contactless RFID functionality for door passage.
3. A logical access pass – a smart card equipped with an ISO 7816 cryptographic contact chip for secure authentication by IT systems and applications.

Even though the card holds three different functions, the number of applications is much larger. You can open several doors in several buildings with the same card. When working with a smart card for logical access, single sign-on (SSO) to multiple software applications is often accomplished. Time recording is standard and some companies also implement an internal cash function for the staff canteen. There are

many ways to achieve general usability and the challenges often only lie within the organization itself where different functions are managed by different departments and are therefore more difficult to coordinate. A management-driven approach to set up appropriate processes is crucial for successfully implementing the corporate badge.

Cost-effectiveness

Having one single multi-purpose card in place of several cards will immediately reduce the related production and maintenance costs. The cost of subsequent life-cycle management and emergency handling will bring further savings in comparison with an IT landscape with numerous passwords and cards in use.

A larger number of PINs is known to be a considerable cost factor. Many reports show that helpdesk costs associated with resetting and unblocking applications due to users forgetting their passwords are very high: in a typical “multi-password” environment, users tend to need 1 to 4 password resets a year, with each case costing \$25 to \$50. The higher the number

Nexus

www.nexusafe.com
contact@nexusafe.com



Identifying and Authenticating
the Connected World



WHITE PAPER

of PINs and passwords, the higher the probability of forgetting them and the higher the costs.

Two factors increase security

Smart cards increase the overall security level simply because the need to constantly use them enforces compliance with security policies.

One important security feature of a smart card is two-factor authentication. An authentication factor is something that verifies a person's identity. Authentication factors are generally divided into three different classes:

- ✓ A username/password combination and personal identification numbers (PINs) are **knowledge** factors, meaning they are something that (hopefully) only the holder knows.
- ✓ **Ownership** describes something that a user is in possession of (a smart card).
- ✓ **Inherence** is something that the user is (a fingerprint).

Combining at least two factors is seen as "strong authentication" and is considered to provide a good basis for high security.

The use of two-factor authentication with a smart card and a corresponding PIN (ownership and knowledge) is the most common combination for "strong authentication" and is a method often used to protect people's bank accounts.

The human factor, acceptance and efficiency

Often, when implementing security solutions, users either fear that their everyday work will become more complicated or that there will be more restrictions. With the corporate badge, working life actually becomes easier for users. There are less cards and tokens to keep track of and fewer PIN codes to remember. A larger number of PINs - as easy to deal with as they might seem - can comprise a significant obstacle in practice. Not only do they generate costs in the IT department for resetting and unblocking procedures, they may also temporarily hinder employees from working until the problem gets fixed.



Having one multi-purpose card will increase usability and raise acceptance. The idea of one card and one PIN is easy and will be intuitively adopted. The general and constant use of this one card quickly becomes a habit. A person is not likely to forget the card in the card reader of his or her computer if the same card has to be used to operate the coffee machine or open a door in order to leave the building.

A combination of a smart card login with a security policy that locks workstations automatically upon smart card removal is good security practice and a step towards user convenience. Single sign-on is the next natural step for an organization to take, and will effectively save time and make logins for diverse applications even more convenient.

Single step card production

The easiest and most efficient way to produce a multi-purpose card is to do it all in one single step. Card management systems (CMS) gather user information from external sources, like corporate directories, graphically print the card, encode the RFID chip for physical access and personalize the cryptographic chip for logical access. The single step production is highly suited to large volumes, where production can be done in batches. Every employee then receives a card together with a letter containing the associated PIN code.





Evaluation of card management systems

Purchasing and deploying the card management system will probably be the most significant investment. Many things have to be considered long before a CMS is deployed and the exact requirements can only be ascertained individually for each company or organization.

The basic aspects to consider before investing in a CMS are:

1. Supported card functionality – make sure that all your requirements for the card are supported by the CMS and the attached card printer.
2. Flexibility – integration with existing systems. In order to have an automated process for personalizing cards, sometimes information must be gathered from several different systems, such as directory services and HR databases. In some cases, it could be appropriate to push information to other systems, such as the physical access control system. It is then crucial that the respective integration with the company's processes can be easily implemented.
3. Scalability – how does the CMS scale with the card production volume you have today and does it allow you to grow as expected?
4. Additional features – different CMS offer different lifecycle management features. User self-services enable users to block lost or stolen cards and to unblock a card if an incorrect PIN is entered by mistake themselves. Alert functions enable reminder e-mails and warn the user when e.g., the card is about to expire.

Careful planning and the choice of a suitable, scalable and flexible card management system that meets all requirements ensure cost-effectiveness.

Individual considerations

Many organizations already have some authentication and identification solution in place, sometimes even a smart card-based PKI solution. The questions to consider then are: Does the card solution need to be

replaced or can you build on it? Is a card solution in place that can be extended with new functions?

If you already have invested in a flexible and scalable smart card-based PKI solution, the good news is that the implementation of corporate badges should be straightforward. The way to go is a flexible and scalable card management solution with attached card printer. Integration with the PKI is usually fairly simple.

Other individual concerns to address may be coordination in diversified and distributed organizations. Card management may have to be dealt with by each department or location separately. And, what if your office space is rented and the landlord manages an independent physical access system?

Providers' various approaches

There are many card manufacturers who can offer cards with any required functionality. It is also possible to order cards with a custom configuration, where you choose the exact card components. You can find manufacturers that create cards from scratch by adding all components, while others will start with a card that already has one or two functions and simply add the rest.

There are also companies that offer card management as a service, which may be a very cost-efficient alternative if only standard demands need to be met.

Promise fulfilled

You can rest assured that there is always a technical solution once the political and organizational challenges have been overcome. As soon as all relevant aspects have been considered, requirements defined and organizational obstacles pushed aside, the evaluation and choice of technology will be much easier and the decision straightforward.

After the successful integration and deployment of the chosen solution, the production of the badges can begin. Finally, the promise of lower costs, higher security and higher user satisfaction can indeed be fulfilled with just one advanced card.

