White Paper

Hardware Security for Smart City & Smart Nation Concepts

Introduction

For more than a decade, local and national governments around the world are investing in "smart" initiatives – digital, intelligent, innovative & sustainable. Two major trends have been driving this development since the late 20th century: urbanization and digitalization.

People are increasingly moving into bigger cities, looking for better infrastructures, education, well-paid jobs and overall higher living standards. An estimated seventy percent of the world population will be living in big cities by 2050 (OECD Environmental Outlook to 2050, 2012). Not only cities need to ensure they can accommodate and adequately provide for all these additional citizens, but they need to actively compete for attracting businesses & a qualified workforce to foster sustainable economic growth.

With numerous benefits for citizens and cities, there comes a long list of challenges as well:

- Increased traffic congestion
- Pollution & waste disposal, with a yet incalculable health impact
- Day-to-day management and maintenance of public and urban services, such as transportation, education, health care or recreation infrastructures
- Availability of water, gas and other natural resources, including a high potential for abuse and blackout scenarios
- Public safety and management of emergency services

A brief review of worldwide "smart" milestones

Back in 1999, Singapore became one of the first cities to be recognized for their smart initiatives. The Intelligent Community Forum awarded Singapore with their first Intelligent Community of the Year Award for the Singapore One project, which aims at providing high-speed Internet to every business and citizen. In the meanwhile, Singapore is in the midst of implementing an extensive and ambitious "Smart Nation" concept.

Up until 2016, numerous other cities and communities have received this award, such as Taipei (Taiwan), Waterloo (Canada), Stockholm (Sweden) or Eindhoven (The Netherlands) to name just a few. R&D & innovation, large-scale urban (re)development programs, traffic improvement and renewal of overall infrastructures have been decisive criteria for the award jury.

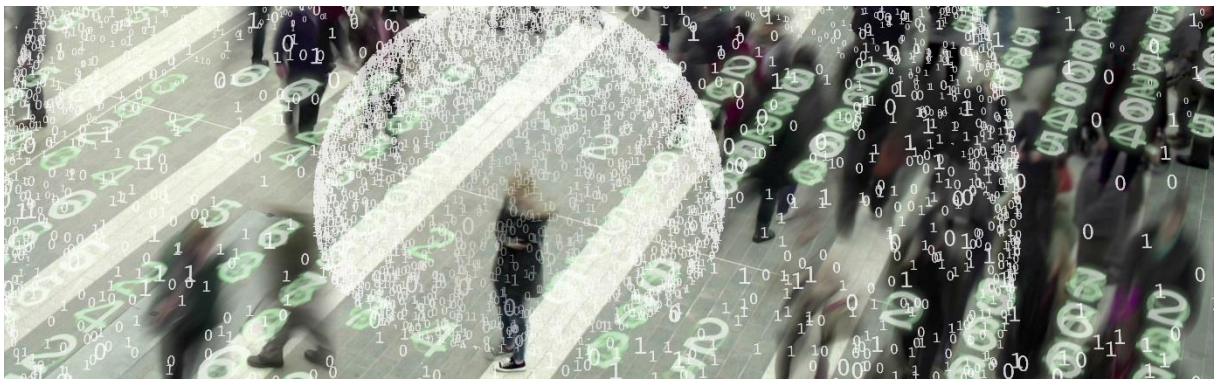
Forbes in turn names Barcelona and New York City among the top five smart cities in the world, among others for their environment and smart parking, respectively smart street lighting and traffic management (Forbes, 2015).

The simultaneous, rapid evolution of information and communication technologies contributed to an exponential economic and social development and provides means to address these challenges. But every solution comes at a price – say, additional challenges in this case!

This white paper will look into hardware security used for protecting Machine-to-Machine (M2M) and Internet of Things (IoT) communication in smart city or smart nation concepts. How can one avoid or at least mitigate security risks when everything becomes connected, with machines and sensors in and around everyday life items communicating with each other and their human and non-human environments.

Smart City: Big Data Explosion and the Question "How to keep it safe?"

With technology as key enabler for smart initiatives, data collection in an interconnected world of people, machines and things has become ubiquitous over the past years. Lawrence Miller, Principal Network Architect at Telit IoT Connectivity brings it to the point. "Considering all of the very interesting things that are already being connected, let alone all the things that have yet to be imagined, the number of very intelligent and determined people that will attempt to gain un-authorized access to absolutely everything, for both malicious and benign reason, will multiply rapidly", Miller states (M2M/IoT Cellular Data Security, Telit White Paper, July 2015).



Smart grid, urban logistics, traffic flow improvement, vehicle-to-infrastructure communication (V2X), smart manufacturing (M2M communication), infrastructure management or video surveillance – cross-industry end points collect, store & transmit data almost non-stop, around-the-clock. Cisco estimates a total of 50 billion connected

devices by 2020, twice as much as there were in 2015. Experts predict that annual data collection in 2020 will be 44 times what has been collected in 2009. This equals nearly 35 Zettabyte (ZB, 1ZB = 1,000,000,000,000 GB) of data compared to only 7.9 ZB in 2015 (Infographic "The rapid growth of global data", Computer Sciences Corporation, 2012).

Any endpoint device collecting, storing and using business data or consumer information is vulnerable to an attack. How can governments make sure their own and their citizens' data is neither stolen nor manipulated, which then can involve financial or reputational damage to affected parties?

Hardware Security as the preferred choice for maximum security

This huge network of connected end points with all their collected data needs to be encrypted, end-to-end! And governments and public authorities overall need to ensure this is done properly – either via project specifications when it comes to public projects or via regulations and compliance when privatized or private initiatives are concerned. More precisely, data encryption and device authentication are the right measures to take for protecting critical business and consumer data. However, a crucial first step is to create and store the cryptographic keys that lock and unlock this data.

Software solutions vs. hardware solutions

Where data needs to be secured – whether structured or unstructured, in use, in transit or at rest – data encryption is required and as a consequence cryptographic methods and keys. Cryptographic keys can be generated and stored using different solutions and the choice between these alternative solutions depends entirely on the value of the data and the feasibility & likelihood of an attack. Software solutions store keys in main memory, together with the data, which means the system administrator or anyone else with server access may create an extra key to get hold of the presumably secure data.

Compared to software solutions, hardware solutions such as hardware security modules (HSMs) offer maximum security even in the most hostile environments. The module can detect an attack when it is happening, including drilling, overheating, power blackout or chemical attack, and automatically initiate immediate deletion of cryptographic keys. In comparison, software-based keys can be captured in the moment of unlocking – offering attackers the ability for side channel attacks by studying the software, exploiting vulnerabilities and running attacks remotely.

The source of true security for cryptographic keys is creation and storage within an HSM as no one else will ever be able to recreate or access the key and the data. Utimaco, as leading HSM manufacturer, provides the highest possible flexibility combined with the most stringent security controls in place through a unique general purpose HSM, without backdoors.

With a FIPS 140-2 Level 3 (tamper evident) or Level 4 (tamper resistant) certification, HSMs are ideally suitable for use within Smart Nation environments. In this context, cryptographic devices are not always located inside highly secured datacenters but might as well be integrated into more accessible infrastructures. A FIPS 140-2 Level 4 physical security certified HSM can be of interest here as it provides highest resistance against physical attacks.

Application scenarios using HSMs

While data(-base) encryption and access rights management give access to sensitive data only to a predefined and authorized set of people, a public key infrastructure (PKI) ensures the identification and authentication of devices, components, sensors and users. The authenticity of each device or component in the network is verified and confirmed by the HSM. Also, software and data transferred from the device manufacturer or in between devices is checked for integrity. In summary, a device only receives software and data with proven source that has not been altered or manipulated while being sent. And the date transfer will only be processed if sending device (e.g. a manufacturer server) and receiving device have been clearly identified as the devices they pretend to be.

Securing the Smart Grid – An Example of Smart Nation Challenges

One pioneering application area for hardware security within the smart nation is certainly the smart grid and smart meters. Energy infrastructures are widespread, vulnerable and a strategic target for cyber-attacks – which is why they need to be protected.

A major difference exists between the US and the German (EU) approach to smart grid and smart metering. While the US approach focuses on the smart grid security (US policy described in 42 U.S.C. ch. 152, subch. IX § 17381), the German and EU approach is rather centralized around smart meter security (Smart Grid European Technology Platform).

From the traditional grid to a smart electrical grid

Motives for the evolution from traditional to smart grid are manifold:

- Integration and management of decentralized energy production sites
- Energy efficiency with less need for spare capacities
- Increased stability and reliability of the grid including load balancing and management as well as the connection and disconnection of large-scale consumers
- Remote (dis)connection, inspection and maintenance, reducing operational costs for grid users moving from one address to another or for implementing legal measures

But there comes risks and challenges too: from sabotage and manipulation to blackmailing and the threat of a partial or complete blackout. Preventing these threats requires awareness creation, and educating those in charge of network and data security matters.

From the traditional meter reader to a smart meter

Reasons for the installation of smart meters include:

- Correctness of measured data
- Reduced potential for intentional and unintentional human error
- Possibility to offer a more flexible tariff structure

Nonetheless, meter and data manipulation are a permanent risk factor – which is why countermeasures need to be implemented: e.g. anti-tamper mechanisms (tamper

resistance and tamper detection) and verifying the plausibility and integrity of commands. To prevent complete blackouts, authentication of servers, meters and transmitted commands is crucial. Last but not least, data privacy concerns are equally important and require the encryption of measured data, data bases and customer information.

The German smart metering approach is regulated by the BSI technical guideline TR-03109 for smart metering environments which defines requirements to functionality, interoperability and security of smart metering IT components. The focus clearly is on data privacy and the smart meter gateway as central security component within the smart metering infrastructure. More information on TR-03109 and Utimaco available on our website.

Summed up: Encryption & Co. for end-to-end security

For confidentiality and data privacy, encryption with high quality cryptographic keys generated by a true random number generator is essential! Together with digital signatures for integrity, authenticity and non-deniability of data and a Public Key Infrastructure (PKI) for unique identification of devices, end-to-end security can be ensured.

2020 onwards – What does our smart future look like?

From autonomous cars and other means of transportation to smart homes and enterprises – the number of connected endpoint devices will continue to grow. An unimaginable amount of business and consumer data is to be collected, stored and used over the coming decades and in consequence needs to be protected against vulnerabilities and all kinds of attacks. Activities of daily human life will become automated, industrialized and detached from the human being they are originally related to, often losing the need to human intervention altogether.

Considerations on how to incorporate security measures and data & privacy protection into smart nation end-points have to start now! Let's make sure that this unstoppable change is based on a sophisticated security concept.

Sources
http://smartcitiescouncil.com/resources/white-paper
http://www.uniassignment.com/essay-samples/information-technology/the-history-of-smart-cities-concept-information-technology-essay.php
http://www.intelligentcommunity.org