

*--- arrowUp white paper ---*  
*Global Logical and Physical Access and Signing System*



***A multifunctional system that combines  
everything in one single card.***

## TABLE OF CONTENTS

Introduction	3
Security in Real Life	5
One Card, Many Applications	9
PayPoint	11
Shortcomings of Existing Systems	12
About arrowUp and its Partners	14
Glossary of Terms	17
Contact Information	20

## INTRODUCTION

Wouldn't it be great to be able to use a single card to get into your building, to pay at your company cafeteria, or at the vending machine? And to log on to your company network using the same card and access all the applications you need, without having to enter a user name and password every time? To be able to use the same card to digitally sign documents? Undoubtedly, the answer is a resounding "Yes!". And yet... By the end of 2009, virtually every Belgian over the age of twelve will carry an electronic ID card. The market is gradually sprouting applications – i.e., everyday benefits – for this e-ID. Of course, this is not the only card in the average Belgian's wallet.

Students at universities and academies use one card to copy valuable documents at the library, probably another to buy a sandwich at the cafeteria, and they certainly use a student card to obtain discounts at places like cultural centers.

Hospital staff uses one card to gain access to certain zones in their building, another to pay at the coffee machine, while doctors use yet another card to digitally sign certain documents or to log onto the computer network, so as to gain access to the applications and data for which they have clearance.

Anyone who works for a large corporation probably has a card for the underground parking garage, perhaps one to use as a time card, one for opening doors, one for getting gasoline, and one for computer access. No shortage of cards, therefore. Practical? No.

All too often, we see situations where every application requires a different card. Not only is this an expensive proposition for organizations; it is also difficult to track and manage. Obviously, users are not well served by having a whole series of cards in their wallets.

Is it that far-fetched then, to cover different applications with one single card? A card that gives users access to a building, or a space inside that building? A card for registering their hours worked? A card that allows them to log onto the computer network once, without having to remember different user names and passwords for every application or document? A card that they can use to digitally sign documents, in compliance with all legal standards and regulations? A card that allows them to securely send confidential information via e-mail? A card that they can use to pay for beverages, snacks, and meals at vending machines or at the cafeteria?

**All of the above functions can be combined into one single card.** The Belgian company called arrowUp specializes in the development of *smart cards* and their management. It developed **GLOPASS**, a multifunctional system that allows many applications to be attached to one card: access control, logical access control or secure logins, time registration, password management and *single sign-on*, digital certificates for legal signatures, cashless payment, and many more. **GLOPASS** stands for **Global LOGical** and **Physical Access and Signing System**.

Incidentally, organizations that already have a card in use for a certain application, don't necessarily have to invest in a new card: arrowUp can use existing *smart cards* and systems and add additional applications. Furthermore, **GLOPASS** features a modular structure: e.g., a company might initially use the card for access control only, and later add the capability of using the same card to pay at the company cafeteria.

*This document starts by outlining a number of possible user scenarios for universities, academies, hospitals, and larger companies. Next, the various different uses for this smart card will be explored in more detail: access control, logins, digital certificates for applying electronic signatures and sending secured e-mails, and, finally, payments. Next, we will discuss what the underlying systems look like and what the dangers or shortcomings of existing systems are. Finally, some background is provided about arrowUp and the **GLOPASS** system, along with a glossary of some of the technical terms used.*

## Security in Real Life

### Universities and Academies:

#### Ready for the Electronic Student Card?

Virtually all universities and academies in our country are currently exploring the possibilities offered by a digital student card. This would offer numerous advantages. For example, it could be used for different functions: paying for prints, for meals at the student cafeteria, or for beverages and candy at the vending machines. Students load the card with cash, and can then use it to pay for smaller purchases. Loading the card can be a simple online process using a load button on the school's web site. Students can load or check their accounts from their dorms or from wherever they have Internet access.

The big plus is that the amount is not on the card itself, but on a central, secured server. In other words, if the card is lost or stolen, its owner is not out any money. Students can transfer the amount to a new card at any time. They can use the card to pay at vending machines, or at the cafeteria. They can also use it to make copies or to print documents via the network printers, eliminating the need for specific (wear-prone) magnetic cards. This would also save universities and academies the extra work and headaches associated with handling cash.

Schools can also use the card for access control. Libraries and laboratories contain many valuable items. Currently, there frequently is no control whatsoever over who enters and exits these facilities. Schools can solve this problem by only allowing access to those students who really need it. The doors will only open to those allowed access by the appropriate authorities. In addition, the system tracks which student enters and exits the premises and at exactly what times, giving the school continuous control.

*In 2006, arrowUp initiated a trial project at the University of Athens. The objective was to automate, simplify, and accelerate existing processes used by students and administrative staff every day. Students can use their cards to check out books at the library, to log into computer systems, and to pay for their photocopies, food, and beverages. Incidentally, the user interface and the language of the various applications adapt to the card's owner. For foreign students, for instance, the system will automatically switch from Greek to English.*

*arrowUp also installed a contactless access control system at the University of Athens, eliminating the need for students entering buildings to swipe their cards, which would be time-consuming, especially at peak times. With the contactless system, students would simply hold their cards close to the reader to get the doors to open. The system tracks the exact time of entry. The same process takes place when students leave the building. The project can be classified as a resounding success. Both the students and the university experienced the ease of use and the benefits of the smart card on a daily basis.*

### More than an Airtight System for Authentication and Identification in Hospitals

In hospitals, it is vital that access to sensitive information contained in patient files be limited to authorized personnel only, making a highly secure IT infrastructure absolutely essential. Medical personnel needs to log onto the computer network multiple times per day, using different user names and passwords depending on the application needed. Who is to say that these passwords and user names cannot be found written down in a note on the doctor's desk, or listed in a document on his/her computer? A *smart card* would offer a simple solution for secure logins: staff members insert their smart card into their PC's card reader, and after entry of their PIN code, are granted access to the applications and information for which they have clearance. An example: all personnel can check the hospital cafeteria's weekly menu via the intranet. Since this is not sensitive information, it can be accessed by everyone. It is an entirely different story when confidential information is involved, such as patient files. Needless to say, only physicians and their medical secretaries should have access to such sensitive information, which is stored on the central servers. Assigning specific access privileges to a personal smart card guarantees the security and protection of information.

In addition to the secure login possibilities (logical access control) described earlier, the same card may be used for physical access control as well. Here, too, the card owner's profile or position determines which doors or gates it will or will not open. While certain rooms will be accessible to many individuals, access to others will be limited. For instance, virtually all employees would normally have card access to the parking lot. The doors to the surgery department, on the other hand, will open for a cardiac surgeon, but not for unauthorized individuals.

But there is more. Physicians can use the same card to digitally sign e-mails and documents. Thanks to a digital certificate supplied by an independent third party, this electronic signature has the same legal validity as a signature on paper. Digital signatures not only save time, they also reduce paperwork and the administrative workload in general. Incidentally, hospital staff can use the same card to send confidential information via e-mail in a guaranteed secure manner.

Finally, the hospital may also use the smart card as a payment card at the cafeteria or the vending machines.



## **Ghent University Hospital: Pioneering the Use of Smart Cards**

Ghent University Hospital will soon introduce a new badge for its personnel, confirming that the need for a multifunctional card is more topical than ever. "Our old magnetic strip badge had only one function: physical access control", says Bart Sijnave, IT Manager at Ghent University Hospital. "It provided access to the parking lot and to certain rooms. That was it. Our new contactless badge with MiFare technology contains a chip that is more flexible. All of our associates will get one before the end of this year."

In addition to access control, associates of Ghent University Hospital will be able to use the new badge at the cafeteria to pay for their meals. The card can be loaded at kiosks located around the cafeteria. Since the actual money is on a central system and not on the card itself, you are not out any money if you lose your card. In the future, associates will be able to use the new badge to pay at the beverage vending machine as well.

Another application that Ghent University Hospital will assign to the new badge is the registration of working hours. Bart Sijnave: "Especially nurses and administrative workers must register at the start and the end of their shifts. For this, we used to use time cards and a time clock. The idea is to replace these items with the new badge. To register, they would simply hold their badges in front of a time clock with a reader. This system is currently being tested, and will be fully operational before the end of 2009."

### **E-ID Promising As Well**

Ghent University Hospital also has several applications for the e-ID. Patients can use it at unmanned kiosks to review their hospitalization costs, eliminating the need to stand in line at the cashier window. Soon, they will even be able to do this from home, thanks to a system designed jointly with the other members of the Gents Ziekenhuis Overleg (Ghent Hospital Consultation).

arrowUp developed an application for the e-ID that requires visitors or temporary workers entering Ghent University Hospital to register first. The system checks whether the individual is a return visitor, and what privileges he/she has. It can also print a visitor's badge. This eliminates the need for a paper visitors' log.

"We have noticed that some of our people prefer not to use their e-ID to sign professional documents. This is odd, because isn't a written signature at home the same signature you use at work? I myself definitely favor digitally signing documents using the e-ID. There is one issue, however: we sign so many documents here (such as prescriptions) that we can't use the e-ID. Currently, the maximum number of electronic signatures per day is five. If you do more, the card will crash after a year." Ghent University Hospital could consider enabling the placement of digital signatures with the new badge, a possible application for GLOPASS.

The future, says Bart Sijnave, is in NFC ("Near Field Communication"): "Virtually everybody nowadays has a cell phone, which they almost always have within reach. NFC enables you to use your cell phone to identify yourself, to open doors and computer applications, and to pay for items. That way, you don't even need a card or a badge." arrowUp couldn't agree more, and it already has applications involving NFC and cell phones, placing it one step ahead of the future.

### **Simpler Control for Large Companies**

Clearly, large companies could also benefit from one smart card that can be used for multiple applications. Besides access control, secure logins or use as a payment card at the company cafeteria, such a card has another interesting benefit: its ability to contain digital certificates. The use of digital signatures reduces administrative processing, especially at companies where legal signatures on documents are frequently needed, such as audit firms. Furthermore, digital signing of important documents requires relatively little modification of existing systems.

Companies could also stipulate how many color prints an associate can make per day, per week, or per month, or determine to which customer file print costs should be assigned, facilitating appropriate invoicing. To this end, the chip on the card communicates with the central systems, enabling the company to control its printing costs and prevent abuse.

The personal card can be connected to laptops as well. This can even be achieved contactlessly, via RFID. When the card is brought near the computer, RFID technology establishes the connection. This makes it possible to keep the exit doors from opening if someone tries to escape with someone else's laptop, without the associated RFID card.

## One Card, Many Applications

After the preceding outline of a number of concrete situations involving the use of *smart cards*, we will discuss the various applications offered by arrowUp in more detail. One single card that combines all functions is not science fiction; it exists today.

### Access Control

An organization may stipulate who can access (certain parts of) its building with his/her card. Doors and gates will or will not open, depending on the identity recognized by the system. Organizations that already have a physical access control system don't necessarily have to renovate it. arrowUp will work with them to make **GLOPASS** fit their situation.

### Logical Access Control or Secure Logins

Besides physical access to locations, the card may also be used for logical access control. Associates can use their cards to log in securely to the organization's computer network via the card reader that is standard equipment in most PCs. This process is absolutely secure. On the one hand, it involves passwords placed on the card's chip. On the other, the authentication is a dual process (*two factor authentication*): logging onto the network requires both the right card and the right PIN code. Which computer applications, folders, files, and documents can then be accessed depends on the individual user. The organization will assign privileges to certain profiles to use a computer in a certain way. *PC roaming* is another possibility. This allows a user who logs off one computer and logs onto another to simply resume the same session.

### Digital Certificates for Legal Signatures

The smart card supports the use of digital certificates. This guarantees computer users' safety when using their smart card to send confidential information via e-mail or leaving it at web sites, e.g., when entering credit card information. Some web sites insist on verifying the computer user's identity. This can be done via the smart card as well. A personal certificate guarantees that the user is who he/she claims to be. This allows him/her to digitally sign documents, in compliance with all legal standards and regulations.

### Cashless Payment

To eliminate the need for cash, while ensuring that the user always has change for smaller purchases, arrowUp can equip the card with a so-called *private purse*. Based on smart card technology, this closed payment system is accessed via the card. With this system, users no longer need to have change on them when they feel like having a soft drink, a cup of coffee, or a snack from the vending machine, when paying for their lunch at the company cafeteria, or for printing or copies.

The big plus is that the amount is not on the card itself, but on a central, secured server. This means that if the card is lost or stolen, its owner is not out any money. After all, the user needs to know the PIN code to be able to use the card. Users applying for a new card can transfer the amount of their old card to the new one.

The card can be loaded in two ways, the first being online. All the user needs is a computer and an Internet connection, wherever he/she is.

Generally, the user will go to the organization's web site, where arrowUp installed a button on one of the pages. The user inserts the card into the reader, enters the PIN code, clicks the button and loads the desired amount. A second option is to use the PayPoint, a unique payment terminal developed by arrowUp. Besides its use for loading the *smart card*, the system is also an interactive information kiosk, complete with a 17-inch color screen. It is compatible with both personalized smart cards and with Bancontact, Maestro and MasterCard and Visa cards.

### Other Possibilities

The above are just the most common options. Virtually every imaginable situation in which a certain card is currently used can be integrated with **GLOPASS**. Examples include:

#### Password management and *single sign-on*

Users no longer need to remember different passwords for different applications on their computer: after logging in once with the card and the PIN code, they can access all applications and information for which they have clearance. Likewise, individual documents containing sensitive information no longer need to be password-protected. For instance, the system can be set up so as to allow only HR and management access to salary information via their cards.

#### Time registration

Companies using a payroll administration application can have their employees use the smart card to clock in and out. This eliminates the need for a separate time card: the time registration is triggered by the same card used to open the doors. Forgetting to clock in is a thing of the past as well: anyone who enters or leaves is registered automatically when the door opens or closes.

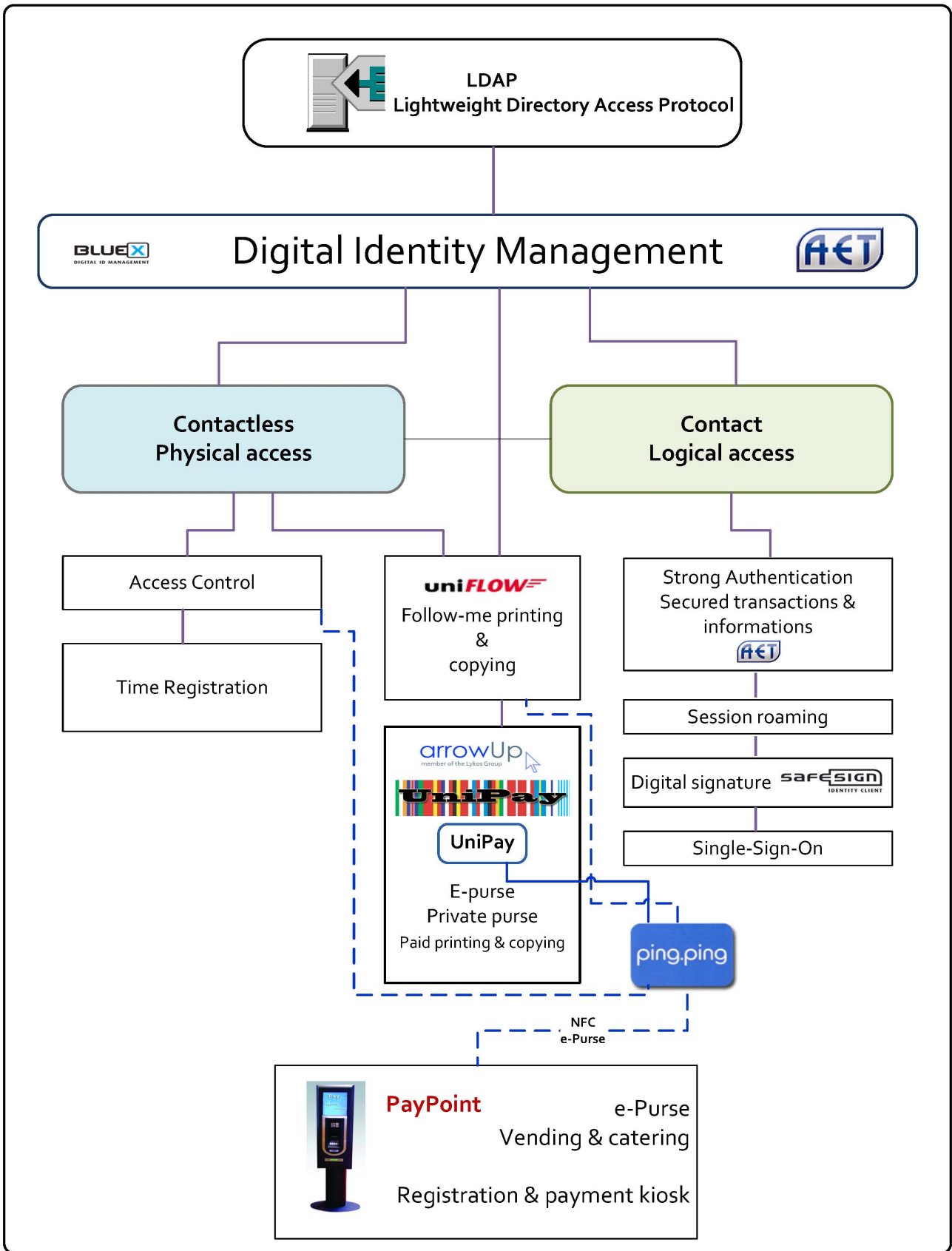
#### Gasoline card

Using your smart card at a gas station with which your company has an arrangement? It can be done. For this application, arrowUp suggests using a smart card with a magnetic strip.

The company makes arrangements with one or more groups of gas stations, enabling associates to get gas there without an extra gasoline card.

#### Access to health clubs, etc.

Companies that offer their employees a benefit like working out at a health club during their lunch break or after work, may enter into an arrangement with such an establishment. This would enable these employees to use their smart cards to access the health club, pool, or other sports facility; no membership card, badge, or pass is needed.



## Shortcomings of Existing Systems

### **An employee leaves the company**

Existing systems using access codes to enter a building offer the advantage of not needing a card to enter. A downside, however, is the fact that a code can easily be shared with others, who have no business entering the building. So what if employees leave the organization? Do you have to assign a new code to the system every time? Using a card is much simpler and safer: only those who have both a card AND the correct PIN code can enter the building. Employees who leave the organization, must submit their cards, meaning they no longer have access, either to the building or to the computer network. This eliminates the need to change codes.

### **A student loses his new copy card**

Currently, students who lose the magnetic card they use for making copies lose whatever amount was left on that card. Furthermore, such magnetic cards are very wear-prone. And what if they need a new card, but the office that sells

them [http://www.booking.com/hotel/fr/kyriadroissy.html?aid=302914;label=Bookings-Keyword-nl-n\\*Y73O2ilg35BwxUsM5RwwS779295565;sid=797e720c778d8062ac3f6aaef4c95c02;checkin=2009-11-16;checkout=2009-11-19](http://www.booking.com/hotel/fr/kyriadroissy.html?aid=302914;label=Bookings-Keyword-nl-n*Y73O2ilg35BwxUsM5RwwS779295565;sid=797e720c778d8062ac3f6aaef4c95c02;checkin=2009-11-16;checkout=2009-11-19) is already closed?

Adding copying to the digital student card's features enhances students' independence. Once they have used up the amount on their card, they can simply re-load it. If the card is lost or stolen, they are not out their money, because that is kept on a server. Without the associated PIN code, the card is of little use to its new owner.

### **An employee takes a break**

Frequently, confidential information is left on the computer screen. This is quite common: we log in securely in order to access confidential information in a computer application. A moment later, we take a break, leaving our work station. The result? Anyone can simply read the sensitive information. Attaching many applications to one card eliminates such situations: the person getting up from the work station will bring his/her card to open the door, or to get a soft drink from the vending machine. By removing the card, he/she automatically logs off.

### **Insufficient balance on the Proton card**

You are at the company cafeteria, and the balance on your Proton card is insufficient. Anyone who occasionally uses the Proton card, has been there: you want to pay, but your card does not contain enough money. Currently, a quick trip to a bank branch is your only option – if there even is one nearby. If your smart card balance is too low, you can quickly re-load it via a PayPoint kiosk or by logging into your organization's web site.

### **Evacuations**

There is an emergency on campus, and for evacuation purposes, authorities need a quick list of all those present. It is a "no-brainer": without smart cards, it is impossible to know exactly who is present in a particular building. You couldn't even guess. However, anyone who used a smart card to enter or leave a building is registered. The system can generate an attendance list in a matter of seconds.

### Cost of many cards

Universities use separate cards for different applications. A card quickly costs € 2. Add any additional cards students use to access the library or for printing and copying, and the university's cost quickly adds up. Using one card for all applications allows for a 50 to 65% cost savings.

## About arrowUp

Founded in Belgium in 2002, arrowUp specializes in smart cards and is a trailblazer in the area of electronic personal identification and security. arrowUp has 16 employees. The company's 2007 revenue totaled € 1.2 million. arrowUp's customers include AXA Bank, Delhaize, Fedict, Belgium's National Register, and TeleTicketService.

TeleTicketService hired arrowUp to develop software for the online sale of tickets to concerts and soccer games. Since 2003, music lovers and soccer fans have used this system to purchase millions of tickets. arrowUp has also accumulated considerable expertise in the areas of the SIS card and the Belgian electronic ID card (e-ID). In addition, arrowUp specializes in hardware and software for bank and customer loyalty cards. The company installed the Delhaize Plus hardware and customer loyalty software (Delhaize, Q8, FRS), integrating both seamlessly into the client's existing IT systems.

In November, 2006, the Greek company Lykos Paperless Solutions (LPS) acquired a participation in arrowUp. Lykos, a Greek family business that is over a hundred years old, specializes in printing and in managing and processing print data. Its products include company and vehicle documents, lottery forms, and bank and customer loyalty cards. The group also supplies secured paper for bank checks, bonds, stock certificates and tax stamps. Its other activities include the development of software for data management and processing and printing. The participation provided arrowUp with the financial resources to realize its growth plans, while Lykos augmented its expertise in the area of smart cards and customer loyalty programs. Thanks to this new knowledge, it was able to help modernize the Greek government via a number of IT projects.

## Partners

### AET

Since its inception in 1998, Dutch software company A.E.T. Europe B.V. (AET) has been supplying digital management systems and PKI technology-based applications for e-commerce and information security. In this context, AET develops cryptographic middleware and card management systems. AET is arrowUp's partner in the development of the eID SafeSign Identity Client, a middleware application that allows authentication based on the Belgian e-ID. Since AET's applications are based on globally recognized standards, they are easy to install in any IT environment and add to customers' existing systems. One of AET's applications, BlueX Digital ID Management, combines logical and physical access control. BlueX facilitates the installation, configuration and production of smart cards and USB tokens with digital certificates. AET not only supplies products, but can also handle their maintenance, in addition to providing client training.

#### Atos Worldline

arrowUp's Software Development Kit allows proprietary payment applications to be added to fixed payment terminals like those by Banksys, an Atos Worldline brand. Due to the contacts and know-how arrowUp has accumulated in this area over several years, it is one of the few Belgian players to have been declared a certified partner of Atos Worldline. This allows arrowUp to develop a unique closed payment system within an organization, enabling associates to use their smart cards for making payments and to re-load them as needed.

#### eID Company

The eID Company offers solutions in the field of electronic identification, electronic signatures and the collection and verification of personal data. These solutions are used both for online (Web, intranet, extranet) as for local applications. Identification, Authentication and Signing are at the forefront of our applications.

Our products allow you to:

Legally sign contracts and other documents electronically

Verify personal and related data (eg.: family status, revenue related debts,...)

Have forms filled automatically

The authentication and electronic signature that we offer have the same legal value as the written version.

They facilitate and reinforce adherence to the law, check-ups such as audits, and traceability within electronic processes.

#### PINGPING: Pay by mobile phone

There's a good chance that you own a device that you can use as a mobile phone, send text messages with and even surf on the Internet.

Would not it be convenient if you could also use this device to make payments? PingPing is now offering a mobile payment system for small amounts up to 25 euro using NFC (Near Field Communication) or a simple text message. PingPing's rapid micro payment gives us the possibility to pay with our mobile device at campus restaurants and hospitals, at vending machines, in car parks and shops and even on the Internet.

PingPing is open to all mobile customers, regardless of their operator.

Besides payments it also enables mobile applications to report malfunctions or other information. The system thus contributes to the overall operational quality of a company.

Within the Glopas application, PingPing can be used as a token for physical access.

#### NTware

In order to interface its smart cards with printers and copiers, arrowUp is working together closely with NTware, which has developed special software for that purpose.

Uniflow Output Manager allows organizations to track what has been printed or copied, by whom, and at what price, enabling them to increase productivity, lower costs, and optimize work processes. For instance, it allows them to control their color copying costs or to allocate them to individual departments, users, or customers.

NTware's R&D team works very closely with customers to ensure thorough understanding of their specific needs and to enable adjustment of its application in response to new questions or developments. Based on an advanced technology platform, Uniflow Output Manager features a modular structure. Consequently, it can be adjusted to an organization's specific processes, allowing it to work as well as its network printers. This makes Uniflow Output Manager ideal for organizations as diverse as large companies, small/mid-sized businesses, universities, and copy shops. Thanks to its Internet architecture, the software can run at multiple locations, while all information is saved in one database. In addition, the integration with other systems is relatively simple.

#### Suppliers of Access Control Systems

Companies specializing in physical access control applications until now are strategic partners for arrowUp. Thanks to **GLOPASS**, they can now expand their service offerings by offering their customers logical access control (secure login) systems as well.

## Glossary of Terms

### Authentication

In practice, a distinction is made between "weak" and "strong" authentication. Weak authentication is the verification of someone's identity by means of, e.g., a password. Strong authentication is identity check via a combination of something in one's possession (the physical aspect), such as a card, and something one knows (the logical aspect), such as a password or a PIN code. Access is not granted until both the physical and logical aspects have been satisfied. Smart cards are one tool for strong authentication. User characteristics can be stored in a smart card, so as to facilitate the login process for the user.

### CA - Certificate Authority

A certificate authority (CA) is an organization that issues and manages security certificates. These certificates are used for the verification of authorizations and identities when performing electronic transactions. A CA is the supplier, administrator and protector of official digital signatures.

### Digital certificate

A digital certificate is a computer file that acts as a digital identity card for its owner. A digital certificate is used within the Public Key Infrastructure (PKI) and is issued and managed by a CA. Such certificates guarantee a high level of security for information sent via the Internet. Applications for certificates include electronic signatures, protection of web sites, and remote authentication or encryption of messages. If a certificate is no longer to be used (e.g., in case of loss or theft), the owner should notify the issuer. The certificate authority maintains a type of black list of certificates that are no longer to be trusted.

### Digital signature

A digital signature provides assurance about the sender or signer of an electronic message. It is added to an e-mail or electronic document as an attachment. Generally, a digital signature consists of two *algorithms*: one to confirm that the information has not been changed by third parties, and one to confirm the identity of the person signing the information. The combination of these two algorithms' results constitutes the digital signature. These techniques are applied via a Public Key Infrastructure (PKI).

### e-ID

The e-ID is the official Belgian electronic identity card. It contains a chip, allowing the card to work like a key: provided he also has the associated PIN code, the holder can use the card to log into different applications. In addition to the information printed on the card (name, gender, date and place of birth, nationality), the microchip contains additional information as well, such as the owner's address and digital certificates. These certificates confirm the owner's identity when the e-ID is inserted into a card reader. In this manner, it can be used as proof of identity via the Internet or to place an electronic signature. By the end of 2009, every Belgian citizen over the age of twelve will carry an e-ID, making Belgium a trendsetter compared to the rest of the world.

### Identity management

Identity management can be used to assign privileges to users of IT systems. This allows an organization to reliably give its users access to networks, applications, servers, or information. Identity management covers such items as *password*

*management*, authentication and *single sign-on*. Therefore, it is not just user management, but access management as well. It links mandates together and determines which privileges a user has.

### Login

Inside organizations, access to computer applications and electronic information is often protected. Access to the computer system is not granted until after the user logs in. The simplest way of logging in is by entering a user name and a password, although that is not the most comfortable (or the safest) method. A better way to secure access is through the use of certificates. One way to achieve this is via a smart card. The login software verifies the certificate's validity. If the certificate has expired, a warning appears, and logging in is no longer possible. A smart card is very convenient: when temporarily leaving the computer, e.g., to get a cup of coffee, simply take the smart card with you. That way, you can be assured that nobody can use your information during your absence.

### NFC

*Near Field Communication* is a technology for wireless communication between equipment over short distances (approx. 4 inches). The exchange and storage of information are possible as long as devices are kept close to each other. This technology is especially popular in cell phones, but can also be used as a ticketing system or for making payments, e.g. paying for a bus ticket with your cell phone. One important characteristic of NFC is that the information exchange doesn't start until after a device has identified itself to another device. NFC is viewed by some as a smart form of RFID (see below). NFC communication is bidirectional and can process signals received. RFID storage and transmission of information is unidirectional.

### PIN code

A PIN or Personal Identification Number is a four-digit security code that provides protection against unauthorized use. You can use this secret code to activate the chip on your card. The best-known applications are the use of payment cards at ATMs and payment terminals and turning on a cell phone.

### Private purse

A rechargeable electronic "wallet" for internal use (e.g., in the form of a smart card) intended to speed up and streamline payment for small purchases.

### PUK code

PUK stands for *Personal Unblocking Key*. After multiple entries of a wrong PIN code, the chip in the card is blocked. The PUK code is an eight-digit code that can be used to unblock the card.

### RFID

*Radio Frequency Identification* is a technology that can be used to remotely identify an object, track its progress and know its characteristics. This is accomplished via a so-called *RFID tag* that is placed on or inside the object and communicates via radio waves. RFID has a host of different uses, including identification of animals, access control, theft prevention in retail stores, tracking foods in the distribution chain, keeping track of library books, and many more. A smart form of RFID is *Near Field Communication* (NFC).

### **Single sign-on**

With single sign-on (often abbreviated as "SSO"), access to multiple different IT applications requires only one login. This login could be in the form of a combination of a smart card and a PIN code, or a user name and a password.

### **Smart card**

A smart card is a chip card the size of a credit card. In a smart card, the chip not only has a memory, but a microprocessor as well, that powers communication and calculation functions inside the card itself.

A smart card is personalized, and is usually secured by a PIN code. Belgium's new electronic identity card is one application of smart card technology. Some smart cards feature RFID or NFC as well.

### **VPN**

A Virtual Private Network (VPN) arranges access to the company network or server from outside the organization. To accomplish this, VPN uses an existing network (usually a fast Internet connection). A VPN connection is often used by people working at home or elsewhere outside the office.

## Contact Information

*For more information about arrowUp's products and services, please use the contact information listed below. arrowUp welcomes your questions and feedback.*

arrowUp nv  
Bijenstraat 12  
9051 Ghent (Sint-Denijs-Westrem), Belgium  
E-mail: [sales@arrowup.be](mailto:sales@arrowup.be)  
Tel.: +32 (0)9 382 00 82  
Fax: +32 (0)9 245 95 54  
[www.arrowup.be](http://www.arrowup.be)