Case study

NASK – DNSSEC Implementation

A safer internet: Poland in the lead

The research institute NASK is the registry for over 2 million .PL domain names and is determined to make the internet as safe as possible. Next to their co-operation with CERT Poland and their extensive efforts in defeating child pornography, they are one of the first registries in Europe to implement DNS security extensions TLD-wide to prevent attacks such as DNS poisoning or phishing. The research institute sees its role not only in providing technical solutions but also in the education of the market. Thus, NASK is organising conferences where it is highlighting the risks of DNS poisoning and the inevitable introduction of DNSSEC to ISPs, government organisations and scientific institutions.

Simulation and support

The foundation to the easy implementation of Utimaco’s cryptographic solution into NASKs DNS system is Utimaco’s use of standard interfaces and a free software simulator. That makes it much easier for clients to fit the CryptoServers into their IT environment as system operator Zbigniew Jasińsk confirms: “For us, it was crucial that we could run comprehensive tests upfront. That is why we were delighted to use the free software simulator. The full hardware that Utimaco’s engineers shipped over enabled us to thoroughly test and prepare our IT environment.”

The implementation of cryptographic hardware solutions in highly individual systems often requires individual support from the vendor: “Basically, we decided to go for Utimaco because they wanted to cooperate with us. But also because their SafeGuard CryptoServers are – apart from very small adjustments - exactly what we were looking for”, says Artur Piechocki, Head of NASK’s DNS Division.

Security, speed and storage capabilities are the keys to success

NASK approached Utimaco with very specific requirements for hardware security modules regarding security, speed and storage that were all met by its SafeGuard CryptoServers.

In terms of security, NASK’s greatest worries were that the keys may get tampered with or even stolen and – moreover - that tampering could occur undetected. That is why the system had to fulfil physical tamper resistance and it had to support RSA keys of more than 2048bit key length which- as a side effect - also provides greater investment security for the future. Both criteria, key length and physical tamper resistance, are met by FIPS 140-2 level 3 certified SafeGuard SecurityServers SE1000 LAN. The technical manager of the DNS team, Krzysztof Olesik was pleased to see that his request for an interface that allows encrypted data transfer through Secure Messaging was met by the PKCS#11 cryptographic interface that is specifically designed to support transactional processes. The fact that the PKCS#11 library is very neatly implemented made the implementation much quicker and hassle free.The implementation: hardware to secure the end-to-end process of music recording

In case of major security breaches NASK would have to immediately re-sign and verify all 2 million domains. That is why they were testing Utimaco’s SafeGuard CryptoServer particularly in terms of speed performance and were pleased to see that it can all be done in less than one hour. The engineers were furthermore convinced by the performance of Utimaco’s CryptoServers that comfortably run NASK’s short cycled dynamic updates every 5 minutes.

Another prerequisite to the solution was internal key storage, which is an advantage of centralised hardware solutions over software solutions. The key storage capacity of the SE1000 LAN devices of the German crypto specialists has proven easily sufficient in the thorough tests of the registry’s project team.

SafeGuard CryptoServer highlights for DNSSEC implementation

- highest security and tamper resistance against unauthorized physical access
- certified compliance with FIPS 140-2 level 3 and 4
- relieves DNS servers from performing complex cryptographic calculations by transferring them to the hardware security module
- support for popular DNS servers and DNS signers such as BIND and OpenDNSSEC
- scalable to a range of needs and therefore cost-effective
- fast implementation process with the aid of Utimaco’s HSM deployment simulator – creates low investment risk without hidden consequential costs

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.

Visit https://hsm.utimaco.com/ for further information.

About NASK

Naukowa i Akademicka Sieć Komputerowa (NASK) is a research institute and the Polish national Registry for .pl country code Top Level Domain (ccTLD) and ENUM numbers under 8.4.e164.arpa. Is also a leading Polish data networks operator which connected Poland to the Internet in 1991. NASK as the research institute conducts scientific and research and development activities in the area of security, reliability and efficiency of the ICT network. In the framework of NASK there is CERT Polska team that is dedicated to respond to security breaches in the network.

The main task of NASK as the national Registry is to maintain a database of .pl domain names (currently over 2.1 million), which are registered and served mainly through more than 170 partners who have signed an appropriate agreement with NASK. NASK is one of the world's first national Internet domain registries to obtain the ISO 9001:2000 certificate covering the entire Internet domain registration and maintenance process.

Visit https://www.nask.pl/nask_en/ for further information.