CRYPTOMATHIC
www.cryptomathic.com

Signer Case Study – LuxTrust

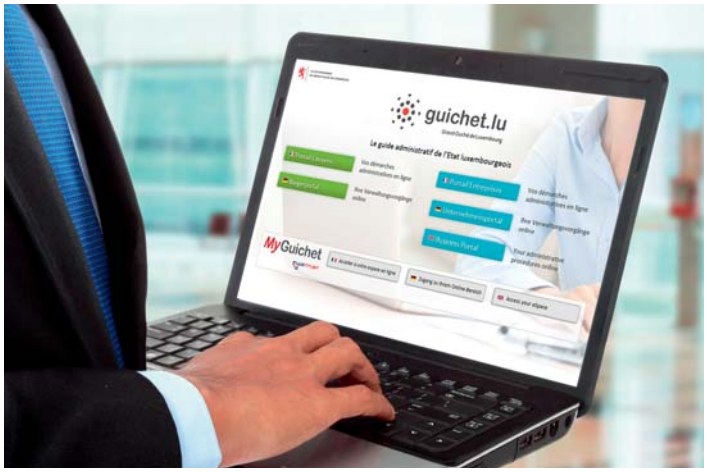
CENTRAL SIGNING SERVICE

Residents in Luxembourg are now able to securely access a variety of web applications such as eBanking and public services, as well as digitally sign legally binding transactions and official documents from an online PC or mobile device, anywhere in the world. With just one LuxTrust certificate, users can remotely access and sign multiple online forms from any organisation connected to the service, whether they are registering their new home or applying for a loan. This highly innovative and flexible authentication and digital signature service has been implemented by LuxTrust, using Cryptomathic's solutions.

LUXTRUST

As Luxembourg's primary provider of digital identity and electronic data security services, LuxTrust provides various IT services, aimed at delivering and enforcing digital trust between parties, including certificate issuance, strong authentication, digital signatures, time stamping, and long term storage to enable secure electronic commerce and to meet the future security requirements for both government and financial organisations. LuxTrust was founded in 2005 between the Luxembourg government and major investors from the private financial sector, to guarantee the promise of secure electronic commerce through technological advancement and a flexible, cost-effective, and user-friendly platform.

With extensive experience in delivering market-leading digital trust services, LuxTrust facilitates and protects a broad range of sensitive and confidential transactions performed in the cloud. LuxTrust is also a trendsetter in mobile security and is actively embracing the changing legal environments surrounding electronic services and identity management. The LuxTrust offerings exceed industry standards when it comes to security and service availability.



Signing Server Certificate

In 2008 LuxTrust launched its Signing Server Certificate (SSC), which enables residents and organisations from various geographic locations to securely access sensitive online information and to legally sign and certify electronic documents. It proved to be beneficial for a significant number of organisations, demanding high security, while avoiding impairment of the essential user experience and, at the same time, reducing the deployment costs.

In order to make the service a success, LuxTrust had to take advantage of combining public key infrastructure (PKI) and two-factor authentication (2FA) to avoid the limitations associated with using the technologies separately. Tradiationally, PKI offers a high level of security, but has severe usability constraints while being prohibitively costly to deploy and maintain. On the other hand, 2FA can deliver the flexibility, cost-efficiency and usability that cloud services require, but lacks the legally binding attributes provided by PKI.

LuxTrust approached Cryptomathic to solve the challenging issue of establishing legal value by way of high security (using PKI and 2FA) without costs escalating and destroying the business case. Today, most Luxembourg based institutions, including eGovernment and eBanking, utilise the benefits delivered by LuxTrust's SSC – a mutual security infrastructure service. The SSC combines this high level of security in the most convenient and portable service, allowing users to authenticate themselves with a choice of two-factor authentication mechanisms to securely access online applications at anytime and from anywhere.

The ongoing trust service delivered by LuxTrust has enabled numerous organisations to significantly reduce security complexity and high costs that are traditionally related to securely communicating and managing sensitive material between various independent parties and legal entities.

The service has also helped organisations and individual users reduce time consuming processes, costs of document handling, and environmental impacts by going paperless through the provision of electronic signatures on relevant exchanges.

Ease of Use

The central signing scheme offers residents the greatest convenience as they can use their standard credentials and a single 2FA mechanism to access every service on the network. Using one common platform that shares the security infrastructure eliminates the need for users to carry several authentication mechanisms in order to securely authenticate themselves on different websites or applications. Avoiding complexity is a great benefit to users *and* service providers, as ease of use results in higher user acceptance and service adoption. Usability is also a key aspect in keeping costs at a minimum, since users can confidently and with ease use all services that are part of the infrastructure.

Lowest Cost Per User

As a centrally managed service, the costs for the user's certificate are shared among the multiple application providers enabling highly secure PKI technology at a fraction of the price of an in-house solution.

Peter Landrock,
Executive Chairman of
Cryptomathic

We are delighted to have found a partner driven by technology innovation for improving business flow and securing digital infrastructure. LuxTrust is a very competent sparring partner with the ability to fully grasp current and future market requirements while having the ability to execute. We look forward to working even more closely with LuxTrust for many years to come."

Pierre Zimmer,
Managing Director at LuxTrust
and Government CIO

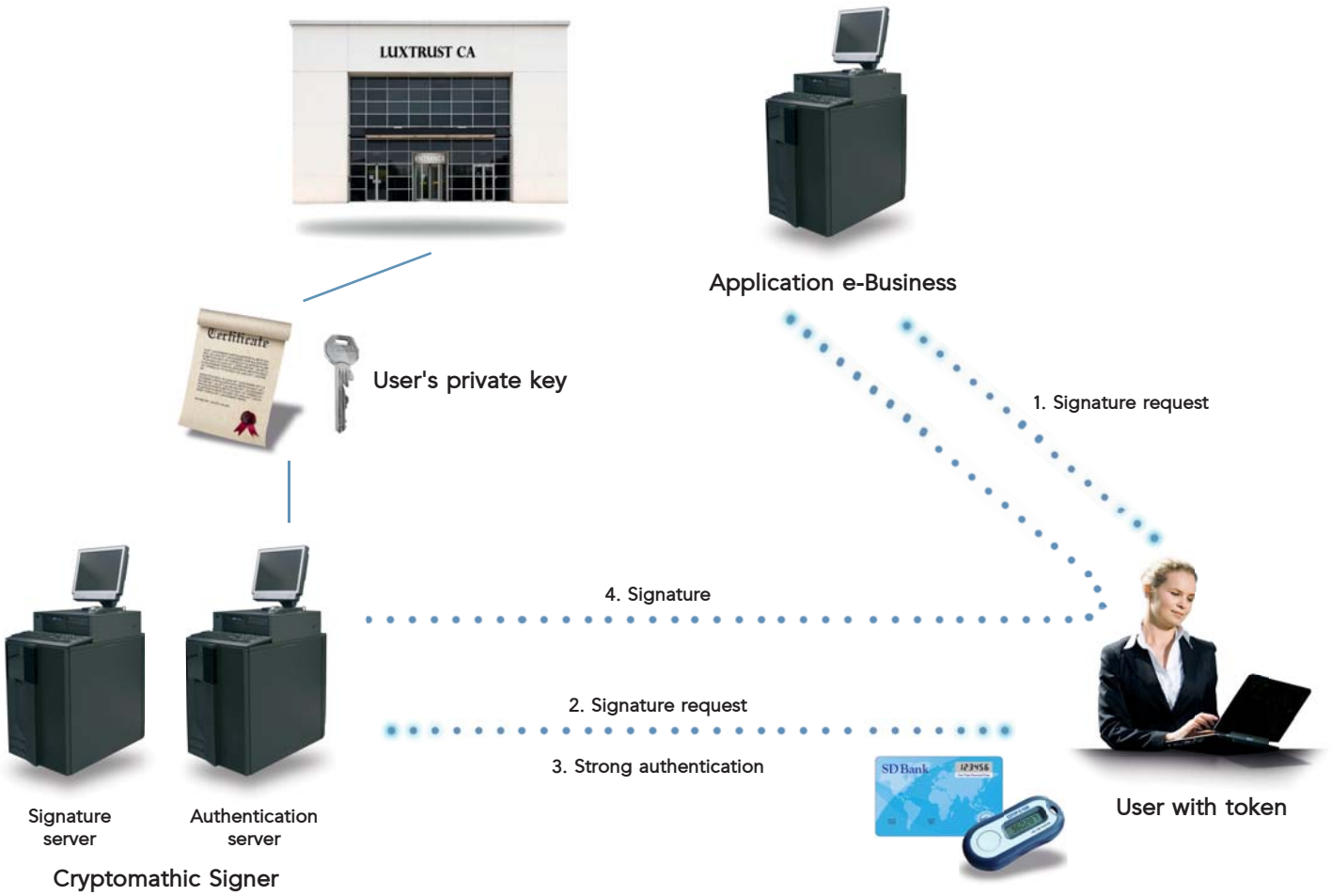
In Luxembourg, perhaps more than anywhere else, we have the need to provide trust, strong usability and excellence. Due to the limited size of our country, it is vital for our residents and companies to interact effortlessly with the rest of Europe. We simply have no choice but to offer services that are completely flexible and recognised on a pan European level. In cooperation with the financial sector, the state took the initiative to set up a centre of excellence for the provisioning of trust services. Initially selected as a technology supplier, Cryptomathic is now a key partner for the ongoing development and expansion of our service portfolio. Cryptomathic has been more than capable of understanding our market requirements and together, we are now taking the additional step of launching an innovative offering in mobile security."

Solution Overview

At the heart of the infrastructure is Signer, Cryptomathic's patented signature server that facilitates the unique combination of mobility, flexibility, and security in the SSC. Signer's exclusive security architecture stores the user's private signature key in the central LuxTrust secured server, which removes the requirement for residents to use connected smart cards and readers - thereby providing full mobility for all users. In order to gain access to the signing service securely, users authenticate themselves against Authenticator, Cryptomathic's complemetary 2FA server. This uses a combination of a traditional password with a range of multifactor authentication mechanisms. The two servers deliver both strong authentication to the application and digital signatures for the transactions.

- A single certificate based solution
- Independent of external connecting device
- The clients private key is stored on a central LuxTrust secured server
- A one-time-password (OTP) is generated every 30 seconds on the 2FA token
- Solution mainly developed for C2B/C2G applications

VIRTUAL CHIP CARDS



Solving the Key Storage

In any solution involving digital signatures, it is essential to choose the right store for the user's signature key. Software key stores remain the most common choice. While they are quite easy to deploy, they offer very limited security and no mobility at all. Hardware key stores, like chip cards, offer higher security and even promise some degree of mobility. However, smart card readers are not yet included in standard PCs. The Cryptomathic Signer combines the best of both worlds. Without having to install any software on the client side, deployment is not an issue whatsoever. For mobile devices no private key or other sensitive data is stored on the mobile side, resulting in optimum protection and physical security, while the user enjoys full mobility.

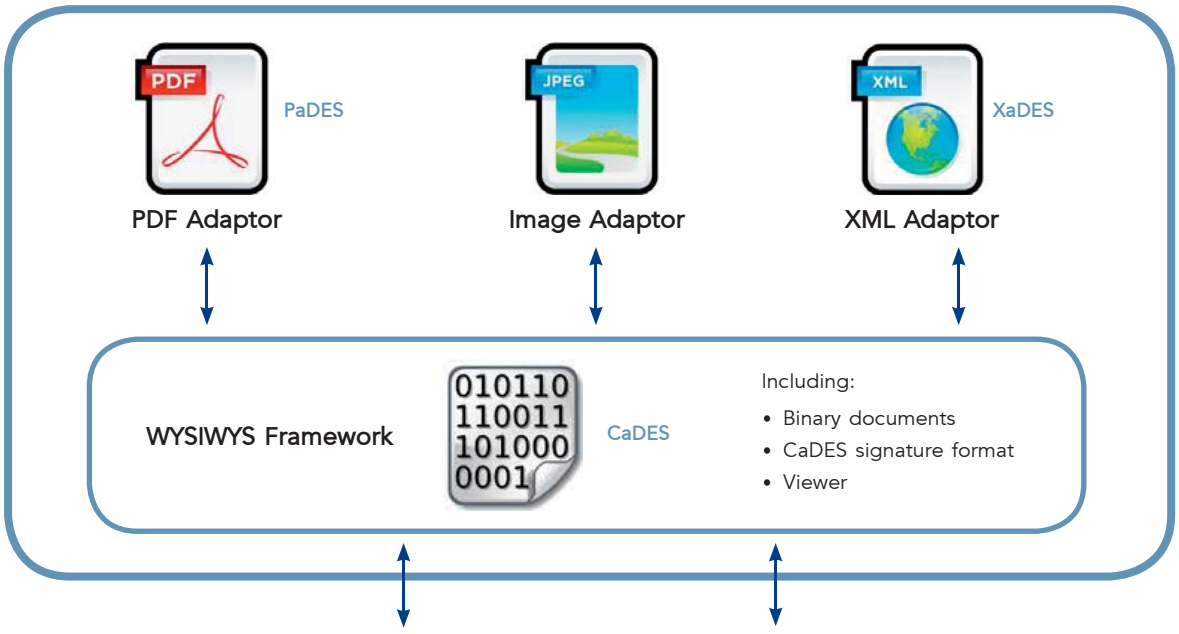
Interoperability

Application Service Providers (ASPs) are provided with a comprehensive digital signature module (DSM) framework allowing for seamless integration with their business application workflow. The DSM is a platform independent module, allowing for raw data or documents in popular formats such as PDF, PNG, XML to be signed with relevant signature format standards such as:

- PaDES
- CaDES
- XaDES

The DSM module follows industry standards and is a powerful and flexible tool, designed especially for ASPs that want to rapidly integrate signing services into their application(s). It contains the functionality they need to address custom requirements (e.g. enveloped or detached signatures / custom fields such signed attributes or signature policies) and also comes with complementary functions such as adding a timestamp, verifying a signature, etc. Thus the ASP has an easy task integrating the signing services supplied by the Trusted Service Provider in their internal business process.

DIGITAL SIGNATURE MODULE



ABOUT CRYPTOMATHIC

Cryptomathic is one of the world's leading providers of security solutions to businesses across a wide range of industry sectors, including finance, technology, government, mobile and cloud. With more than 25 years' experience, Cryptomathic provides customers with systems for e-banking, PKI initiatives, ePassport, card issuing, mobile payments, advanced key management and managed cryptography utilizing best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with an established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

Learn more at cryptomathic.com