L-SEC

LEUVEN SECURITY EXCELLENCE CONSORTIUM

Interface

JULY 2004

The L-SEC Security Magazine

4

Content:

page

■ 1_Preface 3

■ 2_Business

New on the Block 4

New L-SEC member Amano – A Matter of time 5

New L-SEC member BioWise – Upbeat about Biometrics 8

More security doesn't make you more secure – better management does 10

■ 2'_Business Events

Security Talks L-SEC Annual Security Event, April 2004 12

L-SEC June event: The Belgian e-ID card and digital signatures, poised for take-off 14

■ 3_Technology

eID, a promising initiative ! 17

The power of the eID 19

■ 4_Focus On

User Provisioning with SPML 21

■ 5_News & Agenda

Upcoming events 25

Publisher:
Jurgen Truyen,
L-SEC, Kasteelpark Arenberg 10
B-3001 Leuven (Belgium)
Graphic design: Inpro, Waregem

I would like to invite you to read the 4th edition of L-SEC's Newsletter Interface before taking a well-deserved vacation. After 2.5 years, L-SEC is a healthy organization, which has been growing steadily. L-SEC has established a sound infrastructure for information dissemination and networking. The challenge for the next year is to intensify the collaboration and to reach out at an international level. I also would like to invite every L-SEC member to strengthen its involvement and to improve the dissemination of information of L-SEC within the organization. The more you do for L-SEC, the more L-SEC can do for you.

4

We are very pleased with the success of our e-ID workshop, on which you find a report in this newsletter. The electronic identity offers a unique opportunity for the L-SEC members to develop and deploy new applications and to market these outside Belgium. Currently about 60,000 new cards have been issued, and for about 85% of these cards the electronic functionality has been activated by the citizens. By 2009 every inhabitant of Belgium of 18 year or older will receive such a card, but specific target groups can request to receive an e-ID card sooner. This government investment can have a very positive effect on the widespread deployment and use of public key cryptography and contribute in this way to a more secure and trusted on-line environment. This is very important, since individual applications may not provide a business case for this technology, but a large set of applications can benefit from a coordinated approach. While the current e-ID project increases security and convenience, it also offers the possibility to build an infrastructure which also improves the on-line privacy for the citizens. Further research is required to realize this potential; L-SEC is taking initiatives in this direction.

Unfortunately, too much government intervention can also be undesirable.

A good example is the new law of May 7, 2004 which imposes on companies that offer security advice services to apply for a permit issued by the Minister of Internal Affairs. While we believe that the government should protect its citizens, such regulations are probably not helpful for several reasons. L-SEC will take up its responsibility in this matter.

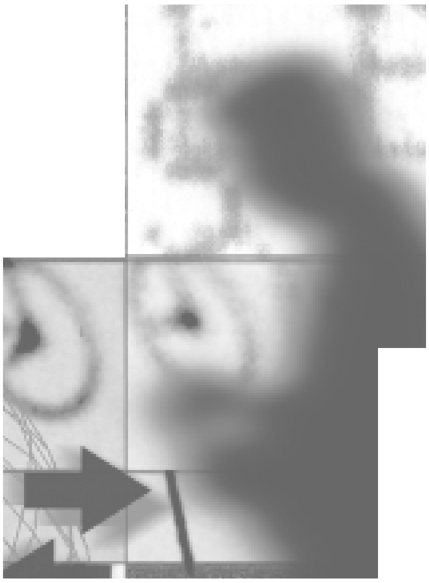
Bart Preneel, Chairman L-SEC

New on the block

L-SEC welcomes two new members

This spring, two new members joined L-SEC: Genk-based European branch of Amano Software Engineering (ASE), a Japanese company that provides trusted time services, and BioWise, a company that grew out of KeyWare's former biometrics team. Both companies are presented in this newsletter. But first of all, why did they join L-SEC? The point of view of Erik Cotman, Sales and Marketing Manager at ASE Europe, and of André Oeyen, Managing Director at BioWise:

➢ A.Oeyen- The field of biometrics is marked by a high degree of specialization. At the same time, biometrics is a relatively small domain. In order to position BioWise in the wide landscape of security technology providers, we decided to use the networking opportunities that L-SEC provides.



➢ E. Cotman- Same here: L-SEC provides opportunities for networking. Meeting people is a vital requirement for each business or branch, especially in its start-up phase. L-SEC is becoming an authority on internet security and, as such, we consider it a very efficient communication channel. The L-SEC events around digital signatures and e-IDs are important to us as well.

➢ A.Oeyen- Personally, I also think that Belgian companies tend to be too low-profile. Our companies can use the positive image and the strong message that a consortium like L-SEC can propagate, also on an international level.

➢ E. Cotman- Belgium, and the Leuven region, is in an excellent position as far as security technology expertise is concerned. This is the reason why Amano decided on Belgium for its European headquarters. Being were the action is, and making the most of that location, that is what it is about.

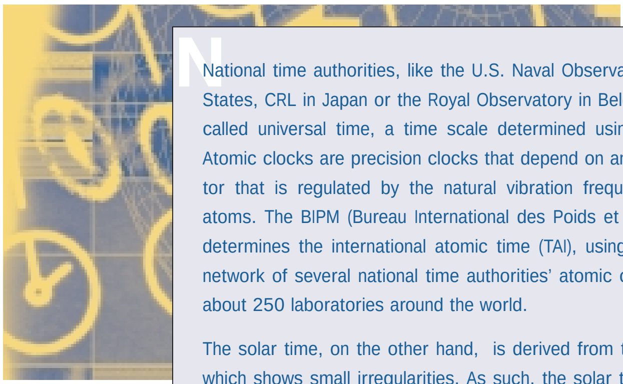
For more information on BioWise, visit
http://www.bio-wise.com
For more information on ASE Europe, visit
http://www.e-timing.net

A matter of time

An interview with Erik Cotman, Sales and Marketing Manager of the European branch of Amano Software Engineering (ASE), a new L-SEC member.

What's Amano's history?

Erik Cotman: Amano is a Japanese holding, founded in 1931. In Japan, Amano revolves around two axes: "timing" on the one hand, "ecology" on the other. Outside Japan, Amano only provides "timing" services. Timing refers to time registration and clocking systems, from the original mechanical systems to the current digital systems, and on related activities like parking systems and HR software. Amano is an established name in Japan. The company has had its European headquarters in Genk for more than 10 years now. Amano Software Engineering (ASE) is in its start-up phase as far as commercial activities in Europe are concerned. ASE Europe will focus on time stamping solutions, parking management systems, intelligent timing terminals and on related HR applications.



National time authorities, like the U.S. Naval Observatory in the United States, CRL in Japan or the Royal Observatory in Belgium keep the so-called universal time, a time scale determined using atomic clocks. Atomic clocks are precision clocks that depend on an electrical oscillator that is regulated by the natural vibration frequencies of cesium atoms. The BIPM (Bureau International des Poids et Mesures) in Paris determines the international atomic time (TAI), using the time from a network of several national time authorities' atomic clocks, situated in about 250 laboratories around the world.

The solar time, on the other hand, is derived from the earth rotation, which shows small irregularities. As such, the solar time is less stable than the atomic time.

In order to ensure agreement between atomic and solar time scales, the International Earth Rotation and Reference Systems Service (IERS) has decided to introduce so-called leap seconds. These are added as soon as the difference between atomic time and solar time becomes larger than 0.9 seconds. The resulting time is called the UTC (Universal Coordinated Time). This is the time distributed by standard radio stations. It can also be obtained from GPS satellites.

More information:
http://jjy.crl.go.jp/index_e.html,
http://www.astro.oma.be/D1/TIME/index.html,
http://www.bipm.fr/, http://www.npl.co.uk, http://www.usno.navy.mil/

About four years ago, Amano Japan extended its activities by introducing the concept of e-Timing. Can you tell us a bit more about this?

Erik Cotman: E-timing provides the entirely electronic alternative to the former mechanical clocking systems, used mainly for registering employee attendance. E-timing is based on the generation of time stamps. In order to generate these stamps, Amano has established its own Trusted Time Authority, located in a highly secured data centre, operating several atom clocks. Security is obviously extremely important here, as trust is a key factor. Amano has also developed the technology and mechanisms to carry out the actual time stamping. This involves timestamping the hash of a file, using the trusted time that has been provided by the trusted time authority. It can be compared to the digital signature procedure, in this case, however, the ID is replaced with the time stamp.

Amano's Trusted Time Authority compares information from several time authorities in order to derive the universal time. We work with the Japanese time authority CRL (Communication Research Laboratory). The time from a number of atom clocks is retrieved via common-view GPS, a technique for comparing times between clocks at two remote locations. The difference is logged regularly. Based on the mean of these deviations, the standard time is kept.

Do other companies do this as well ?

Erik Cotman: No. There are quite a few commercial time stamping authorities, but they do not establish their own trusted time. Usually, companies use the signals sent out by one of the national time authorities. Having one's own trusted time authority is quite costly, but Amano wants to be in charge of the entire time stamping process. Also, as national time authorities are not commercial organisations, they do not guarantee the uptime of their services. Amano offers services for synchronizing and monitoring customers' servers and PCs continuously, on the one hand ensuring that the servers and PCs use the correct time, on the other hand providing logs that prove that the time on these servers has at all times been synchronised. In order to provide services like these, Amano needs guaranteed availability of trusted time information. We do this by establishing our own trusted time in a secured data centre.

Is the Amano Trusted Time Authority also available for other parties?

Erik Cotman: Yes. However, we will not market that aspect intensively here, as our market research has shown that in Europe, there are more opportunities for the actual time stamping services. For most customers, time stamping will be the more efficient and financially interesting option. As I said, we started here last April. Before that, we have done market research into the possibilities of time stamping on the European market.

What are the advantages of time stamping in a business environment?

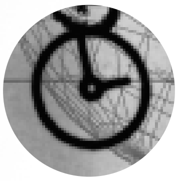
Erik Cotman: Timestamps are used all the time, in daily life as well as in business. Businesses use time stamps to set deadlines and terms, for example for offers. In most cases, the date is more important than the exact hour, but dates are obviously just references to larger units of time. We think time stamping will really take off once the legal background has been sufficiently defined. Digital signatures have now been officially recognised, and time stamps actually belong to the same structure. At the moment, though, they are less specifically defined, and the legal requirements are less explicit.

Time stamps provide ease of use. Our solution for PDF files just requires a mouse click to supply the file with trustworthy time information that can later be used to prove that the file has been generated at a certain moment, and that it has not been changed since then. Using time stamping can greatly reduce the procedural overhead for patent filing and enforcement of intellectual property rights, for instance.

There really are hundreds of possibilities, e-invoicing is just one of them.

But don't digital signatures suffice in most cases? Once a document has been digitally signed, it is legally binding...

Erik Cotman: That is correct, but only as long as the certificate used for the digital signature has not expired. To ensure lasting proof, the digitally signed document has to be time-stamped. This way, the validity of the certificate at the time of generation of the signature can be checked. Time-stamping is an important addition to the digital signature. Sometimes, it is a cheaper solution. Digital signatures require registration. For batch-processing, for instance, time-stamping is very interesting as it simplifies the signing process. For each business requirement, it is a question of establishing the return on effort, determining whether time stamping, digital signatures or a combination of both are the most beneficial.



interview

➢ *Which products does Amano offer in Europe ?*

Erik Cotman: We actually provide services rather than packaged products. Our time-stamping service can be used in three ways. First of all, we have developed a plug-in for Adobe Acrobat. The plug-in can be used for generating a hash of a document, sending it to the network via a patented solution. We use 2048-bit RSA encryption with two keys, which provides enhanced security. Secondly, our customers can opt for a Java class, providing the same functionality, but then without Acrobat. We also provide a DLL, a software development kit that can be used for time-stamping with any kind of application. In this case, the application itself generates the hash, and we provide the timestamp for the hashed file. This is useful for time-stamping of specific files, like video files and audio files or XML streams. As I said, our patented solution relies on 2048 RSA encryption, which involves two private/public key pairs. One public key is stored by Amano and only referenced to, the second PUK is stored in the license file. Every user of our services needs to have a license file, stored on his own system or server. This file contains the private key that is required for authentication prior to the use of our services. While the time stamps can be verified offline as well as online, creation of time stamps can only be completed online. In order to use our services, customers pay a subscription fee, including a number of pre-paid stamps. The use of the plug-in, the Java class and the DLLs is included in the subscription fee.

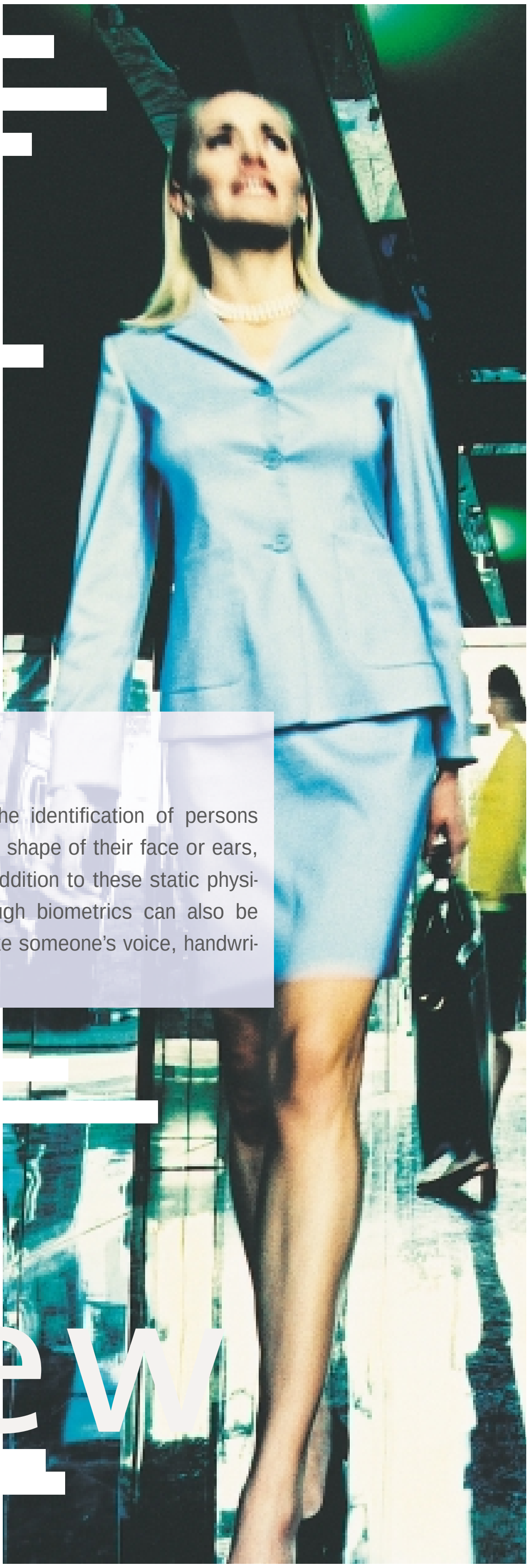
In Japan, the National printing bureau, a governmental organisation, has been using our application intensively for the past two years. Every legal document there is converted to PDF and time-stamped. Commercial companies in Japan like Cable & Wireless IDC inc, IHARA Corporation, use our products as well. The next step for us is Europe, with a first focus on the Benelux. That's exactly why we have chosen Genk as a location for our European headquarters.

An Schollen

The next step for us is Europe, with a first focus on the Benelux.

Upbeat about biometrics

An interview with André Oeyen, Managing Director of BioWise. BioWise joined L-SEC last spring.



➢ *Can you tell us a bit about the history of BioWise ?*

André Oeyen: BioWise was founded in April 2003, as an initiative of the former biometrics team of Keyware Technologies. We all learned the ropes at Keyware. Though the technological principles we used there obviously still apply, BioWise's overall approach is new. A few years ago, most businesses were working towards long-term objectives, set against the backdrop of an expanding global market and a booming economy. From the onset, BioWise realised that the customer pool is not unlimited and that the only way to grow is by responding to actual market needs. With our relatively small team of highly-experienced experts, we want to provide middleware for a defined market segment. In the past year, BioWise has collected several customer cases, including the s-Travel project, using biometrics in international travellers' identity verification.

➢ *How would you define biometrics ?*

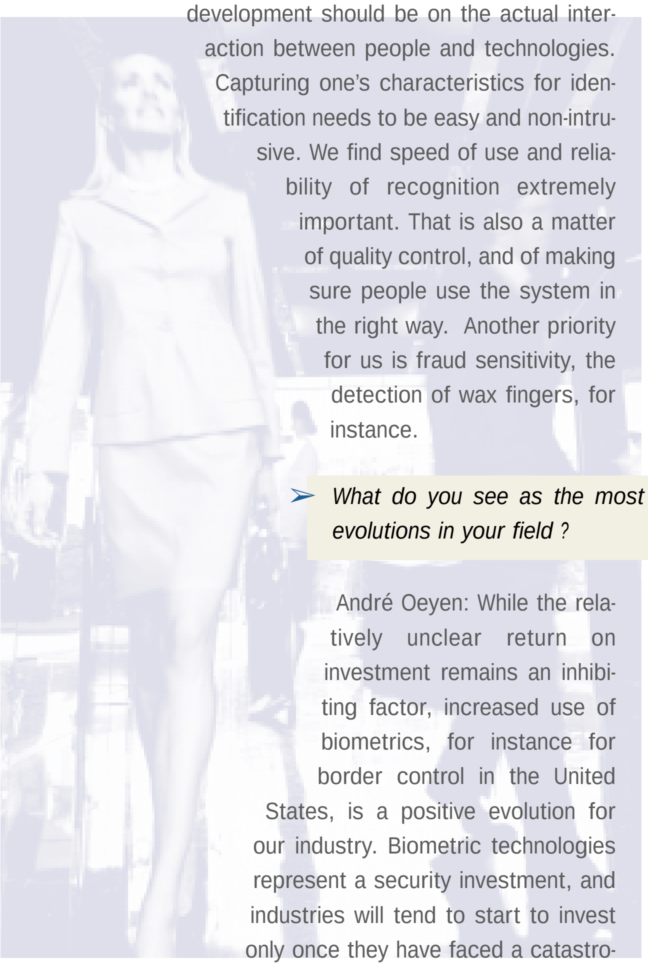
André Oeyen: Biometrics, put simply, is the identification of persons based on their body characteristics, like the shape of their face or ears, the colour of their iris, their fingerprint. In addition to these static physiological characteristics, identification through biometrics can also be based on dynamic aspects, or behaviour, like someone's voice, handwriting, or way of typing on a keyboard.

➢ *Biometrics is often defined as a very capital-intensive business. Is that your perception too ?*

André Oeyen: In general, it is true that developing biometrics technology is not cheap. First of all, there is obviously a lot of research involved before a product goes on the shelves. Secondly, making the case for biometrics means incurring extensive marketing costs, and this in a relatively small market.

➢ Are biometrics technologies mature enough to compete with other systems, like digital signatures, which can be considered more straightforward and established ?

André Oeyen: Biometrics technologies are certainly trustworthy for a whole lot of applications today. I think the main focus of development should be on the actual interaction between people and technologies. Capturing one's characteristics for identification needs to be easy and non-intrusive. We find speed of use and reliability of recognition extremely important. That is also a matter of quality control, and of making sure people use the system in the right way. Another priority for us is fraud sensitivity, the detection of wax fingers, for instance.



➢ What do you see as the most important evolutions in your field ?

André Oeyen: While the relatively unclear return on investment remains an inhibiting factor, increased use of biometrics, for instance for border control in the United States, is a positive evolution for our industry. Biometric technologies represent a security investment, and industries will tend to start to invest only once they have faced a catastrophe. But in general, the combination of enhancing quality of the technology with decreasing prices makes the outlook for biometrics very promising.

➢ So biometrics are on the upbeat ?

André Oeyen: Absolutely. One positive factor is that we now have a realistic view on what the market is waiting for, which allows us to develop affordable biometric applications that can be used on a large scale in production systems.

When you allow your fingerprint to be captured once, it can be stored and used for a lifetime and impact you in later life. People may find this a frightening prospect. How about the privacy-aspect involved in Biometrics ?

André Oeyen: This has been taken into account in the so-called proportionality principle, outlined by the EU Advisory Body on Data Protection and Privacy. The use of biometric information has to be justified in view of the goals one wants to attain. To safeguard privacy, biometric data can be stored in encrypted form, or they can be stored solely by the individual they identify, for instance on a smart card. Even the actual verification can be carried out on the card itself, so the biometrical identification data do not have to be stored or processed on external systems. As far as storage in databases is concerned, BioWise is devising a set-up that makes it physically impossible to immediately link biometrical data to the names or identity of persons. These aspects are at least as important for the growth of biometrics as the technology itself. Biometrics still suffers from a negative public perception.

➢ Today, biometrics is used mainly for border control, large-scale public services and in highly secured sectors. When will all industries start applying biometrics on a large scale ?

André Oeyen: The most common use of biometrics today is in access control, for instance for employees (75 percent of the uses of biometrics are in the field of access control). Another possible wide-scale use is visitor control, in situations were private companies frequently have to deal with large numbers of previously unknown visitors. Airlines, for instance, like to know exactly who is on their flights. In the Netherlands, some night clubs use smart cards with biometrical data for access control. Stealing the smart card is no use, and whoever has been blocked from the visitor list can never get unauthorised access. In this case, visitor control is made more objective and acceptable and, as such, easier to enforce.

An Schollen

More security doesn't make you more secure – better management does.

More than ever, security is the order of the day in the IT world. That's why Computer Associates now positions itself with its eTrust products and services as a fully-fledged security partner. Ardatis didn't fail to notice this, and acted accordingly.

Heverlee-based Ardatis responds to the security challenge with consultancy, package implementations and tailored projects to meet the IT needs of government organizations (ministries and government institutions) as well as the private sector. At the same time Ardatis is also an outsourcing partner for many of its customers. The company takes care of the maintenance and management of applications and infrastructure. Obviously security is becoming an increasingly important part of this. "That's why, when we talk security, we work in two well-defined areas," says Hedwig Vergeylen, COO of Ardatis. "On the one hand, we have to take care of the security of our own infrastructure, on the other hand we formulate recommendations about security for our clients." Ardatis has managed its own infrastructure with Unicenter for quite a while now. Recently the company took a long, hard look at the eTrust range. It reflects on the added value that these products can offer.

"Sure, a company does need concrete security solutions," continues Hedwig Vergeylen. "But it is more important that we have a well-founded security policy, both logically – for example through software – and physically. For the latter we have a disaster recovery plan that we test twice a year. However, it's also very important that the company keeps adapting its security procedures to present needs. Our own security is also a criterion for our customers. We show them that we have the confidence to meet set Service Level Agreements (SLAs) without any problem.

Hedwig Vergeylen

Real added value

With eTrust, CA offers solutions for identity, access and threat management. With these solutions the customer can guarantee users a secure and efficient working environment, keep hackers and viruses out, organize network access in function of the staff members, … However, the real added value that CA offers with security is on a higher level. "Security applications generate logs," says Guy Duray, Business Technologist at CA. "These logs reflect what happens within the company: who logged in, on which systems, if any viruses were intercepted, … But there is a practical problem. In Europe alone there are more than six thousand security companies on the market and all of their logs look different." With Security Information Management (SIM) CA has a suite of solutions that transforms the information in these logs into concrete management actions.

Immediate view

"The core of our solution is eTrust Audit," explains Guy Duray. "This is a solution that brings together in a uniform and structured way the logs of different platforms, databases and applications. At the same time the manager can grade these logs according to the threats that are posed. The result is that the company has an immediate view on a situation in which the security of both systems and information is at risk." To further increase the user-friendliness and efficiency of eTrust Audit, CA has built a portal - Security Command Center - around it. And with CA's 20/20 solution the company can extend the security management of the Security Command Center with measures that are not IT-related. "SIM really makes the difference with CA", adds Guy Duray. "The final goal is for the client not to have to look at dozens of screens anymore to check the security status of his company. You don't just increase the security of your company by installing additional applications, you have to manage it in the right way."

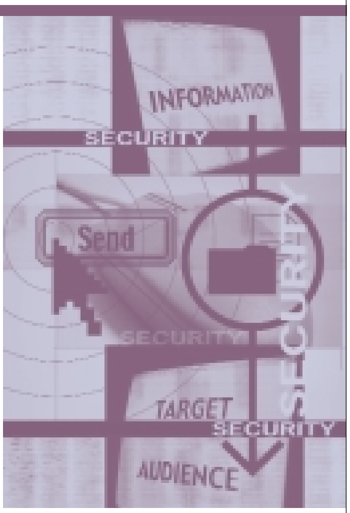
L-SEC, VBO, ICS and Belcliv

are organizing an information session about the new law on security advisors.

July 8th, 2004
16u00 - 17u30

Permit required for enterprises offering security advice

Since June 3, companies offering security advice services need to have a permit issued by the Minister of Internal Affairs. The new law (May 7, 2004) extends an existing law on surveillance, security and internal security firms, to also include enterprises offering security advice. The objective is to impose quality standards after audits by a certification body. Taking into account the transition measures, this means that companies offering security advice to third parties as their core business have to request a permit from the FOD Binnenlandse Zaken (Internal Affairs) by August 3, 2004 at the latest, in order to be able to continue their activities. This also applies to enterprises offering security advice on information technology.



Program

15u30	**Registration**
16u00	**Presentation of new law concerning security advisors** *Jan Cappelle, Directeur Private Veiligheid, Federale Overheidsdienst Binnenlandse Zaken*
16u45	**Questions & answers**
17u30	**End**

Place

Verbond van Belgische Ondernemingen,
Ravensteinstraat 4, 1000 Brussel
Routeplan

Date

Thursday July 8th 2004, 16u00 – 17u30

Registration

Free registration - Download Faxform Dutch or French

More Information for registration
Christine Taskin, T : 02 515 08 97 - F : 02 515 09 55 -
e-mail : ct@vbo-feb.be

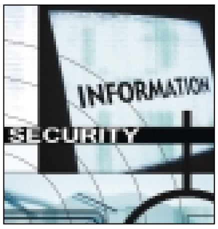
Security talks

L-SEC Annual Security Event, April 2004

Annual Security Event

L-Sec invited technology, service and product providers and professionals in the end user market to have their say on the most recent evolutions in IT security during the L-SEC Annual Security Event (April 22, 2004). attendants from various industries were informed about the latest trends and technologies.

During his opening speech, L-SEC Chairman Bart Preneel presented a list of technologies that are gaining a foothold. Public Key Infrastructure, intrusion detection and prevention, role mining, biometrics, ID management, secured software, protection against side channel and fault attacks, as well as Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) were on the "in" list. Topics like role mining, intrusion detection and prevention and ID management were elaborated on during the day. A recurring observation was that managing security means managing increasing complexity. Though terms like self-defending and self-configuring networks seem to suggest a reassuring autonomy of technologies, security is on the minds of more than just the IT managers today. Businesses rely heavily on ICT. Network downtimes, spam, worms and viruses have considerable business impact. Sophisticated fraud techniques call for technological solutions, for sound processes and for awareness on how to make the most of security. The more ICT-reliant businesses become, the more important ICT security will be rated by the board. 2004, according to Deloitte partner Chris Verdonck, is characterized by an increased interest in security. In addition, corporate governance and legislation impose stringent regulations. While security awareness has been raised and mature technologies are on the market, security officers face a plethora of challenges: balancing the required openness to facilitate growth with the necessary protection, meeting regulatory demands and facilitating business processes, with limited, sometimes even trimmed budgets.



The mid-day panel discussion revolved around the question "Security Certification – a need or a demand". Many product-specific certification programmes are organised by technology vendors. The number of vendor-neutral programmes is on the increase too. Some attendants at the event expressed their doubts as to the actual value of certifications on applicants' CVs. However, some replied, a well-known certificate gives credence to candidate's experience and commitment to security. As the annual security event has shown, managing security is becoming ever more complex. To include all the aspects related to information security in the curricula of information technology programs is not feasible. As a result, new graduates opting for a job in IT security as well as seasoned professionals may be daunted by new technological and practical challenges. Good certification programmes can meet their needs, and benefit their employers as well as their customers. Employees' certification shows that companies want to maximise knowledge in ICT security and actively invest in it. Two examples of sound certification programmes, referred to during the panel discussion, are CISSP Certification and CISM. Together with independent certification programs, university programs can contribute to the continuous distribution of security knowledge to novice and experienced IT professionals, and to the further development of professionalism. Both will contribute to the consumers' confidence, a key requirement in the competitive IT security industry.

Annual Security Event

"How well-secured are we today", is what one of the event's attendants asked, and "will it get worse before it gets better?" Though ICT departments are technology-wise probably better equipped than ever, and though security is a concern shared across the company, more vulnerabilities seem to be reported. But that is partly due to perception too, the experts answered. We are more reliant on ICT. Hence, breaches have a deeper impact and attract more attention. This may reduce the perceived value of today's security technologies. The net result though provides a more positive picture, with companies taking a more strategic approach to security, through security technology and practices that enhance overall business processes, through investments in user information and through a public discourse on topics like the privacy-security paradox.

The presentations at the L-SEC annual security event have shown how recent technological, societal and economic evolutions continuously re-shape the security landscape. Security threats hit faster and have a deeper impact, while businesses and end users rely ever more heavily on the wide variety of electronic devices that characterize business operations as well as daily life. Increased regulatory pressure has turned security into a shared management concern. User awareness, on all levels, is heightened and companies and vendors invest further in informing employees and users about potential risks and appropriate approaches. Network architectures take new shapes. Intrusion prevention complements intrusion detection. Paradoxes like the privacy-security issue and the false-positives/false-negatives dilemma urge companies to take a strategic approach, balancing profitability, consumer trust and security. As a result, security is increasingly hooked into business processes. Security has become pervasive, a relevant topic in all businesses and for all user types.

Two papers have been written on the topics presented during the L-SEC Annual Security Event. "Security talks - Strands of L-SEC April 2004 Annual Security Event" and "Security Certification – a need or a demand" are available for members in the members login section of the L-WEC website.

Speakers at the event were Georges Ataya, Chairman, Benelux ISACA Chapter, Luca Bertagnolio, Cisco Systems, Eddy Cormon, Director Strategic Partnerships, Vasco, Remi De Brandt, Beleidscel Staatssecretaris voor Informatisering van de Staat, Jan De Meester, CEO, Integri Professional Services, Dirk Dussart, Principal Advisor, PricewaterhouseCoopers, Detlef Eckert, Senior Director Trustworthy Computing Microsoft EMEA, Tim Groenwals, IT Security Manager, AGFA, David Naccache, Director Applied Research & Security, GEMPLUS, Professor Bart Preneel, Chairman L-SEC board, Carlo Schüpp, Executive Vice President, Ubizen, Marc Sel, Director, PricewaterhouseCoopers, Steven Van Hooste, Managing Consultant, Telindus, Chris Verdonck, Partner, Deloitte Enterprise Risk Services. Georges Ataya, Carlo Schüpp, Marc Sel, Chris Verdonck participated in the Security certification panel discussion.

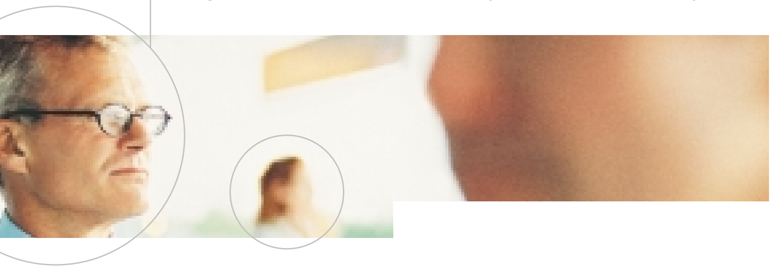
L-SEC June event: the Belgian e-ID card and digital signatures, poised for take-off

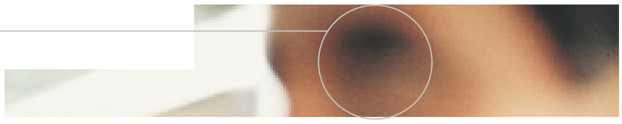
Belgium is one of the first European countries to provide electronic identity cards to its entire population. In a service-oriented environment, the introduction of the electronic ID can spur economic growth, as it facilitates and promotes e-services in the public and private sector. The data capture, authentication and signing functionalities of the eID card can provide great business advantages.

Last June 10, L-Sec organised an event focussing on the introduction of the electronic ID card in Belgium and Europe, and on the digital signatures that can be created with the card. 120 professionals from various industries and governmental institutions attended the event. The positive feedback sent in by the attendants reflected the ambience of the day. A mix of informative presentations providing a wide-angle view, informal networking opportunities for L-SEC members and participants and interesting demos by ASE Europe, Certipost, Intesi Group, K.U.Leuven, Novell, SecurIT, Telindus, Vasco and Zetes made the event yet another successful L-SEC initiative. A brief overview of the presentations:

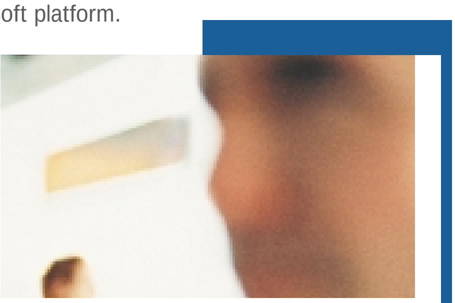
Bart Sijnave, Project Manager at Fedict opened the event with a presentation of the roll-out of the Belgian eID project. The decision to introduce the eID in Belgium was taken in July 2001 by the Federal Government. A pilot project in which over 50.000 electronic ID cards were distributed among the inhabitants of eleven Belgian municipalities was completed in the beginning of 2004. The gradual roll out of the eID in all Belgian municipalities is expected to start in the second half of 2004. Certipost is the supplier of the Belgian electronic ID card certificates. Zetes is responsible for the production, personalisation, activation and distribution of the card and for the overall project management. In July 2004, about one fifth of the Belgian population will have received an eID. By 2009, all Belgian citizens will own an eID.

Two presentations focused on the legal aspects related to the use of eIDs and digital signatures. Ubizen's Legal Practices Manager, Dr. Andreas Mitrakas, explored current identity management schemes in a European context. He showed that standardisation efforts of European standardisation bodies like CEN/ISSS and ETSI are essential for the international deployment of eIDs and digital signatures. Jos Dumortier, professor at the KU Leuven and co-founder and director of the Interdisciplinary Centre for Law and Information Technology (ICRI), explained the legislative framework for the use of the eID and described the use of qualified electronic signatures. According to the European 1999/93/EC directive, an advanced electronic signature is "an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable". Qualified electronic signatures are advanced electronic signatures that are based on a qualified certificate and created using a secure signature creation device. During his presentation, Mr Dumortier stressed that it is hardly possible to pre-determine the legal value of qualified electronic signatures created with Belgian e-ID cards. Electronic signatures will gain acceptance once the use of Belgian e-ID cards for signatures becomes a common practice.





Qualified electronic signatures were at the heart of the next speaker's presentation too. Ronny Bjones, Security Program Manager at Microsoft EMEA detailed the use of QuEST, the Qualified Electronic Signatures Tutorial that Microsoft developed in cooperation with European specialists in the field of qualified electronic signatures. QuEST is aimed at legal professionals, IT professionals and developers designing qualified electronic signature solutions. QuEST provides information on how to develop qualified electronic signature applications. It includes a knowledge base with blueprints covering all related aspects. A sample scenario shows how a QES solution can be implemented in practice on a Microsoft platform.



Erik R. van Zuuren, Senior Infosec Consultant at Ascure co-authored the BelPIC blueprint (Belgian Personal Identity Card). He played a central role in the PKI-enabling of the Flemish Government. In his presentation, Mr Van Zuuren described the Belgian government's route towards a variety of secure e-government applications, with increased information security, and safeguarded privacy. He described the user-friendly eID-applications that grew out of existing applications in legacy environments.

Sylvie Lacroix, Trust Solutions & PKI Projects Unit Manager at Certipost elaborated on the eID potential for expanding and securing e-services and for establishing identity management. In order to stimulate the adoption of the eID, Certipost provides an eID Starter Kit as well as an eID Development Kit that can help developers make their applications eID-compliant. The developer kit contains eID test cards with digital certificates, an eID-compliant smart card reader, access to certificate validation services, a set of tools, user manuals, software and code samples and one year membership to the eID Forum. On this forum, available via http://www.eid-forum.be, technical questions concerning eID are answered by Certipost eID technical experts. Starter and development kit are available via http://www.eid-shop.be.

Marc Sel, Director at PricewaterhouseCoopers introduced the presentation of Jesper Skagerberg, Product Manager at Nexus Technology AB. Mr Skagerberg advocated the use of attribute certificates. While public key certificates certify the identity of their owner, attribute certificates detail attributes like profession or role. Attribute certificates are useful in transactions where attributes, rather than identity, are determinative. Scheme-based PKIs also offer a solution in situations where authorisation should be granted to members of he same association or group, users of one or another application, or users who share qualifications, rather than to individual persons. Malek Bechlaghem, Senior Product Architect at Cryptomathic, provided information on these scheme-based PKIs, their value, business and trust models and key success factors. Signature servers, like the Cryptomathic signer can be used as a digital credentials server, allowing secure central storage of private keys. This way, physical protection of the private key is no longer the responsibility of the end user and the fact that a user owns several digital certificates is no impediment. Mr Bechlachem showed that the e-ID, when used as a strong authentication mechanism in conjunction with server-generated signatures can be the enabler of scheme-based PKIs.

The functionalities of the eID can be used for providing trustworthy information exchange. Anthony Belpaire, CEO of Info2clear explained how current perimeter-based technologies fail to control what happens once content has been received. Trust2 leverages the eID functionalities in order to share documents, mails and web-content, ensuring information rights management protection within and across organizational borders. Trust2 prevents accidental or intentional digital leakage of valuable or private documents and mails within and across organizations. It also offers support for flexible rights management policies, including prevention of forwarding, copying or printing, and management of limited time access (digital shredding, digital lending). Any file format, including HTML, or native Outlook mails can be protected.

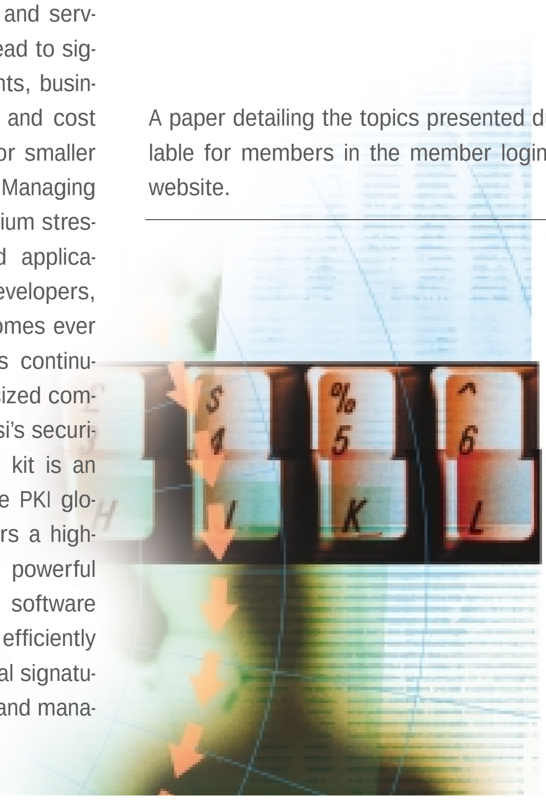
Bart Symons, Business Development Manager, Zetes, detailed how the e-ID can be employed in business environments. Although e-government is the first target of the Belgian e-ID card, the eID is also very valuable for non-governmental organizations and service providers. The eID can lead to significant security improvements, business process enhancements and cost savings for large but also for smaller organisations. Wim de Bie, Managing Director at Intesi Group Belgium stressed that providing secured applications is no easy task for developers, as the security domain becomes ever more complex and changes continuously. Smaller and medium-sized companies can benefit from Intesi's security development toolkit. The kit is an innovative and cost effective PKI global security solution. It offers a high-level, simple, compact and powerful security API, which allows software developers to easily and efficiently implement features like digital signatures, encryption and the use and management of certificates.

The final presentation by Chris Van Den Abbeele, Systems Engineer at Novell, showed how users can get started with the eID, configuring the smartcard reader and the eID card middleware, and preparing the e-mail client for sending digitally signed emails. In a last part, Mr Van Den Abbeele demonstrated how users can adapt existing web infrastructure for eID authentication without having to rewrite web services.

The business potential of the eID was a recurring theme during this event, as was the conviction that standardisation and internationally concerted action in the field of legislation are requirements for optimising this potential. In five years' time, all Belgian citizens will have an eID at their disposal. Initiatives and business cases like the ones presented by the speakers at the event should provide the momentum required for realising the eID's full potential. Event attendants received a Vasco Digipass 850 secure card reader for eID, allowing them to try it all at home.

A paper detailing the topics presented during the event is available for members in the member login section of the L-SEC website.

An Schollen



eID, A promising initiative !

The introduction of the eID card provides an interesting platform for enhancing the security of web based applications. However, while the eID certainly is an enabler for new applications, it is never the ultimate goal. In the end, the focus remains on the functionality of the application, as this is what directly impacts the success of the business.

Too often still the integration of high-end security, of which the eID is yet another example, is perceived by the business as an extra technical and financial burden placed on the application owners. It is very difficult for them to build a business case when they have to consider the costs involved in knowledge transfer, initial application integration and maintenance.

While most targeted communities are convinced about the positive technology impact of the eID card on their business, they still fail to see how they can implement it in a cost effective way.

But what have we learned from the past?

In the past few years we have come to realise that PKI did not take off quite as fast as we had expected. Vendors made us believe that PKI was the long expected solution that would finally enable e-business.

Today we know better. Most organisations that started PKI pilots have learned that there are mainly two reasons why their initiatives have failed to outgrow their embryonic stage. These two reasons are the lack of widely deployed PKI infrastructures and the complexity and cost related to the integration of PKI within their existing and new applications.

While the introduction of the eID card looks like a very promising first step for tackling the former problem, still very few vendors show evidence that they have finally understood that success can only be guaranteed if the latter issue gets solved as well.

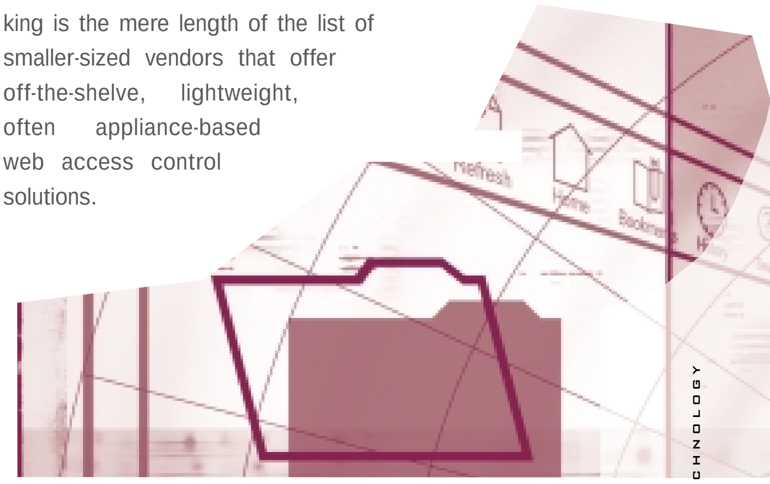
The pioneers of infrastructural application security…

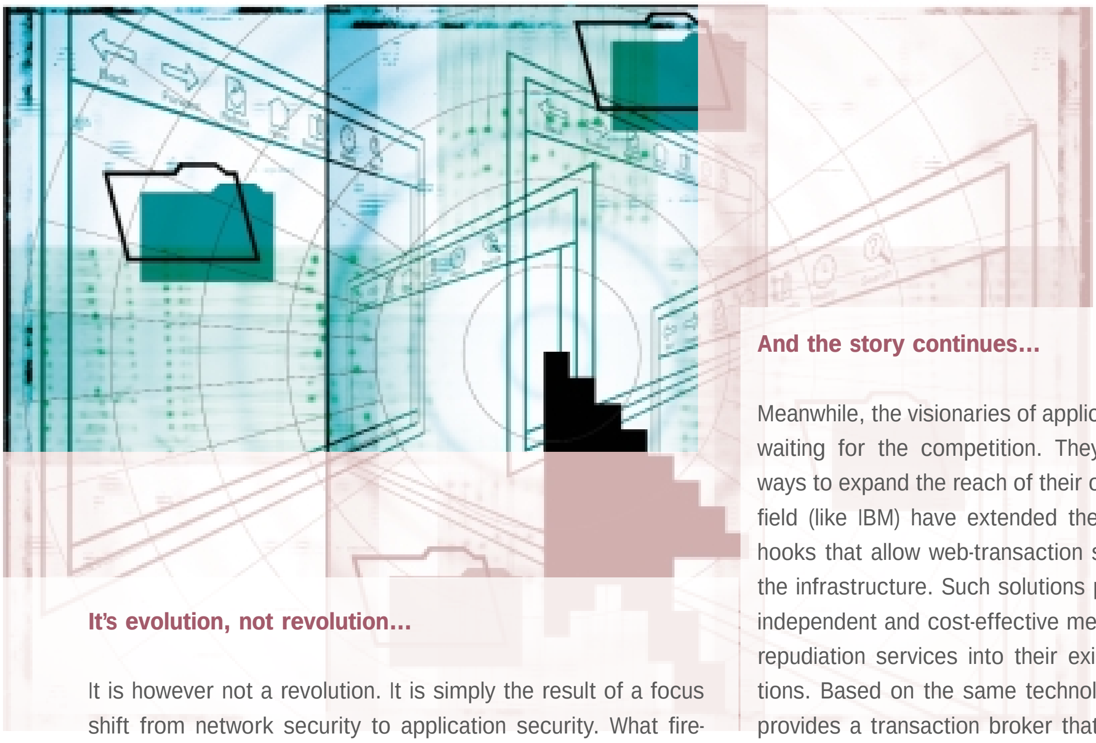
More than five years ago a handful of visionary companies like Netegrity and Dascom (today integrated within IBM) realised that application security, like strong authentication and authorisation, was too complex and costly to be built-in into all applications. Instead, they offered an application-independent solution that would allow these services to be delivered by the infrastructure.

While the message was clear and obvious, these companies found it hard to survive. The main reason for this was the vision of the so-called traditional security experts of those days. They made us believe that real security had to be end-to-end and, as such, was not supposed to be delivered by the infrastructure. According to them, it had to be integrated in the applications.

Today we know better. Multi-tier architectures have commonly been accepted by organisations that take e-business seriously. While each of these tiers is responsible for a part of the security (e.g. block unwanted requests, keep out spam and viruses, intercept attacks, identify users, control access, …) they keep a trust relationship among them. Technology today allows extending that trust relationship to the application as well.

PKI-based mutual authentication and encryption is the cornerstone of a trusted channel between the infrastructure and the applications. As a result, the vision of this handful of companies has become generally accepted and the list of vendors has expanded enormously. Today we cannot think of any security related vendor that is not offering some kind of infrastructural solution for strong authentication and authorisation for web based environments. Among the big players in this field today are vendors like Netegrity, IBM, Oblix, RSA and Novell. However, what is more striking is the mere length of the list of smaller-sized vendors that offer off-the-shelve, lightweight, often appliance-based web access control solutions.

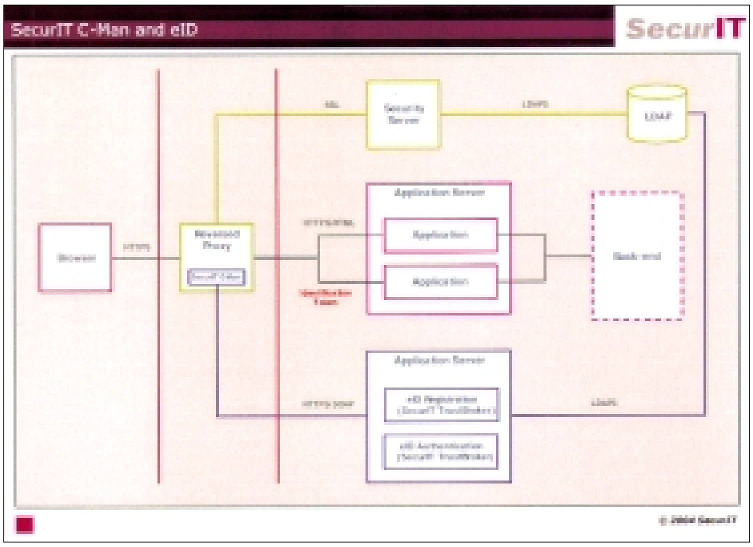




It's evolution, not revolution…

It is however not a revolution. It is simply the result of a focus shift from network security to application security. What firewalls and DMZs have been offering out of the infrastructure for network security for years now, is similar to what reversed proxies today are offering for application security.
Today, no large organisation even considers building strong authentication into each and every of their web-based applications. They rather go for a web SSO solution, providing flexible authentication hooks that allow them to deal with multiple authentication mechanisms in parallel and migrate to stronger ones as the technology evolves.

Leveraging these hooks, SecurIT offers a flexible authentication broker, called SecurIT C-Man, that already expands the authentication facility of IBM's Web Access Management solution (WAM), called Tivoli Access Manager, into the area of eID, or any other authentication mechanism for that matter. In the near future, this functionality will also be made available for other WAM solutions. Today, there is a growing tendency to export application access control and authorisation from the application. This is now made possible through standardisation initiatives like J2EE, SAML and Web Services Security.


SecurIT C-Man and eID

And the story continues…

Meanwhile, the visionaries of application security have not been waiting for the competition. They have been exploring new ways to expand the reach of their offerings. Early players in the field (like IBM) have extended their solutions to also provide hooks that allow web-transaction signing and validation out of the infrastructure. Such solutions provide an easy, application-independent and cost-effective mechanism to incorporate non-repudiation services into their existing and new web applications. Based on the same technology as C-Man, SecurIT also provides a transaction broker that allows using the eID cards for these services.

Nils Meulemans (SecurIT) & Bart Donné (IBM)

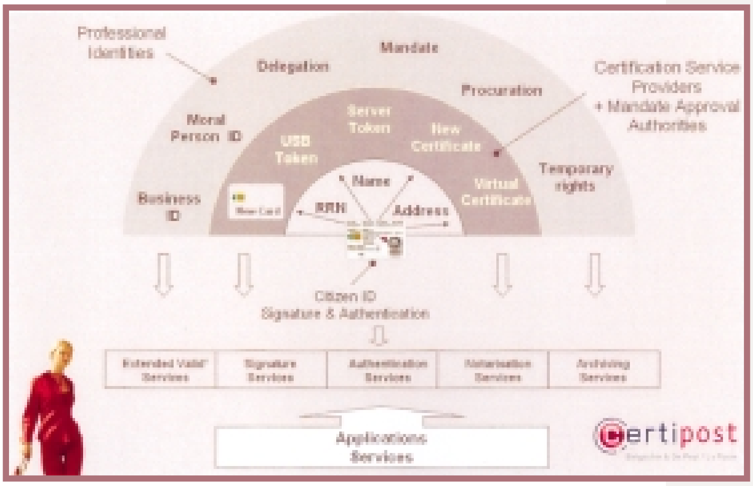
The power of the eID

In the very near future, all Belgian citizens will own a unique tool for authenticating themselves and for generating digital signatures: the Belgian electronic identity card (eID). In addition to its digital signature and authentication functionalities, the eID provides a powerful tool for establishing professional identity management, and for expanding and securing e-services. The opportunities are multiple, get ready today !

The eID provides certification of each citizen's identity. Thanks to digital certificates, eID also allows so-called 'electronic citizen signatures' and 'electronic citizen authentication'. Furthermore, the 'electronic citizen signature' enabled by the eID has the same legal value as a citizen's handwritten signature. eID can help to address a certain number of business scenarios. The eID only certifies the private citizen's identity data, and does not provide information on additional attributes (the card holder's profession, company, etc.), nor does it provide encryption facilities. However, the Belgian eID card is the perfect tool for initiating requests for the new credentials that are required for addressing these business scenarios.

eID becomes a standard identity tool

The Belgian eID is a powerful business-enabling tool.



Thanks to the certified data and the digital certificates on the eID, it is very easy to initiate the issuing of new credentials in order to address other business scenarios, i.e. identity data can be securely "extracted" from the eID and the requestor of new credentials can be strongly authenticated for his/her certificate request.
Certification Service Providers - like Certipost - with the support of Mandate Approval Authorities can very easily issue additional PKI credentials on the basis of the eID. These additional PKI credentials can take the form of a new smart card, an USB token, a server token, a new certificate or a virtual certificate (i.e. attribute certificate). The purpose of these new credentials is to certify a professional identity, such as a business identity, or a personal identity and can be used as delegation, mandate, procurator credentials (e.g. when a person signs in the name of someone else either for another person or for a company). As part of the process of issuing professional credentials, the Certification Service Providers will include the approval from the Mandate Approval Authorities, certifying that the requester indeed benefits from these professional attributes.

The additional PKI credentials must be supported by additional Trust services, allowing applications to use these credentials. These extended services (services for validating the status of the PKI credential and the professional attribute, signature services, authentication services, notarisation services for providing long-term validity of documents and associated digital signature and archiving services) are based on the same PKI technology underlying the eID card. This means these credentials can be used straight away, once one has decided to use ID technology.

The usage of the eID with an additional PKI credential, supported by additional Trust services, provides signature, authentication and encryption for professional identities, enabling a very broad range of eID-based solutions for third parties.

PKI-based additional credentials on native eID services will maximize the ROI of eID integration. Compared to database-oriented credential allocation and management, you gain in interoperability, standardization, technology outsourcing, transparency and time to market.

Case Study

Case Study:
Managed Authentication Services in Healthcare Sector

Let us examine the case of a nurse who has to connect to a portal. Her private identity must be verified but she must also be authenticated as a nurse in order to benefit from the services for which access is restricted to nurses only. She connects to the portal using her electronic identity card.

The portal will then send an authentication request to the Authentication Services Trusted Third Party (TTP), e.g. Certipost. This Authentication Service TTP will check the validity of the electronic identity card digital certificate via eID OCSP services. Next, the TTP will check whether she has a virtual certificate (or attribute certificate), whether that virtual certificate is valid and contains the expected rights. Once the checks have been performed, the TTP sends an answer to the portal's authentication request.

The complexity of the authentication has moved away from the end-user and the application (portal) provider, and is now handled entirely by the TTP.

More information: www.certipost.be/eID

User Provisioning with SPML

Gavenraj Sodhi
Computer Associates

Introduction

During the past half-decade, the economy has been going through a cyclic process. Businesses have been encouraged to cut spending, which has sometimes resulted in lay-offs. Large-scale mergers and acquisitions have occurred. Corporations have learned that to succeed in this type of environment, they must be versatile, lean, and economically diligent. As it is often accompanied by lay-offs, this approach usually does not sit well with employees. Employee dissatisfaction has, in some cases, led to corporate negligence, espionage, and identity fraud. Another major initiative for curving spending has been the development and enhancement of business practices. All the concepts discussed above have one common theme: managing identities and securely provisioning and de-provisioning them effectively, to resources inside and outside of the organisation. This may sound easy, but with new technologies come hurdles of developing and incorporating business practices, privacy policies, corporate goals. New technologies, while often immature, may have raised visibility with management, especially because of the large cost of purchasing and implementing.

I thought it may be interesting to talk about where the technology is going and how standards like Service Provisioning Mark-up Language (SPML) are being developed to ensure the longevity of the technologies. As investments in technologies are often huge, companies are determined to ensure that they facilitate efficiency within the organisations. Provisioning is difficult to implement from a business process point of view as well as from a deployment point of view.

Provisioning and Security

Provisioning and Security Management go hand in hand. Communication between the provisioning server(s) and the managed endpoints (target systems) must be secure and encrypted. Next to that, the underlying fundamental business processes need to be generated dynamically, so as to support the security policies and business practices of the organisation.

User information can be used to create a profile of a person or role that indicates exactly what resources should be allocated to that person or role. Changes to the profile can automatically trigger provisioning or de-provisioning activities. This means that, when an employee moves to another business unit, for example, all of the necessary workflow items start and proceed to the reassignment of provisioned items, based on approvals received and external systems like those from HR.

An organisation's security is improved when you can automate the process of managing access to managed endpoints. You can also essentially roll-back the provisioning process, clearing all access rights for any employees that have left the company or moved departments via a single process while maintaining a complete audit of all changes.

Auditing

The provisioning system's auditing system should help to ensure that all events and activities associated with identities or resources can be tracked. Auditors can see when an identity was created, by whom, where the identity went, what it accessed, what it touched, what it morphed into, when it was suspended, by whom and when it was terminated. It tracks all provisioning activities across the entire enterprise and the extended enterprise, monitoring, collecting and filtering events, providing centralized management of organisation-specific audit policies, triggering alarms and alerts.

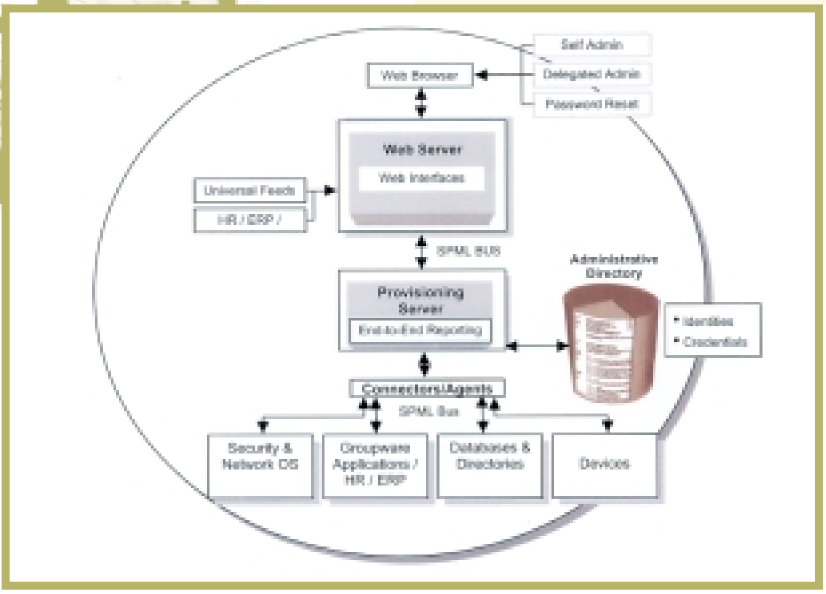
Provisioning Standards Support and What is SPML?

As the co-founder and current secretary of SPML, I recognized in 2000 that Employee Provisioning solutions needed to interchange with other solutions, repositories, applications, services, and that there was a need for interoperability at some level with other provisioning and meta-directory solutions. SPML started as a group of technology companies. It eventually evolved from three competing specifications into one specification, Service Provisioning Markup Language (SPML) version 1.0, which was agreed upon as an OASIS standard.

Through the years of operating and implementing business process management systems, creating connectors for systems, services, and devices, I came to understand that each unique system has its own concept of workflow and that SPML would not be an easy process to standardize. Standardizing would be difficult and politically charged. Most important to the vendors involved was the fact that organisations have one or more identity-based provisioning systems, employee lifecycle management tools, meta-directory systems, or applications and devices that are based on identity information within their internal or external enterprise. Technologies may have been acquired via mergers and acquisitions, and over the years certain technologies may have become legacy to a certain degree.

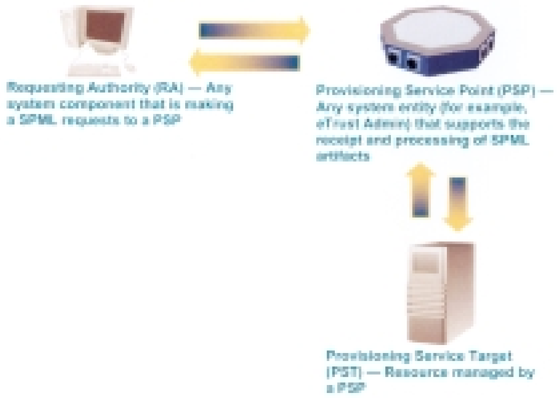
Service Provisioning Mark-up Language, SPML, is a provisioning standard developed and ratified within OASIS, Organisation for the Advancement of Structured Information Standards. It is intended to provide standard methods for provisioning and de-provisioning, querying, modifying, suspending, and restoring user accounts across heterogeneous systems, devices, and non-computing resources (e.g. credit cards, laptop computers, phones), which require a manual activity to be kicked off via the systems workflow, while notifications are to be automated to respective approvers. This common administration can significantly reduce IT workloads, helps to ensure compliance with security policies, and provides employees with immediate access to critical resources. Changes in human resource systems can be propagated automatically to IT applications without human intervention.

Based on an XML-based framework, SPML allows a provisioning system's capabilities to be extended to any enterprise system or web service, adopting the necessary compliant interface. SPML would allow businesses to deploy and use web services via a common language, to more securely manage the identity of users, including the dynamic allocation of their associated resources/web services, across trusted boundaries.



SPML v1.0

Version 1.0 of SPML was ratified within OASIS in November 2003. SPML version 1.0 marks the first step in the development of a standardized interface for exchanging provisioning requests. To enable truly secure access control to resource allocation, system and web service allocation, SPML is designed as a standard, a protocol that allows the automation of access control for system and user access to systems, devices, and web services.


Requesting Authority (RA) — Any system component that is making a SPML requests to a PSP
Provisioning Service Point (PSP) — Any system entity (for example, eTrust Admin) that supports the receipt and processing of SPML artifacts
Provisioning Service Target (PST) — Resource managed by a PSP

SPML v2.0

In January 2004, the Provisioning Services Technical Committee (PSTC) met to discuss requirements for version 2.0 of SPML. Today, SPML version 2.0 is work in progress.

Conclusion and "What can I do …"

Get involved. Identity and Access Management, of which provisioning is a key technology, is here to stay and the market grows substantially each year, while technology evolves. The PSTC is not only a standards body made up of software vendors, but also of customers, customers, and even more customers. More customers need to get more involved, state their needs and problems, and in turn, SPML will enable deployments and integrations to be made much easier for them, thus reducing overall costs and providing for a faster ROI.

Provisioning and Identity Management are key technologies for enhancing operations and increasing the efficiency level. More importantly though, they are of key importance in managing one's identity securely, wherever it may travel. Standards are a necessary requirement for solutions to interoperate with existing as well as new systems. In case of mergers and acquisitions, one or more organizations may already have identity or provisioning-based solutions and will need to integrate them.

Vendors need to get engaged on a world-wide basis, because building a standard interface to Identity Management systems is a competitive advantage for each of them. It is as important to encourage a larger audience of users to purchase SPML standards-compliant solutions, because they "can" interoperate with the standardized interfaces of Identity Management systems.

For more information about SPML and about joining the PSTC, please visit:

http://www.oasisopen.org/committees/tc_home.php?wg_abbrev=provision.

Individual Membership Program

The Value

The Leuven Security Excellence Consortium organization represents a unique platform of world-class e-security expertise and professionals and contributes to innovation and high-tech entrepreneurship through its synergy with other organizations and networks

As a member of L-SEC you will have an independent partner in finding solutions for all your security challenges. The membership keeps you up-to-date with the fast moving information security industry and brings you high-quality conferences, workshops and publications.

Through a single point of entry you get access to the knowledge and technology provided by its members and academic institutes.

As an L-SEC Member, you will receive:

- Invitation to the L-SEC annual event focusing on new trends, challenges and solutions in e-security
- Invitations to market or solution specific events focusing on e-security developments and evolutions for that specific area
- Invitations for our advanced workshops intended to promote the e-security aspects within a specific domain
  Receive the quarterly newsletter with market and e-security information
- A 50 € rebate for the annual and market specific events (minimum 3 events yearly)
- Discount to attend the workshops
- Discount to attend the education and training program
- Access to presentation section for members only

Who should join us?

- IT Security Consultants who guide their clients towards the right level of security
- Security Officers who wants to be kept informed about the latest evolutions and trends in the e-security market
- Hosting companies, B-to-B, B-to-C companies, consultants: who needs to be aware of the fast evolving security solutions required to protect the assets of their clients.
- Security and network administrators and those who are responsible to protect the company's electronic infrastructure, privacy and information.
- IT Auditors and controllers who help companies verifying the information infrastructure and control mechanism

Register on-line for individual membership www.l-sec.be

Upcoming events

Information session"new regulation security advisors"

Date: 8 July, 2004
Place: VBO, Ravensteinstraat 4, 1000 Brussel
Info: www.l-sec.be

Security Return on Investment workshop

Date: 15 September, 2004
Info: www.l-sec.be

Intesi Group PKI Suite workshop

Date: 14 September, 2004
Place: UBCA, Drie Eikenstraat 661, 2650 Edegem
Info: +32 3 826 93 00 or ubca@ubca.be

Forensic Analysis workshop

Date: 16 September, 2004
Info: www.l-sec.be