Nils Gerhardt

Chief Technology Officer of Utimaco

Utimaco follows the maxim of creating solutions that build trust in today's digital world. These include its Hardware Security Modules (HSMs) for cryptographic process management.

We spoke with Nils Gerhardt, CTO of the company, about this technology and its evolution; he stresses the need for these solutions to be accompanied by certifications, such as Common Criteria.

Apart from this, the big challenge for HSMs and other solutions will be to adapt them to the needs of quantum computing once it is in widespread use.

"Governments and businesses should start to use post-quantum cryptography"

By Enrique González Herrero
Photos: Utimaco

The Spanish company Realsec was acquired by Utimaco almost two years ago. What does this acquisition mean in terms of technology?

Realsec's HSM (Hardware Security Module) portfolio is highly valued by its customers. As part of the Utimaco group, Realsec has added to the expertise of the Utimaco team its experience in the fields of cryptography, as well as in the development of encryption, digital signature, PKI and cybersecurity solutions for blockchain and the Internet of Things (IoT).

With this acquisition, Utimaco increases its sales, adds talent and expands its offerings in HSM, data protection, key management and identity management.

What features and capabilities do the company's HSM solutions have?

As a leading cybersecurity provider, Utimaco offers a wide range of HSMs for general, payment and additional use cases. Our portfolio serves all industries by meeting a wide set of different requirements and certifications. In doing so, we enable our customers to safeguard their business by protecting their data, communications, infrastructure, information and business systems based

"Certifications such as Common Criteria,NITES,FIPS,PCI or eIDAS provide the necessary confidence"

on a certified combination of hardware and software to protect key material and sensitive processing.

In addition to these cryptographic hardware technologies, what other cybersecurity solutions does Utimaco have?

If you imagine a smart city and all the exciting situations in which everyone's life would be influenced by digitization, it becomes more than obvious that those use cases need to be secured. This is where Utimaco excels, in providing the root of trust for the digital society. Utimaco offers a range of solutions from key management, data and cloud protection and identity management to critical event management for the complete protection of all those living in an increasingly digital world.

Knowing that customers have different needs, Utimaco offers everything from reliable products, solutions and services to certified data centers.

You recently spoke at ICCC22, held in Toledo, about the importance of HSMs having Common Criteria certification. Why do you consider this certification so important in the application of this type of hardware?

Common Criteria (CC) is a very important certification for various industries, as it enables mutual trust between interacting parties in their cybersecurity solutions.

At ICCC22 I highlighted the benefits of CC for governments facing the challenge of digitizing internally and externally, interacting with other governments, citizens, businesses and their employees. Naturally, this requires maximum security.

Certifications such as Common Criteria, NITES, FIPS, PCI, or eIDAS, in their respective markets, provide the necessary confidence.

HSM already has cloud versions, it is not just an *on premise* solution. What are the benefits and for which type of companies is one or the other model recommended?

With the adoption of cloud technology across all industries, cloud-based HSM offerings are becoming increasingly important. There is no general recommendation for specific companies or organizations to use HSMaaS. It always depends on each organization's specific objectives and scheme.

With our HSMaaS portfolio we offer our customers the possibility to choose the deployment option that best suits their needs. For example, our u.Trust Anchor HSM, which has been CC certified, NITES and FIPS certified and submitted for PCI, is the only one of its kind. It can run multiple tenants, multiple functionalities and different certifications on the same hardware, totally separated and protected.

It is therefore ideal for providing trust as a service. For example, a cloud service provider can use u.Trust anchoring to serve a multitude of customers, scaling up and down and providing different applications. Similarly, IT departments (e.g., in Public Administration) can provide segregated services to different divisions.

For those customers who do not wish to operate the solution *in situ*, *Trust as a Service* is a great alternative for optimizing total cost of ownership, gaining scalability and flexibility. Customers can simply connect and rely on the systems already in place in a secure and reliable way.

Interestingly, there is no one type of customer preferred *as a service*. Utimaco serves customers from different industries and volumes. However, some sectors, such as energy, mobile networks or governments, still rely on *in situ* installations. This often has to do with the regulations in force.

What is the added value of having Hardware Security Modules aligned with the European eIDAS regulation for electronic identification, authentication and trust services?

Europe has created some very good regulations that have received worldwide recognition and have inspired their application in many other countries, regulating aspects such as data protection (through the GDPR), open banking (PSD2) and electronic

identification and trust services (eIDAS).

As Common Criteria, eIDAS is an enabler of trust between the parties involved. It can be used, for example, for the issuance of passports and identity documents, as well as for legally binding cross-border business transactions in Europe, by providing qualified electronic signatures and time stamping. It is essential for the transition from paper-based to electronic processes and, with the use of HSM, provides the necessary security, reliability and traceability, as well as long-term archiving.

With our offer we contribute to secure digitization in Europe and worldwide.

The possibility of using quantum computing in enterprise environments seems closer and closer, but this will require different and much more robust cryptographic formulas than the current ones. What is your future perspective on this technology in terms of security?

It is very likely that quantum computers will be powerful enough to break the current asymmetric cryptography used for many everyday activities such as email encryption, VPN communication, TLS connections (e.g. to access secure Internet pages), etc. This threat is not limited to a specific industry but poses a risk for any company or organization.

In fact, anyone could store encrypted communications today, and once quantum computers become powerful enough to break cryptography, they will be able to decrypt confidential information. This is why governments and companies must react today and start using post-quantum cryptography, which is currently being standardized.

HSMs are fully equipped and, in fact, already offer post-quantum cryptography (PQC). In addition to deploying HSM PQC and key management technology, there is another important aspect for both enterprises and governments: it is important to understand what data needs to be protected and for how long. Furthermore, taking stock of the cryptography already in use today is equally important for migration strategy and cryptographic agility.

How will Utimaco be able to solve the needs of its customers in relation to quantum computing?

Utimaco already provides extensions to its HSMs, using algorithms that are among the NIST finalists, with new algorithms to be added as they become standardized. Key management and PKI solutions complement Utimaco's offerings.

In general, how can HSMs help to security in the environment of technologies such as 5G or IoT?

HSMs provide the secure root of trust in many industries. In 5G they help authenticate mobile users and secure communication. In addition, virtualization is at the heart of the migration to 5G. Virtualization can also be secured by HSMs.

In IoT, HSM can help loosen production *air-gapping* and provide a secure migration to the cloud. Similarly, they can help to give IoT devices an identity and facilitate secure management throughout their lifecycle.

As a central root of trust, they enable the security of any use case and process based on digital technology.

> "Utimaco stands out for providing the root of trust for the digital society"