AN INTERVIEW WITH

THALES

Future Digital Awards Gold Winner:
Best IoT Security Solution

JUNIPER® RESEARCH

1.1 Mover & Shaker Interview with Thales, Future Digital Awards Gold Winner for Best IoT Security Solution

Juniper Research interviewed Stephane Quetglas, Marketing Director at Thales Digital Identity & Security, in October 2024

1.2 Can you describe your approach to IoT cybersecurity throughout IoT devices and their lifecycles?

As the number of connected devices grows, individuals, their property and their data are increasingly exposed. And, because of this, we are seeing a sharp increase in the number of cyberattacks.

To secure an IoT device, it is firstly important to identify it. Securely identifying a device is fundamental to protecting users and businesses. The identity of the device can be defined and will be available and applicable throughout its lifetime. It is defined at the time of manufacture and will remain available and applicable; this is used as a root of trust. However, the manner in which you authenticate the device has to be adaptable. You need to ensure that you can make adjustments throughout the device's lifecycle, because threats are evolving all the time, and not updating your security increases the risk of exposure. Additionally, credentials of devices can vary – and this is what Thales' ID management is all about.

Through our solution, device IDs are created and managed across the entire lifecycle. We also leverage secure hardware-based solutions, such as eSIMs and embedded secure elements. Regarding security on the network service side, we provide HSMs (hardware secure modules) to protect the device's credentials. Our IoT Security Management solution is built to cover the creation/manufacture of a product, plus its deployment and management across its whole lifecycle.

1.3 How do you address the unique security challenges posed by the growing number of IoT connections and the increasing number of use cases?

Clearly, there are many different use cases in IoT. Not all of these require the same level of security. Therefore, it is important to have a solution that uses modular, end-to-end security processes. This will allow the enterprise to adjust the level of security when designing their solution by applying the security by design approach. For example, if you consider critical infrastructure, such as a smart grid, this is vital and will require a high level of security. However, consider an IoT use case such as a tracking-free parking space. This will not require the same level of security. This is exactly why we want our offer to be modular in order to allow our customers to choose the best approach for their business.

1.4 How does Thales ensure that its IoT security solutions are scalable and adaptable to different industry needs?

Scalability comes from the ability to deliver certified hardware-based products in high volumes and that fit with the requirements of various industries, eg in terms of lifespan or environmental resistance. We draw this capacity from our long experience in manufacturing products that require to handle identities in large volumes, in a secure manner, such as SIM, eSIM and banking cards. Our partnerships with cloud providers and hyperscalers also contribute to the scalability of our approach.

1.5 Can you share some real-world examples of Thales' IoT security at work?

Taking examples from different segments, automotive is an important one. First of all, there is a need to protect the car itself, but telematics is also a prime example of data that needs to be protected to allow for the car to be remotely monitored and its software updated. If there is a breach, someone could tamper with the car's software and cause issues for its users. This is an example of Thales' solution at work, as we can secure the module with a specific secure element that provides secure exchanges between the car and the remote management application.

Another example is in the smart grid and smart meter markets. We provide a solution that creates IDs for these devices and implements the necessary credentials needed to add security directly into the device when they are manufactured. At a later stage, we can manage these IDs when the meter is deployed and operational. Additionally, smart-grid solutions must be highly resilient to security threats due to their long lifespan; necessitating the implementation of future-proof measures such as post-quantum cryptography. At Thales, we are proactively developing advanced security solutions to address these evolving challenges and ensure robust protection.

1.6 What regulation trends do you see in IoT security, what impacts are they likely to have, and how is Thales preparing to address these?

Security within IoT has been identified as a challenge for many years. In some cases, players in the market have taken it very seriously for the critical aspect of the business in which they operate. For other IoT applications, security was overlooked too often. But regulation is going to change that.

We have seen several initiatives in Europe, including the additional cybersecurity requirements to the Radio Equipment Directive (RED). The next upcoming regulation is the European Union's CRA (Cyber Resilience Act). This aims to protect every digital element deployed in the European market by adding the requirement to make security updates available for 10 years.

The emergence of regulations around the world is very important as it will create real momentum for cybersecurity standards for IoT devices. It will hold the market to a higher standard and will make enterprises choose better cybersecurity, such as the one Thales proposes.

1.7 Why choose Thales' IoT security solutions?

We have a range of very comprehensive solutions, including services that we can provide for remote management and in-factory provisioning. In the design phase, our solution is very modular, so that we do not have just a single high-security solution. As discussed, having this type of solution wouldn't make sense for all users. Instead, our customers can have a solution that is fully adaptive to their needs. IoT isn't just about cellular technologies, so we don't just provide security to companies using these technologies. This is where Thales comes in.

More information, on Thales eSIM IoT solutions