Case study

Protecting health records: secure, transparent, cost efficient

The motivation: increasing transparency and cost efficiency in public systems - ELGA in Austria

Public health systems can be costly. In order to ensure maximum transparency and thus cost efficiency, Austria had decided to introduce ELGA, a public system of health care records. ELGA is an information system that allows all the patient and all participants of the public health care system to access a patient's records including documents supporting the diagnosis as well as the subsequent prescriptions. The benefit of this include a faster and greater transparency for each practitioner (doctors, hospitals, care institutions, dental practitioners, pharmacies, etc.) about a patient's history and thus improve the quality or appropriateness of the care provided and thus potentially to work more cost efficiently. It also allows patients the possibility of accessing and managing this information. In this respect, Austria takes a leading role within Europe for eGovernment and eHealth projects via early implementations especially also of projects addressing the issue of intra-national compatibility and interoperability[1].

[1] Kraner, Klaus (2016): Cloud-Technologien im extramuralen Bereich in Österreich, Master Thesis, Donau-Universität Krems, S 26

The challenge: putting health records into the affinity domains while ensuring confidentiality, availably and integrity

From security point of view, online availability of health records is an ambitious and potentially complex challenge. The list of requirements is a long one: Since every health file needs to be accessible to patients over the Internet using their “citizen card” for authentication, while doctors and hospitals and other service providers exchange data via closed, proprietary networks like “eHI”, “HealIX” and “GIN”. For both privacy and compliancy reasons, health records need to be encrypted. Access needs to be secured, and the new system was to be integrated into the existing e-card system. Data storage was meant to be in Affinity domains to make sure accessibility and scalability was granted, and backup for the data provided.

On top of this, it was not sufficient to encrypt the transportation protocol (according to the “Gesundheitstelematikgesetz” of 2012 in line with EU regulation); in a publically accessible network all data at rest had to be encrypted, not just data in transportation. Having said this, neither the user nor the usage data are accessible to support employees. Other requirements included the fact that according to ISA 27001 sensitive data is to be accessible only according to 4-eye-prinziple, which called for a role-based key management access system, ensuring that system administrators did not have access to the keys. In this particular case, the choice was to store the keys externally, and based on best practices, certainly also in a separate organization as well as a dedicated hard ware based location.

The solution: hardware-grade security as a Root of Trust

The SVC (short for Sozialversicherungs-Chipkarten Betriebs- und Errichtungsges.m.b.H) was commissioned as a system integrator for the ELGA Portal and the integration into the existing e-card system by the Association of Social Insurance and the prize winning[2] end user web portal that allowed patients to access and manage their data.

It combines certified hardware-grade security with extreme ease of use, deployment, and operations. Here is how the Utimaco Hardware Security Module as the “Root of Trust” of this particular architecture / solution.

The technical solution: a Public Key Infrastructure to protect patient data records.

To protect patient health records, a multi-layered PKI was used: certificates are issued and stored on smartcards and other tokens. This enables different stakeholder to authenticate themselves to sign, encrypt and managed data. The respective crypto and keys is generated and stored by an Utimaco HSM.

“It was a pleasure to work with Utimaco. We chose them for their good track record and the reliable partnership we have had with them“, says Klaus Kraner, Deputy Head of Data Center from SVC Austria.

[2] See http://www.egovernment-wettbewerb.de/gewinner/gewinner-2014.html

About SVC

The Sozialversicherungs-Chipkarten Betriebs- und Errichtungsgesellschaft m.b.H. - short SVC - is a 100 % subsidiary of the Association of Austrian Social Insurance Institutions. The SVC developed and implemented sophisticated IT projects in the field of social security like the Austrian e-card system, the electronic health record system and e-medication system or the web portal of Austrian Social Security Institutions.

With the e-card system, the SVC has laid the foundation for the use of health telematics in Austria and operates Austria's largest high-security data network for Doctors surgeries, pharmacies, hospitals, other health care providers (such as ambulance organizations or bandages) and more than nine million insured. Based on the e-card infrastructure the SVC now develops innovative services in eHealth and electronic health records (EHR). These include the Austria-wide introduction of e-medication, the ELGA portal and electronic prescriptions. In addition, the SVC has taken over the product management, development and operation of the web portal eSV of Austrian Social Security Institutions. For more information, visit http://www.svc.co.at/

About Utimaco

Utimaco is a leading manufacturer of hardware-based security solutions that provide the root of trust to keep cryptographic keys safe, secure critical digital infrastructures and protect high value data assets. Only Utimaco delivers a general-purpose hardware security module (HSM) as a customizable platform to easily integrate into existing software solutions, embed business logic and build secure applications. With German precision engineering, tamperproof Utimaco HSM offers scalable performance with the highest level of physical security and self-defense for hostile environments. For more information, visit hsm.utimaco.com