



Security Magazine

2009



Card and reader security

will become increasingly more important in the future

Airport gate control - manageable at last

a winning combination that significantly
improves security and efficiency

nedapo[®]

Table of contents

2009

Trends

Card and reader security	3
Airport gate control - manageable at last	5

Case studies

Belgacom chooses AEOS to go 'All IP'	8
Access to University of Applied Sciences INHolland	11
Fundación Albéniz	14
GUST University in Kuwait	16
AEOS and Aperio implemented at Mürdter	18

Solutions & Products

Wireless access control in AEOS	18
Graphical Alarm Handler	20
Nedap AEOS & Hitachi Finger Vein	22
New: the Invexs series	22
ISMI -- International Security Management Institute	23

Reader Service

Nedap N.V. Security Management
Marketing & Communications
Phone +31 544 471 743
Fax +31 544 46 42 55
E-mail info@nedap-aeos.com

Reproduction is subject to permission
from Nedap Security Management.

Nedap®, AEOS®, AEOS faces®, etc.
are registered trademarks of Nedap N.V.

Card and reader security

Until just a few years ago, card and reader security was never much of an issue. Large numbers of people were using Mifare Classic RFID cards to everyone's satisfaction. But when the card's encryption was broken, the security of millions of RFID cards could no longer be guaranteed. Companies were forced to look into the security of their cards and card readers.

A company's overall security is determined by a wide range of aspects. Material aspects such as the kind of building where the company is located and the door types that are used in the building are relevant security factors. But also immaterial things like the kind of organization and the discipline of its employees play a crucial role.

Additionally, the security of the equipment is essential to determine the security of a company. When it comes to the protection of the access control equipment, things like login, database protection, network security and card and reader security are important matters that need to be taken into account.

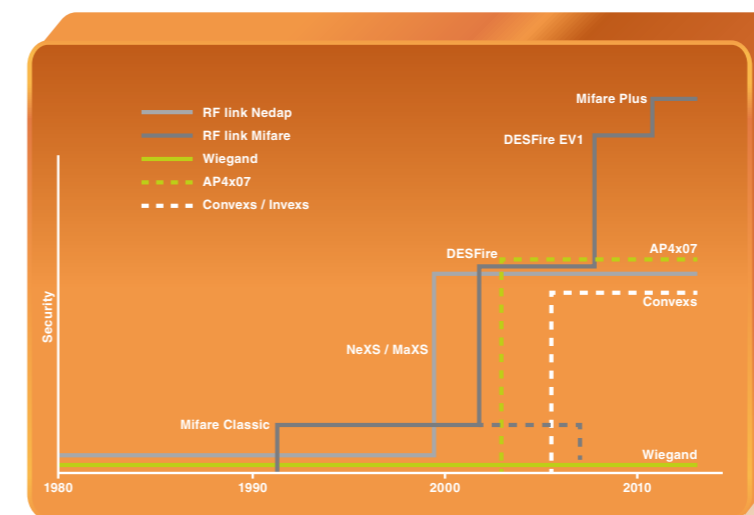
Security of cards and readers

Although card and reader security is one of many security aspects, it certainly is a crucial one. Card and readers are literally and figuratively speaking the key to your building, making it essential to protect them. If the security of the cards and readers is not looked after carefully, all other security measures become irrelevant. Three critical aspects should be considered.

The first one is the RF interface. The communication between the card and the reader is done through Radio Frequency. As soon as the card comes within range of the RF field of the reader, the information on the card is being processed and decoded and then transmitted to the reader. When this transmittal is not protected, the information is freely available, creating substantial security risks. That's why the RF interface is usually protected with authentication and encryption. Authentication is used to perform a check of mutual trust; encryption makes sure that the data that are being transferred are unreadable for outsiders. For both methods, an algorithm and a key are necessary. In order to ensure maximum security, it is common practice to use a public algorithm, so that researchers can evaluate if the claimed security is sufficient, and a key that for obvious reasons is always kept secret. Common algorithms are Crypto1 for Mifare Classic cards, 3DES that is used for DESFire, NeXS and UltraLight C cards and AES 128 for Mifare Plus and DESFire EV1 cards.

The second security aspect to keep in mind is the uni- or bidirectional interface between the reader and the controller. The protection of this interface can be plain, for instance with Wiegand, but it is preferable to encrypt the communication. The encryption can be generated in the reader, but this still leaves room for a breach. It's more secure to have the encryption inherited from the card being used. This is particularly safe as the encryption goes directly from the card to the controller on the safe side.

Finally, key storage is vital, because if the key can be taken out of the reader, all security measures taken are rendered useless. Keys can be stored in flash or a volatile memory, but the latest development in access control is SAM or Secure Access Module. This hardware module has a tamper-resistant crypto processor and a secure memory, in which it can securely store cryptographic keys and take care of the encryption and decryption of algorithms. It can even handle key diversification, a powerful security tool that procures that every single card has a different key that derives from the



master key. If one card would be hacked, the damage would be limited to that card. Nedap is one of the first manufacturers that has integrated SAM in its readers.

Security threats

An unpleasant but inevitable part of security is that there are always people who want to break the encryption. In a brute force attack they systematically try a large number of possibilities with fast computers. They can also intercept data on the RF channel, called eavesdropping. Or they record a communication message, such as the badge number of an authorized person, and replay it later to get access. It is even possible to use someone else's card without owning it or knowing anything about algorithms or keys. In such a relay attack the attacker only forwards the data; he relays the communication between the card and the original reader. When the owner of a card is sitting in a restaurant, for example, the card is read unnoticed by a reader of the attacker. The code is transmitted wirelessly (e.g. GPRS) to a second attacker who receives the code and presents it with a card emulator to the original reader. Other ways to hack encryptions are cloning, emulation or side channel attacks.

Security developments

Despite all these security threats, card and reader security was generally at a low level until the year 2000. Most reading configurations were secured in a conventional way, storing the key in the reader firmware and realizing the interface with Wiegand, clock-data or another simple connection. No encryption was used between the reader and the interface, making interfacing simple. Only with the introduction of the Nedap **NeXS card** and the NXP Mifare DESFire card, RF link security increased considerably.

A positive development was the creation of Nedap's **AP4007 Mifare reader** with a passive antenna, where the key is stored in the Mifare reader unit. The big advantage of this is that the antenna and the active reader can be installed up to 30 meters apart. This means that the active reader can be installed on the secure side of the wall, keeping all the sensitive components and data within the secure area and reducing the risk of sabotage to a minimum. Furthermore, the encryption is inherited from the card, ensuring a high level of security.

With the Nedap **Convexs** and **Convexs SAM** readers, two multi-frequency readers with multiple interfaces were developed. In the case of the Convexs reader, the key is stored in the embedded protected flash memory and the RS 485 communication is encrypted with the RC4 algorithm. The Convexs SAM has similar functionality, but the difference is that the key can be stored in a SAM. This guarantees that the key cannot become known to outsiders.

Then the encryption of the Mifare Classic RFID card was broken in December of 2007. All of a sudden the security of millions of RFID cards could no longer be guaranteed and manufacturers were forced to think of other ways to protect the reading configurations. Since then, card and reader

security has progressed in a rapid pace and is now directed at the further development of the DESFire EV1 card and the Mifare Plus card (see figure).

Effects

The effects of these new developments are diverse. The Mifare Classic card is likely to disappear gradually. And since the old systems cannot yet handle new cards very well, manufacturers will be forced to revise their systems. The end users will not notice much of all this, but consultants and customers will have to acquire knowledge of the relevant technologies, especially concerning encryption and related fields. With the Nedap Convexs reader a smooth migration to other cards is already possible. It is capable of reading a mix of Nedap and Mifare/DESFire credentials, allowing for gradual migration from one card to another. This is particularly handy when a company has many cards in circulation and it is therefore impossible to change all cards overnight.

Depending on the kind of application for which they will be used, cards will have to comply with different requirements. For comfortable and secure cards, the Nedap NeXS card with 3DES authentication is an excellent candidate. This badge has already been developed by Nedap years ago and is Nedap's response to the increased demand for affordable high-security access badges. UltraLight C can also be used for access control. And for additional applications like cashless vending, Mifare Plus is a good choice. For multi-functional applications that require maximum flexibility and security, and therefore highly advanced cards, the DESFire EV1 will be the best option.



Conclusion

Card and reader security is only one of the many elements of a building's overall security. Nevertheless, it will become increasingly more important in the future. As things go, a high level of security can be obtained with the latest solutions. The Nedap Convexs reader and Nedap NeXS card are perfect examples of the products that are currently available to fully comply with all security demands. And the innovative character of Nedap will surely bring along new progressive products in this respect.

Airport gate control - manageable at last

Gate control plays a crucial role at airports. Until now, gate control was often managed locally at the gate. This will change with gate control by Nedap. The gate control application derives from Nedap's security controller, the world's first controller that combines all security functions previously performed by separate dedicated systems in one generic device. The so-called gate controller links the gates with a network that centrally monitors the door settings and with a database that contains the personal data and biometric characteristics of the airport's staff. At the same time, the controller manages the task of locally controlling the gate. A winning combination that significantly improves security and efficiency.

At European airports, gate control is essential for monitoring the difference between Schengen and non-Schengen* passengers. The situation at many airports is still such that the staff member who is responsible for the gate has to personally check all the entrances each time an aircraft arrives or departs. This person controls the doors for each docked aircraft, either manually or using some form of technology. The gates are multifunctional and are used for flights from Schengen and non-Schengen countries. For that reason, access via the gate needs to be set up in a way that arriving and departing travelers are separated accordingly. The most important issue is to be absolutely sure that the various passenger flows follow different routes. The gate doors are generally controlled using passes or a key system, possibly in combination with a local technical set-up

that locks or opens the doors. This often requires a manual intervention that has to be performed under the supervision of the authorized member of staff who is present.

Risks and consequences

There are all kinds of circumstances in which something can go wrong with controlling the gates, with all the ensuing consequences. When door settings are incorrect and passengers from Schengen and non-Schengen countries are mixed, serious measures have to be taken to restore security. The gates have to be evacuated, as well as all the docked aircrafts and the areas between the security check and the gates. This is a time-consuming operation. There is also a real risk that the key or the pass that operates the gate falls into unauthorized hands.



There may also be situations where the doors to the gate remain open longer than strictly necessary. Each time this happens, valuable minutes are wasted, which amounts to many (expensive) lost hours each year. Furthermore, the chances of a human error by the gate staff cannot be ruled out. The problem is that these errors are often not registered since they take place locally and there is no check on whether or not the gates are set to the right configuration. While an alarm generally sounds when doors are illicitly opened, this always takes place after the event. Systems based on local management also have the disadvantage that the settings cannot be easily supervised or checked. The implementation of changes in order to adapt or optimize processes is also complex and time-consuming.

Gate controller

One thing is certain: the process at the gate can be optimized in various areas and ways. In collaboration with NEDAP, a number of airports have drawn up a list of requirements to make their gate controls both easier to check and more secure. NEDAP has developed a workable solution based on these requirements. The main objective was to keep existing local control equipment operational in view of the investment involved.

Linking the control system to a network infrastructure was the main change that NEDAP introduced. All the gate doors in the system can now be monitored online via the network. The gate controller plays a crucial role in this. The operating equipment and the doors are connected to this controller. The programs that control the doors are still locally present (in the gate controllers) but are visible in the central online display. Moreover, the system can reference staff data and data relating to contractors who may be active at the airport both centrally and locally. This information includes the passes that have been issued to these persons and their biometric data. The gate controller links the personal data on somebody's pass, that person's biometric data and the code (flight number) to a defined door configuration. After the correct values have been entered, the gate is set up according to the agreed procedure.

Greater security

Verification of the identity of the staff member who is authorized to operate a gate is an important factor in improving gate control security. Verification using biometric data minimizes the chance that unauthorized personnel operates the gate. Security and efficiency are further improved by the use of codes or flight numbers to automatically set doors

to the right configuration. The authorized staff member at the gate enters a code (or flight number), which is used to automatically set the gate doors to the right position. This takes place locally, because it happens regularly that aircrafts have to dock at another gate, making it necessary to change the door settings as well. The doors that have been set generate a feedback signal to confirm that they have in fact adopted the set configuration. Only then does the process of aircraft embarkation or disembarkation start. The doors at the gate are opened for a programmed time. Movement detectors signal the movement of persons in the gate. If movement is no longer detected for a preset time, the gate door closes automatically. Obviously the door can also be closed before this (centrally/locally).

Greater efficiency

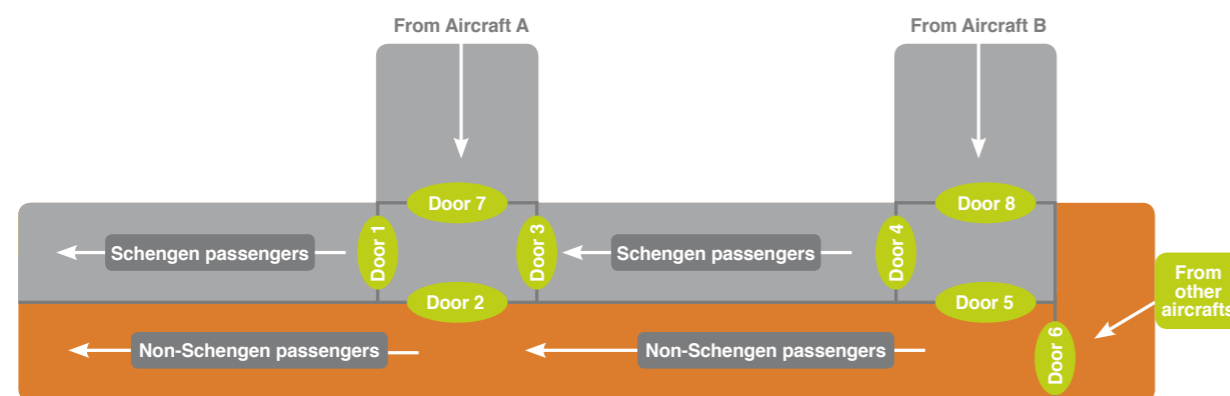
The use of a network infrastructure and gate controllers saves time and makes it possible to operate the gates with less personnel. The chance of errors is also minimized and possible errors/abuse are reported immediately. The network allows the control programs at each gate to be viewed and ensures consistent control. A network failure does not prevent execution of the programs as they are locally active. Implementing changes to the control program however takes place centrally; this is faster and less complex than changing all the gates at local level. The link to the HR system means that a staff member's personal data are directly accessed by the gate controller. The information at the gate is always current because the system is updated immediately when a staff member leaves the company or when a staff member's authorization is suspended. All the events relating to persons, gate operation and door positions are collated and given a clear date and time stamp. The system can be set in such a way that combinations of events automatically result in an increased state of alertness or trigger an alarm. Data that are stored in the database can easily be retrieved via a search function and are directly available.

Visual identification

Some airports have indicated a need for visual identification when setting and operating the gates. This can also be engineered via the gate controller. Video images can be linked to existing authorizations by connecting a local IP camera to the gate controller. This means, for example, that the gate may only be released for operation after the image of the staff member has been verified against the information in the database. A further option is to store the video footage together with the registered events. This can be particularly handy when events need to be evaluated at a later stage; instead of looking at badge numbers, you can immediately see the faces of the people involved in a particular event on the corresponding video footage.

NEDAP's gate controller enhances gate control security and efficiency through (visual) verification of staff members, central control of settings and local gate control following the entry of a code. The airports where this controller is in operation are very enthusiastic about the system. Gate control is fully manageable at last.

Separating passengers is a major security objective at international airports. Regardless of the type of passenger: travelers who are arriving or leaving, passengers who have reached their final destination and those who are in transit to another destination, passengers from Schengen and non-Schengen countries, managing the separate passenger flows starts and ends at the gate.



* The Schengen countries (Belgium, Denmark, Germany, Estonia, Finland, France, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Norway, Austria, Poland, Portugal, Slovenia, Slovakia, Spain, Czech Republic and Sweden) have entered into agreements that facilitate the free movement of persons. Named after the town where the agreements were signed: Schengen in Luxembourg.

Belgacom chooses AEOS to go 'all IP'

In 2006, the Belgacom group – Belgium's leading provider of telecommunication services – decided its various access control systems needed to be migrated to an IP-based system that would be consistent throughout the company. The group also wanted to introduce an integrated, higher-level security platform. Careful comparison led Belgacom to opt for the system that satisfied all their requirements: Nedap's AEOS. Telindus, one of Nedap's business partners in Belgium, is responsible for the implementation of the AEOS system.

As in many companies, access control at Belgacom has grown organically along with the company's expansion. This resulted in the use of three different access control systems, each with its own database and two of which were not native IP-based. Nearly 300 buildings were using a VSK (Wesp & Foxnet) system with a total of 1,250 card readers. More than 450 buildings were equipped with an ID-Tech system with 1,600 card readers, while Belgacom headquarters in Brussels was



using MAXxess. The only common denominator was that all three systems used Hitag 2 badges.

Ripe for change

"The situation was definitely ripe for change," said Marc Moris, Corporate Prevention & Protection Director at Belgacom. "Non-IP based systems are really a thing of the past. We wanted to migrate to a single, IP-based system that would be implemented throughout the company." Standardization was to take place, starting with the replacement of the 'ancient' non-IP based VSK systems (1,250 badge readers).

Initially, Belgacom aimed at simultaneously introducing a higher-level security management platform to integrate all its security systems (access control, cameras, intrusion and fire detection). It was later decided to split this into two separate projects: Access Control IP Migration and Integrated Security Platform. Dividing the projects considerably accelerated the decision-making process and facilitated implementation. Belgacom selected Nedap AEOS for the IP migration and Entelec Skywalker as the (graphic) platform for integrating all of the company's security systems. Both projects were to be implemented by Telindus.

No dinosaur

Belgacom's main reason for selecting AEOS was the system architecture and in particular its scalability and flexibility. AEOS can work with an unlimited number of remote control units and -- in very large systems -- with multiple application and database servers to maintain its standard high performance. The fact that AEOS uses standard hardware modules and embedded software components is a major advantage. It means the system can be expanded infinitely as Belgacom's needs change, without requiring Belgacom to buy any hardware or functionality until they are actually needed.

Additionally, AEOS can handle a limitless number of badges. Moris: "Because of the phasing of the project and the possibility that that card technology will change in the future, it was crucial that we find a system flexible enough to accommodate growth and change. We did not want to find ourselves a few years from now with a dinosaur. We wanted to make absolutely sure that we could migrate to other card technologies or integrate biometric applications without having to replace all our card readers." This was another requirement that AEOS could easily meet: it seamlessly integrates with most card technologies, such as Hitag, HID, Mifare and Barcode, using Wiegand, Omron, RS232 and similar communication protocols. Migration is simple and there is no need to replace existing cards and card readers. AEOS is also suitable for integration with biometric systems and offers a user platform for enrollment and verification of biometric parameters (fingerprints, handprints, face recognition, iris identification).

Fully compliant

"Another important consideration," added Michael van der Heijden of Telindus, "was the requirement that native IP controllers could communicate peer-to-peer, independently of the server. Belgacom put a lot of stock in the redundancy and security of the system. They wanted it to be possible to use different servers for application and database. Plus they wanted communication over IP between the controllers, between controllers and server and web-browser-based clients." AEOS controllers are the system's distributed intelligence. The AEOS Processing Units (AEPU's) store the user-defined local functionality, such as all the authorizations for the connected readers. Each AEPU can function as a stand-alone unit or be connected to the IP network to communicate peer-to-peer with other AEPU's and IP-based devices independently of the server. In other words, truly native IP. "Our RFP included a compliance matrix of

course," Moris continued. "This is an exhaustive list of all the functionalities for which Belgacom had minimum



requirements. The vendors were asked to indicate whether they were fully compliant, not yet compliant but ready by the beginning of the project, partially compliant or non-compliant. AEOS scored tremendously well on this. They were able to answer almost all the questions regarding the access control system with FC, Fully Compliant."

Customized functionality

Peter Rommens of Nedap Belgium added that the flexibility of the AEOS system again proved to be its greatest asset. "That and our willingness to develop customized functionality for specific clients, provided it is compatible with our philosophy of developing software that can be integrated into the general system and made available to other customers. In this case, we decided to prioritize Belgacom's wish for advanced Alarm Handler functionality within our general development process. But I'd like to emphasize that this does not mean the alarm handler is solely available to Belgacom. On the contrary, it's now completely integrated in the latest AEOS version. This approach has great advantages for

our customers, because the new functionality is automatically included in the next upgrade. We purposefully avoid building customer-specific functionalities because they can create problems in upgrades."

Roll-out

Implementation started in early 2007 with several pilot projects in smaller buildings. Telindus is currently rolling out the system. The system consists of five servers (an application server and a database server, two back-up servers for application and database, and a test server. So far, the hardware used includes 148 AP4803 and 54 AP4003 controllers; 32 AP3002 and 21 AP3004 controllers and existing card readers and Hitag 2 badges. In the long run, Belgacom will probably migrate to Mifare card readers and badges. The system is linked to HRM software (for importing personal data) and to Entelec Skywalker (a higher-level security management system).

provides both private and professional customers with a comprehensive range of solutions in fixed and mobile networks. It offers a complete quadruple-play solution that integrates fixed and mobile telephony, internet and television. Belgacom invests in innovation and draws on the latest technological developments to anticipate its clients' needs.

At the outset – when the project was first put out to tender – Telindus was one of Nedap's Belgian business partners. Following the merger of Belgacom and Telindus, the Belgacom Group's ICT activities have been offered under the Telindus brand, which was renamed Telindus-Belgacom ICT in June 2006. In its 40 years of existence Telindus has evolved from a technology supplier to a solution integrator and sourcing partner.



With implementation well underway, Marc Moris is convinced AEOS was the right choice: "We are very pleased with the performance of the system and the support Nedap has offered. Their 'can-do' attitude is highly appreciated. They were willing to really listen to us. That new, advanced Alarm Handler functionality was initially developed because we had a need for it. We feel we have embarked on a valuable long-term relationship."

The Belgacom Group is Belgium's reference provider of integrated telecommunication services. The Group

Belgacom: Facts and Figures

- 751 buildings in total
- 292 VSK sites (50 migrated to AEOS, 242 left to go)
- Approx. 17.000 employees
- 50,000 badges
- 1,370 access points

Access to University of Applied Sciences INHolland

transparent, keyless and online

The creation of the University of Applied Sciences INHolland and the introduction of a new education model started a continuous flow of employees and students between the university's different locations. This made it harder each time to comply with the organization's philosophy of openness and transparency as far as its access control was concerned. That was the reason for INHolland to start looking for a new access control system, setting a high level of ambition: 100 percent keyless and online.

Visitors to the site of the INHolland university in Rotterdam notice two things. The first one is the absence of any kind of access control and the second one is the tremendous spatial effect of the sixteen-floor building. Due to the use of a lot of glass, all class rooms and workplaces are open and trans-

parent. This explains immediately what Timo Stortenbeker, Manager Safety & Security, means when he explains why he started looking for a new access control system for all locations of the University of Applied Sciences about four years ago. 'INHolland practices a philosophy of transparency and wants to be welcoming and open. After the merger in 2003 we noticed that this became harder each time, because since then employees of central services such as ICT and HRM visit all locations. Apart from that, the introduction of the new major/minor education model caused teachers and students to also visit other locations more often. These developments made a normal and hospitable access more difficult. That's why we started looking for an access control system with which we could maintain our openness and transparency and give access to everybody up to the last level, and which would arrange access to a class room for example only at the last door.'

Facts and Figures

Organization:	University of Applied Sciences INHolland
Students:	32,000
Employees:	3,000
Locations:	Alkmaar, Amsterdam, Delft, The Hague, Haarlem, Rotterdam and branches
Access control system:	AEOS
Contractor:	Nedap Security Management
Number of card readers:	Momentarily: 600. Beginning of 2010: 750



'Management per section was very important for me. I wanted a system that fits the size of our organization and the decentralized organizational structure.'

'We offer convenience to our users and that's an added value that we are willing to pay for'

Business case

Until then, all locations still had keys, a situation that Stortenbeker wanted to get rid of. 'Keys would get lost and you would always have to make the decision whether to change a locking plan or not. In some occasions we did, but in others we didn't because of financial reasons. This means you're running a risk.' This was the reason for him to go after a solution that would be 100 percent keyless.

In practice, this turned out to be a very ambitious wish, says Joris Lampe (Business Unit Manager at Nedap Security Management). 'The narrative of our first meeting is that Timo had to explain things to me three times and that I asked him several times if I had understood correctly. I couldn't come up with any organization that really has a card reader for each door based on an online system and is thus 100 percent keyless. All this together made it a special project.'

Stortenbeker's idea was not only ambitious, it was also costly. In order to convince the management, he prepared a business case that provided insight into a number of expenses, specifically: replacement of locking plans after the disappearance of keys, issuance and collection of keys due to staff turnover, as well as other general and technical services such as laptops, telephones and facility cards. But also the need for security guards to have to walk to a class room to open it because employees refused to take along a key, and ways to make the problem of access control, due to employees working at several locations, manageable.

Management per section

After the Manager Safety & Security received the go-ahead signal for his plan, he formed a project team that consisted of a couple of general and technical employees and the coordinators of Security and Reception Services of the different locations. They formulated a so-called Program of Demands that the new system needed to comply with. The top 3 of the program was formed by scalability and management per section, user-friendliness and the possibility of connecting the system to other management systems. Stortenbeker explains:

'Management per section was very important for me. I wanted a system that fits the size of our organization and the decentralized organizational structure, in which a general and technical department can manage its own location in a protected area. But the system also had to be comprehensible and easy to use. The reason that the system had to have the possibility to be connected to other systems comes from the fact that we will be issuing keys via our management system for general and technical services. By connecting to the access control system, we can easily process these modifications.'

What followed was a market study that compared several systems, among others by implementing them in practice on a small scale. Ultimately, INHolland decided upon Nedap's Aeos because it complied best with the Program of Demands.

Early consultation

Despite all the preparations, the implementation of the new access control system experienced a more or less false start at the new housing built at the location in Dordrecht. 'This was caused by the fact that the project in Dordrecht was already running and our general and technical service was involved too late. Because of that, Dordrecht is not fully keyless, although we managed up to the level of compartments', comments Stortenbeker. The lesson he learned from this, is that for future projects he sits down with his colleagues of Real Estate at an early stage, making sure that the installer gets floor plans that show where Security wants the card readers to be placed.

The result is that INHolland, partly thanks to the many new buildings that are being constructed, is progressing well in reaching Stortenbeker's ideal, keyless world by now. In Delft and The Hague, keyless buildings will be surrendered shortly, in Rotterdam 15,000 m² of newly constructed buildings have been realized keyless and the existing building of 20,000 m² has been reconstructed as such. As far as the other locations are concerned, the existing system is scheduled to be reconstructed and for the locations

Amsterdam and Alkmaar it will be included in the building plans. Stortenbeker: 'I expect to be complete in a time span of four to five years.'

Super user

Being asked if the system meets his expectations, Stortenbeker frankly responds 'yes'. He continues: 'It is very satisfactory and yields a lot. And what's more, the users notice it as well and value the advantages.' He then explains how he organized it in practice: 'I myself am the so-called super user of the system, which means that I determine what way to go. Next, we have the department of functional management that maintains and manages the system in cooperation with the ICT department. The authorizations are granted at the locations by the general and technical employees, but there are rules and I establish them. As for the authorizations of, say, technical spaces, the so-called outer layer, they are done by the coordinators of Security at the locations.'

Acceptance of the new system by the direct users didn't pose any problem, which proves that the system is user-friendly. Lampe: 'For the super user, the system is elaborate, but someone who uses just a part of it, only sees a part of it, which makes it much easier to use.' 'Here as well, you could see the advantage of the connectivity of the system', adds Stortenbeker. 'The majority of our users make use of our general and technical management systems for granting authorizations. The other part is done by functional management and the coordinators of Security and they can handle it after a short and simple instruction.'

And other users like teachers? Stortenbeker: 'They don't need instructions. In practice, it only becomes simpler for them. That's why they are eager to start using it as soon as they find out that we're going to install the new system. They will only need their badge, which they always carry with them anyways because they need it to buy coffee, make photocopies or a print-out.'



Joris Lampe (on the right) relates about his first meeting with Timo Stortenbeker (at the left): 'I have asked Timo several times if I understood correctly, because I couldn't come up with any organization that really has a card reader for each door based on an online system and is thus 100 percent keyless. All this together made it a special project.'

Wireless

Even though the new system is not fully implemented yet, there already is a new development: the wireless online card reader. Lampe explains what this means: The ironwork is integrated with a card reader and a cylinder inside. It communicates over five to ten meters with a hub on the network, which in turn communicates with the access control system. This reduces the costs of cabling considerably. In existing buildings, where it is mainly the last meters of cabling that are very expensive, you can save substantially.'

This development was interesting enough for Stortenbeker to take part in a pilot. 'It may help to implement the online access control systems in our existing buildings more easily.'

Being asked if this is the future of access control, Lampe answers realistically 'As soon as you can make the online solution cost-neutral compared to offline solutions, I would prefer the online solution. And as soon as wireless technologies make that possible, you're there. But don't underestimate the reality. Banks don't want wireless systems, certainly not when it comes to security. Neither do hospitals want to have wireless connections. So you have to watch the situation carefully and listen to your client. Whichever way you look at it, wired systems are still more trustworthy than wireless systems. You are talking about access and the question you should ask yourself is whether you want security or convenience. If you want security, you will want to have assurance. But those are considerations that the end user must make.'

Added value

Considerations in which the costs nevertheless always play an important role, recognizes Stortenbeker. 'With each new project we realize that a lot of money is involved, but then we reach back to the business case. Obviously this doesn't cover the whole investment, certainly not, but we also offer our users of the new system convenience and that's an added value that INHolland is willing to pay for.'

Photocredit: Eduard van der Worp

Publication: Security Management Magazine (Arjen de Kort)

Summary

- The access control system of the University of Applied Sciences INHolland did not comply any longer with the organization's philosophy of openness and transparency
- The university looked for a new system with a high level of ambition: 100 percent keyless and online
- With a business case a number of expenses were made visible, after which permission for the purchase followed
- The new system complies with the most important wishes from the Program of Demands: scalability and management per section, user-friendliness and connectivity with other management systems.



Fundación Albéniz

Fundación Albéniz is a non-profit organization dedicated to the education of new talents in the field of performance and composition of classical music. The organization is located in a modern seven-storey building in the historical and cultural center of Madrid and has recently been equipped with AEOS as its access control system.

The organization's building consists of a number of areas with specific access needs and Fundación Albéniz wanted a system to control the access to the different areas. They were also looking for an online reservation system for class rooms in the building and an integrated online ticketing service and seating capacity control system for the auditorium.



By choosing Nedap's access control system AEOS, Fundación Albéniz has been able to combine the use of Mifare

type cards, ConveXS readers from Nedap and HID readers, biometrics from Sagem and Aperio wireless locks from Assa Abloy. With the combination of all these products, the strict requirements of Fundación Albéniz have been fully met.

Online reservation system

An online reservation system for class rooms was developed by INSTASOFT, who created a web-based application for students to reserve a class room at any convenient time. Thanks to the import module of AEOS, that can integrate with other applications and that can interact with a person's profile, the INSTASOFT system could be easily integrated. The student's reservation leaves a registration file in the import module of AEOS, allowing access to the student who made the reservation to the specified class room at the specified time.

Integration online ticketing service and seating capacity control system

The integrated online ticketing service and seating capacity control system for the auditorium was developed by connecting the existing ticketing service of



www.entradas.com with the AEOS database. Visitors to the auditorium get access to the premises through the turnstiles by presenting the barcode on their ticket. All tickets sold for a show are exported to the AEOS database, which then turns the number of sales into the number of visitors.

Wireless Aperio locks

Another feature in the building of Fundación Albéniz is the use of wireless Aperio locks from Assa Abloy. Six glass doors in the building did not allow for any cabling or antenna installation. Thanks to the cooperation between Assa Abloy and Nedap, these doors can now be controlled with wireless Aperio locks.



Elevator control

Since some of the areas in the building are restricted access areas, the use of the elevators also had to be restricted. To solve this, ConveXS readers have been installed

in the elevators, which activates the control panel if the person in the elevator is authorized to use it.

Access through mobile phone

In two nearby buildings, Fundación Albéniz has student residences that also needed to be equipped with access control systems. Because of the monumental architecture of the buildings, readers, antennas or surveillance cameras could not be mounted. Therefore, it was decided to use an access system with mobile phones. A VPN network was created in order to connect the buildings with AEOS. By simply calling a special phone number, the student's mobile phone number is identified by the AEOS database and if the number is authorized the door to the building is opened.

Facts & Figures – Fundación Albéniz

- System Integrator: Telefónica Sistemas Auditivas
- Installer: Niscayah España
- 110 access points
- Convex readers from Nedap
- HID readers
- Biometrics: Sagem
- Wireless Locks: Aperio from Assa Abloy



GUST University in Kuwait

Comprehensive and advanced security management



GUST is the first private university established in Kuwait. Being a university with a progressive and innovative outlook, GUST is envisaged to grow as a modern center of excellence for education and research in the fields of arts, sciences and business administration. GUST is a liberal arts university that offers four-year courses. Operating in a new state-of-the-art facility called the Mishref campus, GUST has enrolled more than 3,200 students since its inception.

During its five years of operation, GUST has continually improved and expanded its educational and organizational capacities while steadily increasing its enrollments. At its first commencement ceremony in June 2007, GUST conferred diplomas on approximately four hundred graduates, many of whom were eagerly received by the leading business sectors in the state of Kuwait.

With the move to the new and bigger campus, GUST decided to improve its security management system as well. At the old campus, GUST was using an outdated security



Student lockers at GUST University



system. The system complied with the university's previous requirements but it was not a web based application. When they moved to a bigger campus GUST decided to go with a centralized, flexible and IP based system with a comprehensive and advanced security management.

Nedap was chosen among different suppliers to provide a complete, integrated and future proof system from Vehicle Gate Control (TRANSIT) to Access Control (AEOS) to Class Attendance (PreAbXS/Gronos) and Locker Management (LoXS).

The AEOS access control system at GUST University consists of over 50 AP4801 Nedap controllers installed across the campus. Local functionality is created by deploying embedded software components to the controller; this then controls the entrances and provides the local integration. Over 400 DC080F antennas are used for providing access to the students and employees.

GUST's main objective is to use a "single sign-on" system with one unified access badge for multiple services such as cashless payment by using the Mifare technology. In addition GUST is now looking into adding the new state-of-the-art library to its integrated system as well.

AP5808 registration terminal in classroom



Having a single sign-on badge provides the students, faculty members and staff the flexibility of moving around the campus and using the systems that require a badge. This all-round solution from Nedap turned the university into a secure and manageable place. For a place like GUST University, where the number of people is increasing enormously in a

short period of time, this is extremely important in order to guarantee a safe working and learning environment.

The locker management system uses the same badge that is used for the other applications. When a student requires a locker this can be issued on a scheduled basis and it can be re-issued when free.

The class attendance system uses the AP5808 registration terminal to register the presence and absence of students by reading their student badge. The system is integrated with the AEOS access control system so the data can be collected at each entrance.

For Vehicle Control at the gates of the University's campus, the Nedap TRANSIT is being used. This long range reader identifies a vehicle at distances up to 10 meters, even when a vehicle is traveling at high speed.

The Nedap Certified Business Partner who implemented the system, INCUBE, is studying the possibility of implementing a middleware for all the systems available at GUST, including the NEDAP system. AEOS' open architecture will prove to be a secure and reliable backbone to carry out just that task.

Facts & Figures - GUST University Kuwait

- 150 teachers
- 2,500 students
- 525 doors
- # of readers: 629, including DC080, DC1400, TRANSIT, Gronos Registration Terminal
- # of lockers: 21 locker areas with 830 locker units

AEOS and Aperio implemented at Mürdter

Nedap N.V. Security Management has realized a seamless integration of offline cylinders in its access control system, in corporation with Assa Abloy. The first “wireless online” solution has been implemented at Mürdter Metall- und Kunststoffverarbeitung GmbH.

Mürdter “Mürdter Metall- und Kunststoffverarbeitung” is active in the automotive industry as a manufacturer of plastic and metal mouldings. Mürdter is situated at an industrial park, which is freely accessible. For this reason the security of the Mürdter buildings has to be done attentively and accurately.

For Mürdter, the most important reason to choose for AEOS as its access control system is the possibility to integrate wireless locks. The outer perimeters of the Mürdter buildings are connected to the online access control system. AEOS offers multiple possibilities to control and secure the online doors. However, for some of the doors at the inside of the building Mürdter wanted straightforward access control without additional security measures, and also without cabling. Either mechanical or offline locks weren't an option for Mürdter because they wanted to be able to monitor the inner doors.

With the Aperio Wireless Locks from Assa Abloy, the inside doors can be connected to the online access control system AEOS, without having to cable every door lock. Management and control of the locks can be done in AEOS. It is obvious that a lot of cost savings can be realized since the authorizations and access rights only have to be issued and configured in AEOS and no duplicate databases are necessary.

If an employee now offers his access badge at the wireless Aperio lock (available in escutcheon or cylinder) the online system verifies the authorization and if the person has been authorized, access is granted. The other way around, if a person's badge is blocked in AEOS, this is directly communicated to the wireless lock via the network and the person's access badge is both denied at the online doors and the doors with the wireless locks.

Wireless access control in AEOS

There are many ways to arrange the access to a company's premises. The simplest way is of course to have a traditional key system in place. This is fine for small companies that don't run many security risks, but it becomes a different story for bigger and high-security companies.

For them a traditional key system is far from being enough to protect them against security risks. The more keys are circulating, the more difficult it becomes to keep track of them. And what

to do if keys get lost or stolen? It's obviously very expensive and cumbersome to replace all locks and keys. These prob-

lems can be avoided by introducing electronic access control systems, where traditional keys are replaced by badges that can simply be blocked if they get lost or stolen.

Online access control

With Nedap's powerful security management system AEOS, security risks can be reduced to an absolute minimum. This online access control system is based on smart network technology, allowing companies to

manage and control people flows in their buildings. Its central server stores all kinds of security related information, enabling centralized management, reporting and real-time monitoring of events. It's a convenient system that gives companies full controllability and accountability of their access and security policy.

Wireless access control

What to do, however, if the cabling necessary for online access control systems can not be used everywhere in your building? For those situations, doors can be equipped with wireless locks that don't require any cabling. These stand-alone electronic locks have a micro electronic reader inside and run on batteries. Since no cabling is necessary, the installation costs of these locks are low. Thanks to an excellent new integration between Nedap's access control system AEOS and battery operated locks from Salto and Assa Abloy, wireless doors can now be connected to the online access control system, offering a single management platform to manage all of a company's access control needs.

Integration with Salto offline locks

Salto's battery operated locks do not have any wiring at all. They are stand-alone locks with an offline reader in the escutcheon or cylinder. The locks provide a lot of flexibility, for example at remote locations where installing wiring can be difficult or in old buildings where wiring is not allowed. By integrating Salto's offline electronic locks in AEOS, an integral platform is created to manage both the offline and online doors in a company's building. The authorizations for both the offline and online doors can be programmed in AEOS. The AEOS system forwards the authorization data via the Salto Offline System and the Salto R/W unit to

the access badge. The authorizations for the offline doors are written on the card. This so called “network on card” technology allows communication with the offline locks without the need for wiring or RF communication.

Integration with wireless Aperio locks from Assa Abloy

The locks of Assa Abloy have no wiring to the door either. They only require some cabling for the hubs through which they communicate, but this is a lot less than for online systems. Thanks to the Aperio technology the wireless locks from Assa Abloy are able to communicate directly with AEOS, making it possible to issue and configure all authorizations and access rights in AEOS. The system uses the same authorization schemes for wired and wireless doors, allowing companies to simply monitor and control both types of doors in AEOS. With this integration a unique “wireless online” solution has been created.

Best of both worlds

For companies that want wireless doors, but still want to be able to manage and control all doors from one single management platform, these two new integrations offer a cost-effective and flexible solution. The problem of cabling is no longer an issue and companies can still profit from the usual AEOS functionalities, such as intrusion detection or video detection, or the possibility to restrict access authorizations. People flows can be controlled accurately and security risks are reduced significantly.





Graphical Alarm Handler

AEOS Graphical Alarm Handler step-by-step to a safe and secured building

Security and guard duties are often outsourced, which can lead to frequent changes in security personnel and guards. Clear alarm handling and work instructions are crucial to ensure consistent handling of alarms and registration of this process, every step of the way. Using the AEOS Alarm Handler enables security managers to enforce uniform alarm handling and to check handling of the alarms during and afterwards.

The fully web based AEOS Graphical Alarm Handler provides a clear overview of the maps of your building, additionally with live video images. In a glimpse the security manager has all the important information at his disposal: status of the doors, armed intrusion points, alarm points etc. Commands can be given directly from the Alarm Handler, for example to open a door or to activate the intercom.

The freely definable alarms allow users to set their own definitions on which events an alarm should be gener-

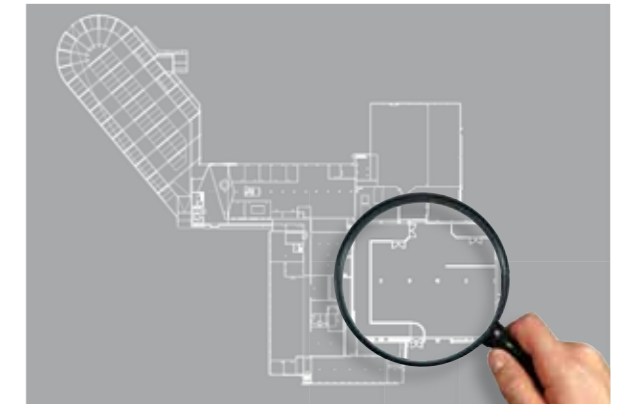
ated. Users generally want burglary attempts to trigger an alarm, but others will consider the presentation of an invalid access badge sufficient to generate an alarm.

The AEOS Graphical Alarm Handler prevents security managers from having to compromise on security: alarms can not be missed or lost; each alarm requires an appropriate action.

This tutorial shows the possibilities of the AEOS Graphical Alarm Handler in brief.



1. Enforce and enhance your security policy for your buildings with the AEOS Graphical Alarm Handler.



2. Analyze the maps of your buildings to determine which alarm points you want to display in the alarm handler. No need to redefine or reconfigure the access points and intrusion points since the alarm handler is fully integrated in AEOS.



3. In the AEOS Graphical Alarm Handler the icons and sounds for the alarms in your maps are freely definable. Drag & Drop the alarm points with the accompanying icons to the correct positions in your map.



4. Determine if you want to add additional information to the maps in your alarm handler, e.g. video images. The status of all the alarm points can be monitored in the alarm handler and commands can be given to open a door or activate an intercom, for instance.



5. If there is an alarm in your building, it appears on the map. Each alarm must be responded to, must be confirmed and assigned to a particular guard. Each of the steps in this protocol is fully logged, allowing system users and their supervisors to keep track of who responded and how quickly etc.



6. Straight forward, unambiguous handling of alarm procedures.

Nedap AEOS and Hitachi Finger Vein

Nedap and Hitachi have worked together to integrate finger vein verification into the Nedap access control system AEOS.

Finger vein recognition is a relatively new biometric technology. Each individual's vein pattern is unique and thus provides an excellent biometric identifier. Finger vein recognition works by shining infrared light through the finger. The infrared light is absorbed by the haemoglobin of the blood in the veins. This results in an image of the unique vein pattern.

The integration of finger vein biometrics in AEOS provides great advantages compared to other biometric technologies.

Since the veins are located inside the body, invisible to the eye and not accessible, they are extremely

difficult to forge and impossible to manipulate. By using light transmission instead of light reflection, it doesn't matter what the condition of the skin surface is.

The full integration in AEOS means that no other system or database is connected and all the features like communication, enrollment, verification and storage of the biometric data are handled in the secure AEOS environment. The finger vein reader can be used in combination with all AEOS features such as event monitoring and real-time update of the authorisations.

Finger vein biometrics in AEOS offers a fast, convenient, and non-invasive method of authentication, while maintaining consumer privacy.



HITACHI
Inspire the Next

New: the Invexs series

With the Invexs series, Nedap introduces another stylish, functional and highly secure reader family.



The Invexs readers and antennas combine modern design with cutting edge functionality. Thanks to the smart dual reader technology Invexs readers and antennas can simultaneously read different credentials providing a smooth migration between different card technologies.

The modern and stylish look of the Invexs readers fits perfectly in today's office buildings. The keypad's high quality touch keys are software-controlled and light up when a badge is presented to the reader. The key pad makes the Invexs suitable for applications with PIN-code verification for instance. The Invexs has an integrated, 3-color LED that provides direct information, e.g. access granted or access denied. The Invexs reader will also be available with a display, providing information to the user and is suitable for multiple applications.

Technology wise, the Invexs readers incorporate dual reading technology. The Invexs readers can simultaneously read

Nedap, Mifare Classic and Mifare DESfire credentials. One of the many advantages of this functionality is that it enables smooth migration, e.g. from Mifare Classic to Mifare DES-Fire. The high AES security standards are supported when reading DESfire credentials. Also, all models are equipped with configurable interfaces: RS485 to connect to AEOS, Wiegand for integration with third party systems, and XS RF modulation for integration in existing Nedap WinXS systems.

There are several models within the Invexs series: an antenna and readers with or without touch keys. In the near future, the Invexs readers will also be available with a display. All the different models are available with a black or a white back panel. The antenna version of the Invexs must be connected to the reader AEPacks. The readers are capable of reading Nedap, Mifare Classic, Mifare DESFire or a combination of those technologies.

The Invexs readers and antennas provide a perfect solution for situations where it is desirable to combine modern design with both smart technology and high security.

International Security Management Institute (ISMI) starts September 1st, 2009

The International Security Management Institute (ISMI) is an initiative to create a safer environment and to optimize security processes through the exchange of knowledge between professionals in the business. The training institute wants to stimulate people to enhance their knowledge of security management.

ISMI The International Security Management Institute

Professionals will give trainings at different levels in the field of strategic and technical development, implementation and use of security systems. The first step will be to train people with Nedap's security management system AEOS. Trainings are available at basic, expert and master level for system users, (sales) consultants and installation/ implementation personnel. Trainings are particularly useful for partners that install these systems and for users that work with them on a daily basis.



The International Security Management Institute wants to become a leading institute in the field of security management, by offering a wide variety of trainings and workshops by and for professionals in the business. Trainings will be organized at one of the four locations

mentioned below. You can register directly at one of the local addresses:

ISMI the Netherlands

Mr. Rene Waenink
Parallelweg 2E
7141 DC GROENLO
T +31 (0)544 471 666
F +31 (0)544 464 255

ISMI Belgium

Mr. Felipe Luis Henriques
Kerkhofstraat 6 B10
1800 Vilvoorde
T +32 (0)22 530208
F +32 (0)22 533001

ISMI United Kingdom

Mr. John Patey
1 Hercules House Calleva Park
Aldermaston, Berkshire
T +44 (0)118 982 1038
F +44 (0)118 982 1040

ISMI Germany

Mr. Bernd Majonek
Otto-Hahn-Strasse 3
40670 Meerbusch
T +49 (0)2159 8145-400
F +49 (0)2159 8145-410

Are you interested? Ask for the ISMI leaflet and pricelist through ilse.peters@nedap.com or take a look at our website www.nedap-securitymanagement.com.

Nedap AEOS

Global reach - Local service



Having implemented AEOS systems in over 55 countries around the world, the Nedap AEOS Partner community has a truly global reach.

The Nedap Certified Business Partner network has grown to over 65 partners worldwide, and when Project Partners are included this existing network can reach some 150 countries. Having Business Partners and Project Partners all over the world means that we are able to execute projects globally but also to provide local service: local

partners speak the customers' own language and can advise and support the customers locally without any cultural obstacles.

For an overview of the Nedap Certified Business Partners, please visit our website www.nedap-securitymanagement.com.

For the countries that are not listed in the figure above, please contact the Nedap Headquarters in the Netherlands.

nedap
aeos