Trusted security for the global IoT business via secure elements and eSIMs

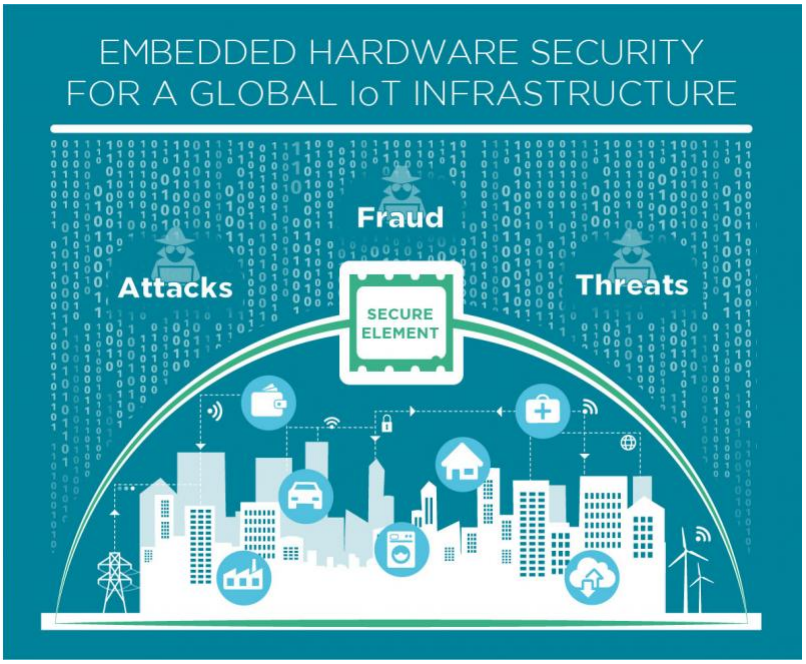
From connected homes to smart cities to global industrial M2M applications: The Internet of Things (IoT) is implemented everywhere, implying in parallel the global implementation of security principles.

 # CONNECTIVITY

POSTED ON 04.12.17

The need for this step is evident: In October 2016 – to name just one example – big DDoS (Distributed Denial of Services) attacks affected 80 major US websites, targeting especially unprotected IoT devices, including internet-ready cameras. These cyber security incidents have been like a global wake-up call about security issues across IoT.

Nicholas Vondrak, Marketing Director NORAM at Safran Identity & Security, contributed to a whitepaper recently published by the Secure Technology Alliance (formerly known as "Smart Card Alliance"), which is announced to be the first in a series to provide an overview of considerations for securing IoT ecosystems. According to the Secure Technology Alliance, the current *"trend indicates that there is an increased need and market opportunity for embedded hardware security in IoT ecosystems,"* depending on the security requirements of the specific IoT application and thus guaranteeing proper authentication and functional access control mechanisms. IoT security encompasses many different aspects of security: secure boot, device authentication, encryption, secure communication, authorized transactions and lifecycle management. Among other things it is particularly embedded hardware security that can deliver significant benefits for IoT environments with critical security requirements – those that require the highest level of confidentiality, integrity and availability and that need to ensure authenticated and authorized access.



> *With a history of providing highly secure platforms for the payment and telecom industries the Secure Technology Alliance and their member companies are uniquely positioned to address the security challenges of the Internet of Things. Embedded security in form of secure elements and eSIMs are one component that can be integrated within IoT devices to deliver a higher level of trust. When combined with secure applications, device personalization and provisioning a secure ecosystem can be established.*
>
> Nicholas Vondrak

Please click **here** to download a full copy of the whitepaper.