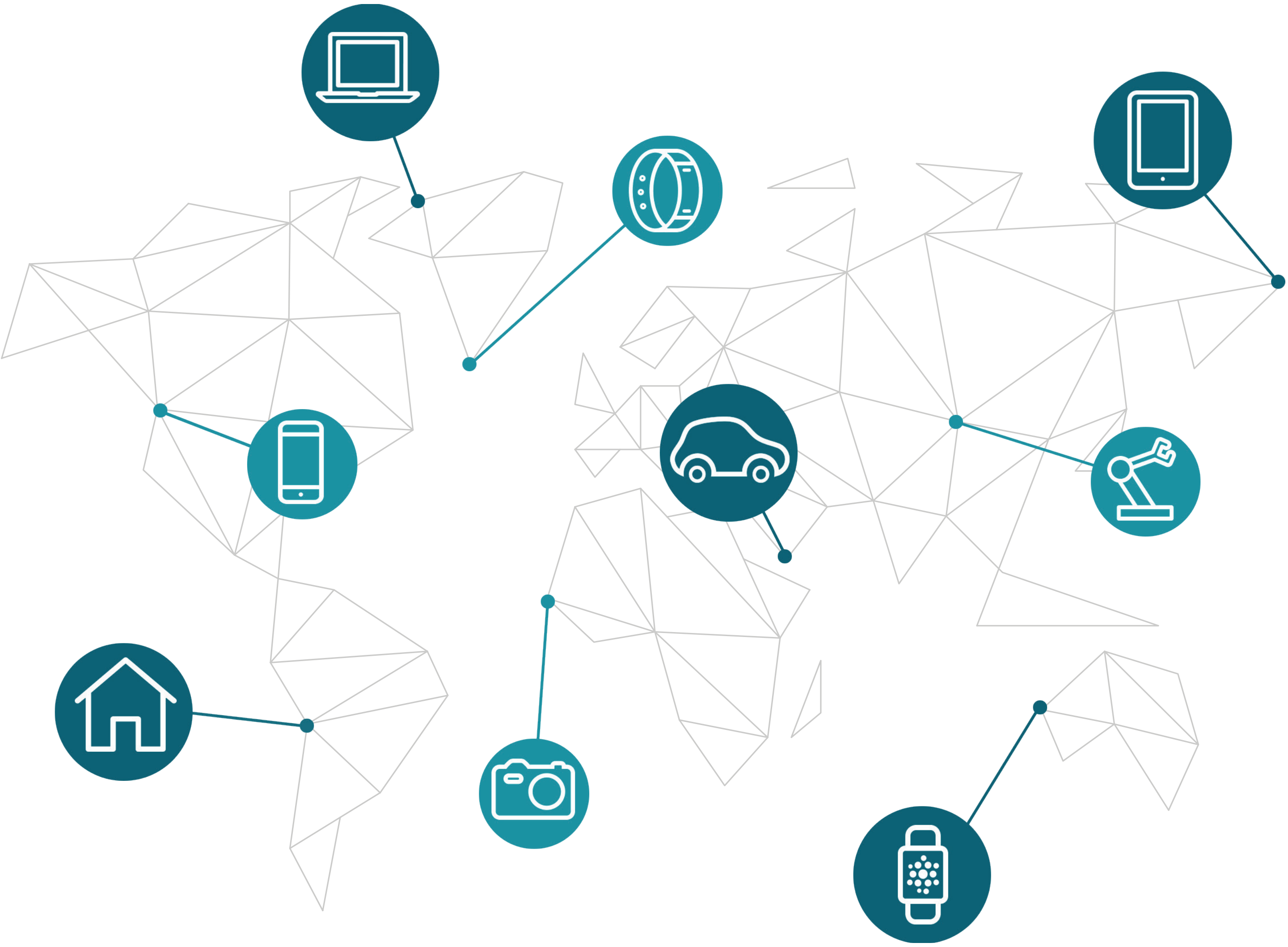
A white paper by Transatel

SECURITY FOR THE IoT



Why is it important?
What are the solutions?

2017

Executive Summary

The current enthusiasm for connecting objects hasn't brought about a corresponding concern for security issues. It's even more surprising when tales of massive data hacking abound. Data theft or device hacking within the IoT ecosystem could lead to dramatic outcomes—and not only in the virtual world.

Every IoT program today should, in fact, have security as a priority.

This white paper explores solutions to identify—and thereby, secure—a device through strong authentication, and to protect data transmission via a Secure Private Network.

Transatel's SIM 901 leads the way in both authentication and global network management. For this reason, it's one of the rare solutions today to offer true end-to-end security for the IoT.

True IoT security

Strong device identity based on hardware + Secure connectivity

CONNECTING WITHOUT SECURING IS HAZARDOUS

The Internet of Things (IoT) is the new telecom revolution. The number of connected ‘things’ is expected to reach 50 billion by 2020, using a large range of connectivity options.

Why do we want to connect things?

The reasons are simple: more services, better control, greater efficiency, and process optimization. When everything is connected, and communicating, things work together. It becomes possible to collect, share, analyze and control data to better manage our homes, our cars, our health, and our environment. From an industrial point of view, it’s an essential part of the 4th industrial revolution, allowing higher systems performance, cost savings, and new revenue streams.

What about data security?

We’re all aware that massive cyber-attacks are taking place in the digital world, with critical consequences such as theft, loss of privacy or ransom. Well, if you believe these threats are important, just imagine how harmful they could be if they occurred in the physical world.

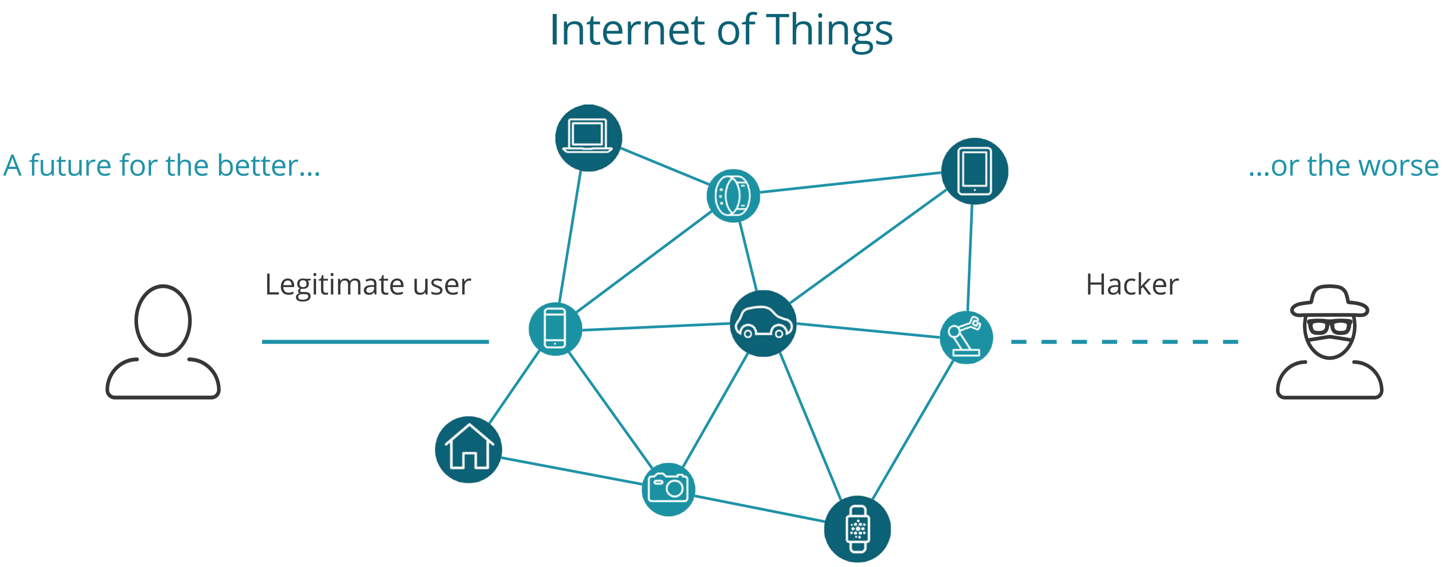
Imagine you’re in your car, driving on the freeway, when suddenly the air conditioning blasts cold air, the radio switches to another station, and washer fluid streams down the windshield. The situation goes from annoying to terrifying when there’s no reaction from the accelerator and the brakes go dead.

This example is not hypothetical*. It happened in 2015, in a publicly organized e-carjacking of a Jeep Cherokee, by two hackers, Charlie Miller and Chris Valasek. They hoped —and managed— to demonstrate that vehicles’ electronic systems, which are part of the IoT, are vulnerable. Shortly after this event made the headlines, Fiat Chrysler issued a safety recall for 1.4 million U.S. cars and trucks that involved a software update to patch the vulnerability. This example alone should serve as a wake-up call to manufacturers and systems integrators, no matter the device.

Without security, the IoT can bring about a disaster

Think of a hacker taking over the country’s energy grid, or a hospital’s glucometers, heart rate and blood pressure monitors. Even devices thought to be ‘non-critical’, when hacked, can have dramatic outcomes. The Mirai botnet attack, responsible for shutting down the Internet in the US during a few hours in 2016, is a good example of this vulnerability. The attack was made possible by infecting non-secure devices, such as baby monitors or home-monitoring cameras.

*https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/



The challenges in implementing security

Even today, the IoT market is still extremely fragmented. Just within the consumer IoT ecosystem, there exist several competing platform providers, many of which are incompatible, impeding devices' interconnection. The situation is identical within the Industrial IoT sector, with the added complexity of multiple organizations simultaneously trying to define specifications for IoT interoperability.

As for security, the questions as to 'where to start' and 'how to implement' a strategy are even greater. There are no general standards or architectural principles adopted as a reference for IoT Security. Many groups are attempting to address the issue, but this is still in the early stages and non-interoperable.

HOW CAN WE BEGIN TO SECURE THE IoT TODAY?

As for company security, the IoT needs a layered approach, one that can adapt as new challenges arise.

A 'strong identity' for things

Security in the IoT starts with strong 'things' identities. With strong identity, things can be authenticated when they communicate with other things, services, or users.

Strong identity allows us to address core security requirements, such as:

- **Trust / Authentication:** when things are authenticated, trust is established between endpoints and secure communications can be ensured.
- **Privacy / Confidentiality:** depending on the device, personal or sensitive information is generated, collected, and shared. With strong identity, this data can be protected and remain private.
- **Integrity:** interpreted as the integrity of the data being transmitted from/ to the device, but also the integrity of the device itself. With strong identity, we can ensure that software code and firmware is legitimate.

The Public Key Infrastructure (PKI)

One established and standard security technology that can be used to protect the IoT is the Public Key Infrastructure (PKI). This technology is like the one you use on e-commerce websites to authenticate your bank account online. In a PKI, asymmetric cryptography, using private keys in combination with certificates, allows users to identify themselves over an electronic network, to communicate privately, and to sign electronic documents. These features can be re-used in the context of the IoT. In particular, a PKI allows the provision of a unique 'strong identity' to each thing via certificates.

The core security enablers are thus ensured with a PKI. And because it's an established technology, it can be implemented today and easily integrated to work with other components of a global IoT Security solution.

Industry preference for a PKI

Using a PKI in the IoT has been acknowledged as the preferred direction by the main IoT cloud platform providers. For example, Amazon Web Services is now mandating the use of a PKI to ensure mutual authentication between a device and its IoT cloud.

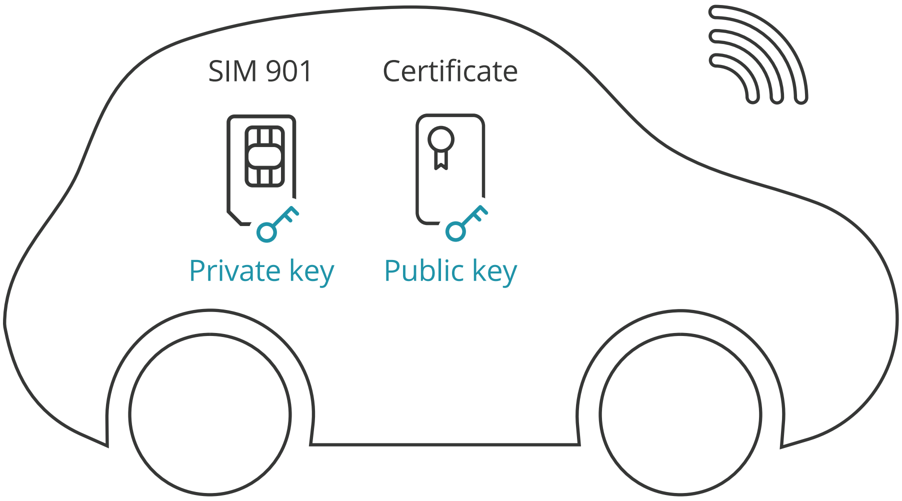
The challenges of a certificates-based system for the IoT

The security of a certificates-based system used in a PKI relies on the well-guarded secrecy of the private key. Thus, the primary challenge for an IoT service provider is to securely provision, protect and manage the private key and associated certificates within the device. This is not an easy task.

Asymmetric cryptography explained—a set of keys

In asymmetric cryptography, a pair of keys (private & public) is generated, and then associated with an identity. The association is made via a certificate signed by a trusted Certificate Authority.

When a device needs to prove its identity, it receives a challenge from the other endpoint. It then signs the message with its private key. The other endpoint checks the signature, thanks to the device's public key. That's why it's crucial for the security of the entire system that the private key never be disclosed.



First, the private key must be securely stored within the device. A typical implementation is to rely on the application software in the device, or on some storage functions provided by the underlying OS. But it is well known that software implementation can be hacked.

There are several ways to enhance the security of private keys, but the best solution to date is to rely on a separate and specific piece of hardware. Such hardware is called a 'secure element' and is dedicated to the secure storage and execution of cryptographic operations.

For example, Apple is using a secure element in the iPhone to secure ApplePay, and Samsung is using one for its Knox services. Chips also play the role of secure elements in bankcards. While still quite specific, the notion of secure element is well defined and standardized by the GlobalPlatform consortium.

What is a secure element?

A secure element is a tamper-resistant device (a physical piece of hardware with specific protection against attacks) allowing secure storage of sensitive information, as well as secure execution of cryptographic operations. Its security level can be assessed and certified with reference to international standards known as Common Criteria.

Secondly, the generation, handling and provisioning of private keys must also seriously be taken into consideration. If private keys are generated externally to the devices, then a secure process must be established to provision them within the devices. This can be a difficult problem, as it means you must be able to trust the entire chain, and configure each device with different credentials. When possible, it's preferable for the private-public key pair to be generated within a secure part of the device itself. Once again, the secure element demonstrates its superiority with regards to onboarding key pair generation and key distribution.

Thirdly, a reliable mechanism enabling the secure management of keys and certificate lifecycles must be put in place. For security reasons, certificates have limited lifetimes, and if compromised, must be revoked, and then replaced. Thus, it's important to be able to manage them in a secure and independent manner.

Dedicated offers for secure elements do exist, such as new pieces of hardware to solder within a device. But then, two issues arise. On the one hand, the secure element brings an extra cost to the device, and on the other, it has no independent communication capabilities.

Luckily, if your device is using cellular connectivity—whether it's the current 2G/3G/4G or soon-to-come cellular LPWA such as NB-IoT, EC-GSM or LTE-M—**then it so happens that you already have a secure element in your device, which is the SIM card.**

Hardware is the best protection

The SIM as a secure element

A SIM is a telecom application on a smartcard, allowing authentication on a mobile network. It's a secure element in and of itself. Moreover, it holds some secure end-to-end communication capabilities (known as SIM OTA), which allow the remote management of its lifecycle and content. In particular, there's no need for a pre-established IP connectivity to communicate with a SIM.

With a SIM, you benefit from the perfect security toolbox—there's no need for additional, costly hardware. Furthermore, a SIM benefits from remote management capabilities via the cellular network.

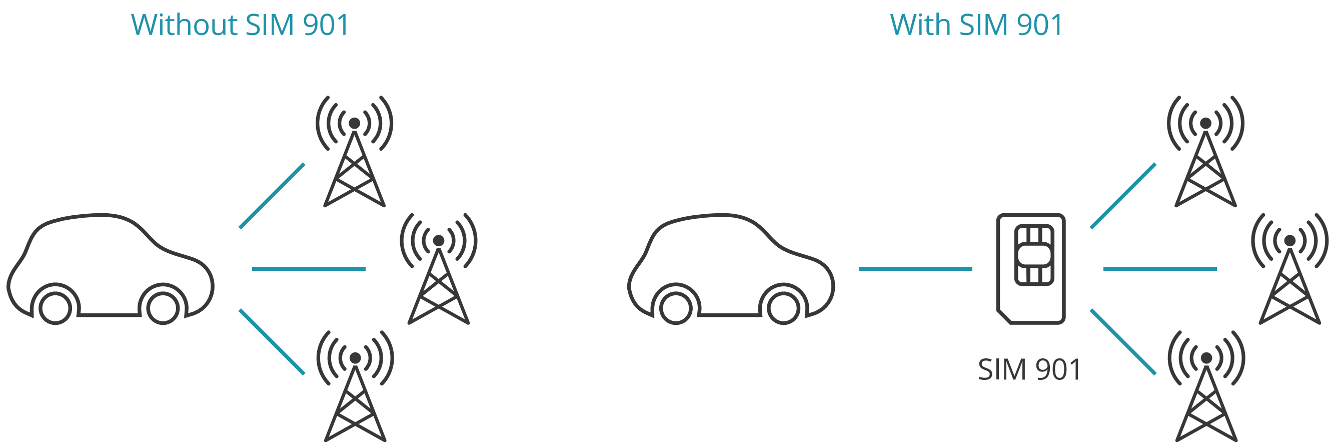
However, in practice, it's often impossible to use the SIM, as the latter is the mobile operator's property. In general, the mobile operator doesn't share this element. Even if the mobile operator did grant access to its SIM, any solution put in place could only work with that specific operator.

This is where Transatel's SIM 901 makes a difference. SIM 901 is a cellular connectivity-enabling platform, which provides cellular connectivity services as an added layer on top of any mobile network. The service acts as a virtualization layer helping the IoT service provider benefit from the SIM as a secure element, once and for all, no matter the underlying radio access network.

Transatel has developed a set of software and services hosted both on its physical SIM 901 card and on its global connectivity enabling platform allowing customers to benefit from this inherent security advantage.

As an example, Transatel has designed its SIM 901 to be able to securely connect to IoT platform providers such as Amazon Web Services.

SIM 901 and the virtualization layer



Without SIM 901

With SIM 901

A Secure Private Network

The second recommended approach in an IoT security strategy is to ensure data security on the transport layer. Even if the application-level security detailed above is important, it's equally advisable to reduce the surface of vulnerability by ensuring that IoT devices are not using the public Internet, but rather, a private network.

Moreover, establishing an SSL/TLS or VPN secure connection on a non-secure transport layer is sometimes complex or even impossible, considering the restricted environment of an IoT device. The process also generates additional data traffic on the air interface, which comes at an additional cost.

The APN secures communications on the transport layer

Cellular networks are secure because devices and users are given a dedicated APN (Access Point Name) to access the network. The APN is an identifier that enables devices to connect to a network. The network can be the public Internet, but also a private network. The authorization to use an APN is granted and managed centrally by the mobile operator.

However, the APN is operator-dependent

An APN is operator-dependent. Any IoT strategy relying on an APN is therefore complex to implement globally, as it entails replicating the system in every single country individually, with potential risks such as loss of consistency and disaggregation.

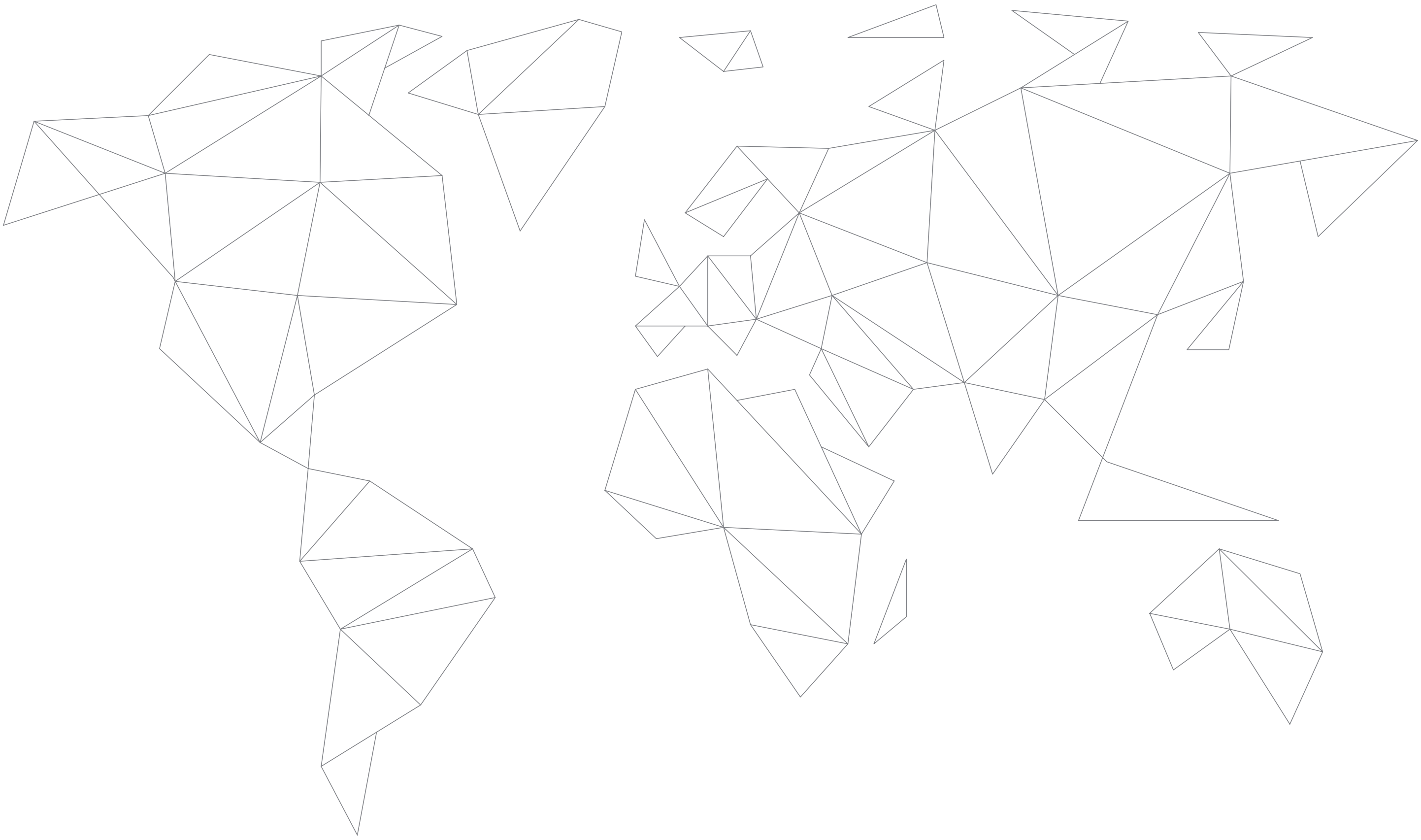
Introducing the global, virtualized APN

Thanks to a virtualized core network, Transatel's SIM 901 lets you benefit from the same APN worldwide. SIM 901 is carrier-agnostic and therefore independent from underlying cellular networks.

SIM 901 is the unified, single, global solution for IoT security

Transatel's SIM 901 is network-agnostic. Only a single integration is necessary to enable communications whatever the country. This ensures consistency, simplifies coordination and logistics, and offers a single point of control for operations and devices globally.

SIM 901 gives IoT players access to the security advantages inherent to cellular networks: transport network control and SIM hardware security.
SIM 901, therefore, ensures a truly secure Internet of Things.



CONTACT US

info.901@transatel.com
www.transatel-sim901.com

Security for the IoT © Transatel 2017