Absolute confidentiality for the Banque de Luxembourg thanks to efficient encryption and Utimaco Safeware's SSO solutions.

"Using Utimaco's solutions we can not only conform to Luxembourg's financial sector regulations, but also fulfil the requirements for internal auditing and control procedures as set out by company auditors. These specify that banks must take the best-possible security measures when handling confidential files… In addition to this, by using Utimaco's solutions we are also able to keep the roles of network administrators, security officers, and users, clearly separate and guarantee something that is very important - making life easier for our users …"

René Chevremont
General Representative, IT security, Banque de Luxembourg

Profile of the Banque de Luxembourg
Founded in 1920, the Banque de Luxembourg (BDL) is a privately-owned bank which provides both private and professional investors with the benefits of its experience and independence in the asset management sector. Although the bank has become one of Luxemburg's foremost asset management institutions it has always placed great emphasis on maintaining a "friendly" image. In 2003 the bank employed 600 members of staff and achieved a revenues of 11.7 billion Euros.

Sector
Financial sector
Area of activity
Luxemburg, Europe
Area of application
50 notebooks and several hundred workstations
Utimaco solutions
1) SafeGuard Easy
2) SafeGuard LANCrypt
3) SafeGuard Private Crypto
4) SafeGuard Advanced Security Single-Sign-On (SGAS SSO)
5) SafeGuard Biometrics
Implementation
Utimaco Safeware
Benefits

- SafeGuard Easy protects sensitive data on notebooks if they are lost or stolen.
- With SafeGuard LANCrypt it is possible to clearly define the type of information that can be accessed by Novell network administrators, security officers and users. Only users are permitted to have simultaneous access to the encrypted files and the key used to encrypt them. Novell administrators can never access unencrypted files. Security officers can access the keys, but not the files.
- In SafeGuard Private Crypto suppliers can be assigned permission to create secure e-mails which contain customer access codes for the bank's web platform. At a service provider's site, users can decrypt sensitive files without the need for any additional software or being able to directly access any of the confidential data themselves.
- The Single Sign On (SSO) solution uses biometrics or a PIN code on a chip card to make the authentication procedure and secure access to one or more systems or applications much less complicated. This solution also means users can easily comply with complex security procedures, especially those involved with creating and renewing passwords.

Challenges presented by BDL

The Banque de Luxembourg (BDL) is a large asset management institution that is part of Luxembourg's financial sector, and belongs to the Banque CIAL, which is part of the (French) CIC group, and to the (French) Banque Fédérative du Crédit Mutuel (BFCM), but has its own supervisory board in Luxemburg. The bank has also created the company *Fund Market*, which specializes in selling funds, and also the company CFG (Compagnie Financière de Gestion), which is also supported by the Banque de Luxembourg's IT department.
From a technological point of view, the Banque de Luxembourg is a completely autonomous entity whose architecture differs greatly from that of its French shareholders. For example, BDL uses IBM AS/400 platforms, Olympic, which is Eri Bancaire's specialist banking software, and a Novell network that is not used either by CIAL or BFCM. BDL relies on security solutions that are available on the open market whereas similar companies tend to use in-house developments.
"We have been dealing with the problem of data security ever since *1993-1994, when the very first PCs were used in networks. In the past we primarily used terminals and a few PCs. The introduction of "distributed" computer technology on workstations resulted in the implementation of security measures"*, explained René Chevremont, General Representative and person in charge of IT security at the Banque de Luxembourg. "*We quickly became aware of Utimaco and implemented the "very first" version of SafeGuard Advanced Security for Windows as our first security product, with only a few licenses, at the bank itself. Then we worked with SafeGuard LANCrypt to ensure the confidentiality of information by encrypting internal, shared files that were then made available over our network. At more or less the same time we started using notebooks and decided not only to protect access to them but also to encrypt the data to prevent it being misused if these devices were lost or stolen. This is why we chose SafeGuard Easy, because it was far and away the best tool for the job…"*
Today BDL has around one hundred licenses for SafeGuard LANCrypt and approximately fifty licenses for SafeGuard Easy (for all its notebooks). "*We selected LANCrypt for a number of reasons", says René Chevremont. "We use Novell file servers, firstly, because you can then encrypt either an entire directory, and/or a subdirectory, or a single file or even the whole A: drive (diskette). Secondly, because the product is installed locally on computers (which means that the files can only be opened unencrypted in the local computer's memory), and thirdly because the algorithms these servers use are the most effective on the market. This allows us to clearly separate the roles of users, Novel server administrators and security administrators. As soon as a user*
closes a file it is encrypted on their computer, saved to the network server, and then encrypted and saved. The keys and key files are generated by the security department and transferred into the network, which means they are also secure. As a result they can be taken into account and used in data backup plans.
Depending on their Novell and LANCrypt rights,a user can therefore access a "key" file which contains the password definitions, the key that was used, the algorithms and the file paths that are to be encrypted. AES is extremely good at defining the most efficient algorithms without compromising the ability to process large files. Our data security and data continuity solutions guarantee complete redundancy. As a result, SafeGuard is with us all the way to our data security center at eBRC."

The Banque de Luxembourg is based at five main sites, which include the Howald site (administration center), Boulevard Royal (company headquarters) with an "empty" computing centre, which contains duplicates of all important systems, Kirchberg, Grand-Rue (with Fund Market) and Gare. There is also a branch in Bertrange (at the Belle-Etoile shopping center).
Alongside SafeGuard LANCrypt and SafeGuard Easy the Banque de Luxembourg also uses SafeGuard Private Crypto for encryption. "*This product is currently hardly used, although an increasing number of our users are showing an interest in it because it is very flexible and so easy to use",* explained René Chevremont. *"With this solution they can use the best currently-available algorithms for file encryption (such as AES) without the need for a program to call up the unencrypted files. This is because the encrypted files can be "unpacked" with the same password used to encrypt them. For example, we use this solution for transferring data that is used to create documents that contain the codes our customers use to access the internet. These secure documents are created externally by a PSF-certified supplier. We send our files (encrypted by Private Crypto) to the supplier and decrypt them ourselves at the supplier site without having to install additional software for this purpose."*

BDL building on the Boulevard Royal

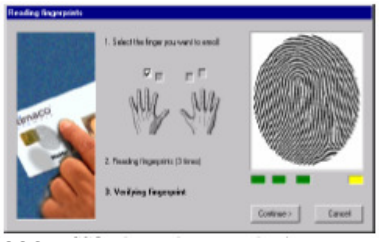
On the way to Single Sign On

At the beginning of 2001 the Banque de Luxembourg started looking for a Single Sign-On solution (SSO).

"*We narrowed down our search to three types of SSO: one running on a Novell server, another using an authentication server with communications agents and the last being a system-independent variant running on workstations using efficient authentication."* stated René Chevremont. The tests, which were first carried out in the IT department with around 30 users, showed that the third solution was by far the best and that the others had severe problems with AS/400, which is the platform on which our bank-specific software runs, and to which all our users are therefore connected. Since the selected SSO solution is one of the main products in Utimaco's SafeGuard Advanced Security range we did not hesitate to select it. Apart from the fact that this solution supports our AS/400 platform, and provides the functionality for controlling switching Windows to standby, it is fully installed on every user's workstation. In addition, all the information is located on a chipcard that accepts both a PIN code and biometric data. We wanted to give our users the most user-friendly solution so we gave them a choice of authentication via a PIN code or using a digital fingerprint. The fingerprints themselves are saved on the chip card (and nowhere else), so that only the user alone has all the elements needed to create a connection with the bank's systems, i.e. the card that contains the passwords and the digital fingerprints, and also the user's finger, which they use to authenticate themselves to the card. The chip card they use is also necessary for accessing the building, maintaining the flexible workplans and for paying in the company restaurant.

"*Of course, we have also provided a means of "manual" access for the users who have lost their chip card or forgotten it at home. A number of suppliers provided different elements for the SSO project (chips, cards, biometric reading devices), but it was Utimaco that took responsibility for the overall integration and implementation of the solution in our company. More than 500 users use this solution, of whom 90% use the biometric variant. The system can prove very useful for them since they no longer need to remember ten (or more) passwords for the different systems or applications that they access, they no longer have to worry every five weeks about finding new passwords that comply with the complex rules imposed by security, since this is handled by SSO, and so all they need to remember is to bring their chip card and their finger with them. Other users with special profiles, such as the system and network administrators, the IT staff and members of the web team, still need to know and manage their passwords. It should be remembered that solutions like SSO are implemented to make life easier for the users. If this kind of solution brings with it too many restrictions, those users will start to reject it, and it will fail.*

The biometric solution used by BDL, which is supplied by Precise Biometrics, works in perfect harmony with Utimaco.



SSO biometric authentication

If a security layer, no matter what kind, is added to a system or application, this always has a functional and/or effect on the organization, and this is even more true if an SSO application is involved, which affects more or less all the systems in the company. In the Banque de Luxembourg, the implementing of SSO also saw a real restructuring and reorganization of the way in which the bank distributes tools and applications to the workplaces. SSO provides exactly-defined processes, and also settings for booting Windows, Novell, the different AS/400s, Swift, PeopleSoft, etc., or even automatic standby switching. For this reason the information must be distributed in the form in which, and at the exact moment at which, SSO is waiting to receive it, which requires tremendous accuracy. The SSO solution has enabled the use of complex passwords which can contain large and small numerical and alphabetic characters, special characters, non-repeating characters, passwords with regular offsets, etc., a procedure that has been directly adopted from the one used on the AS/400.

This applies both for compliance with the rules of "professional care", as they affect security, and also for implementing the recommendations of our internal or external auditors. With the help of Utimaco, BDL was also able to use the rules on its Lotus Notes email system, even though this product does not actually have these properties.

The way into the future of SSO includes taking into account internet access and better handling of HTML. The Banque de Luxembourg is especially pleased with the support that Utimaco provides: the company has always succeeded in developing solutions that are tailored to its needs. The bank expects greater use to be made of the SSO solution, especially in the case of windows technology. BDL is relying on Utimaco to make all possible efforts to ensure the mutual compatibility of the products, on the Novell platform, wherever Novell is implemented at BDL. However the way into the future also leads towards authentication solutions using web tunneling, for which Utimaco and Telindus, the local partner of Citrix, are striving to find answers for the bank. An alternative is better-tailored solutions such as USB tokens for notebooks. As SafeGuard Easy performs pre-boot authentication, it is difficult to make the program support chip cards with particular reader devices during booting.

"*We should never lose sight of the fact that, while the company's information must be given maximum protection, it must at the same time be accessible by anyone who is authorized according to the defined rules, and that the quest is for high security with great user flexibility: two things that in general terms contradict each other",* said René Chevremont. "*Our role is to find the best compromise and some of Utimaco's products help us a lot there.*

The future with Utimaco

"Like the bank itself, the products and applications used in the bank and in the market are undergoing constant development, and new products and hardware are implemented. We expect from our relationship with Utimaco that the company can keep up with these developments and even anticipate them. This is the case with the more systematic use of the portal used for the intranet and Internet, which SSO needs to be modified to suit. To give another example, the bank has just decided to change over its workplaces to Windows XP. This latest version of Windows makes it very easy to use USB ports and plug-and-play hardware, which can present enormous security weak spots for potential attacks. Utimaco supplies a solution that is absolutely ideal for SGAS PnP control. We have tested it, and now want to implement it as quickly as possible. To sum up, our relationship with Utimaco is not simply one of a supplier and customer. Instead we enter into a true exchange with them, through which we work together on solutions that can be used both in our company and also in the entire market, which is of equal benefit to BDL and Utimaco."

René Chevremont
General Representative, IT security, Banque de Luxembourg