Secure Data Acquisition, Communication, and Processing for Your IoT Solutions

Guidelines for Ensuring a Successful Implementation
INTRODUCTION

Secure the Internet of Things – From Devices to Networks and Platforms

From smart light bulbs illuminating smart homes to smart cars racing across smart cities, the Internet of Things (IoT) is making its mark in how we live, work, and play. Businesses need to stay ahead of the game by operating with a comprehensive, cutting-edge deployment that can handle this highly competitive landscape. And it all comes down to one critical factor: security.

Connectivity and a vast array of devices are enabling businesses to achieve unimaginable things. In fact, Gartner estimates that the number of connected devices is currently closing in on 8.4 billion and will possibly exceed 20 billion three years later.¹ However, Gartner also cites that over 50% of all IoT projects are expected to expose sensitive information in 2020 due to the failure of hardware security, a significant increase from less than 5% in 2016.²

Because of the recent boom in adoption growth, connected devices are becoming an attractive target for cybercriminals and amateur hackers. And as devices become less reliant on subscriber identity module (SIM) cards to identify users and authenticate authorized access, IoT security management will be more complicated.

One of the first steps to keeping your devices – and operations – safe and secure is to understand the three pillars of IoT security:

- **Data acquisition**: Every object that gathers information is a valuable asset. It is essential to ensure devices cannot disclose data to unauthorized parties.
- **Data communications**: Information has value when it is accurate. Devices need a layer of security that prevents data manipulation and modification by the unscrupulous.
- **Data processing in the cloud**: Devices have no value if the right people cannot access the data captured at the right time. Businesses need a platform that allows authorized parties to access information, when and where it is required.

Executives cannot prepare to defend their operations if they do not know what they are protecting. In this white paper, we’ll explore the three fundamental levels of IoT device security and offer advice on how you can overcome the impending cybersecurity threats while maintaining the agility you need to gain a competitive advantage.

---


---

About Telit
DATA ACQUISITION

Reshape the Storage Landscape for Internet of Things Data

For years, a wide variety of devices connected across cellular and wireless networks were dependent on SIM cards to establish secure access to operator networks. From handsets and smartphones to machine-to-machine sensors, wearables, and tablets, this technology played two critical roles:

1. **Identity:** A unique reference number identifies the SIM card in the device. The cellular network then recognizes the reference number and allocates associated incurred costs.

2. **Authentication:** This form of mutuality occurs when the cellular network uses a security mechanism to validate the identity of the SIM and grant access and the SIM authenticates in a similar way to the network.

In the world of IoT, we have adopted the traditional SIM for identity because it was already there. However, the security of devices or things is changing. As the IoT markets and wireless technology standards are evolving, we see the physical SIM beginning to take a more software-centric nature – where the SIM functions are directly embedded into the device, as is the case for eUICC and iUICC. This direction introduces new threats that must be addressed by the eco-system players such as SIM vendors, module vendors, OEMs and mobile network operators [MNOs].

Businesses reliant on IoT devices will need to reassess the fundamental aspects of operating secure IoT operations:

- **Storage of device credentials:** In this changing world, an IoT device or thing must provide secure data storage. Thus, credentials need to be stored in the device’s storage or in specialized chips with the highest level of security.

- **Communication exchange with third-party providers:** Because credentials are encrypted and exchanged across a cellular network with the added layer of hardware monitoring identification and authentication, operating systems are more likely to be hacked, leaving the operator profile open long enough to be threatened.

- **Management of the cloud subscription:** When moving information back and forth, users will have the flexibility to change their subscriptions to cloud modules on an as-needed basis. However, this does present a challenge in the entire data management lifecycle — from storage and encryption to exchange and access.

- **End-to-end security:** As the physical and software aspect of SIMs converge, it is more necessary than ever to ensure security not just within the network, but throughout the entire data collection and delivery process. This requires a level of awareness of the data volumes and user access loads experienced in operations today, as well as expected activity in the future.
DATA COMMUNICATION

Transition Data Communications to an Integrated Network

At the heart of the IoT is data communications and the connectivity that enables it. The strength and continuity of this network in which devices are exchanging information around the clock are only as dependable as the MNO. As SIM cards leave behind their past as a separate unit from the device module, businesses can take advantage of complete solutions, tighter integration between captured data and module exchange, and a centralized platform. And no matter where the module is placed and transferred at a later time, that module remains connected.

As more devices are introduced into the IoT network, MNOs will eventually reach a point where they cannot handle all the data traffic. As a result, businesses will experience operational latency, dropped connections, and increased vulnerability to unlawful surveillance, retrieval of information, and hacked machine performance.

With massive deployment of vulnerable IoT devices and connected gadgets and growing volumes of data exchanged over unprotected cellular and internet networks, IoT security is a significant concern.

Businesses should consider taking four crucial steps to ensure device connectivity is secure and agile:

• **Plan the cellular connectivity:** Define KPIs – including access technologies, roaming agreements, quality of service (QoS), cost, and customer support – and benchmark your potential communication service providers. Investigate local regulation to understand permanent roaming. Use dedicated APNs and VPNs to secure data in transit.

• **Scale lower power wide areas (LPWA) devices:** Leverage LTE standards such as Category M1 and NB1 to support devices, such as sensor net nodes, and achieve critical cost and size targets, while improving the ease of installation and manufacturing.

• **Embrace continuous security updates:** Employ the help of a device provider to evaluate security risks on a constant basis and meet security criteria set by MNOs globally.

• **Optimize global interoperability:** Reduce the cost of IoT data plans with the flexibility of bringing together multiple network carriers into one contract based on simple terms.

"Considering all of the very interesting things that are already being connected, the number of very intelligent and determined people that will attempt to gain unauthorized access to absolutely everything will multiply rapidly."

- Alon Segal, CTO, Telit
DATA PROCESSING IN THE CLOUD

Strengthen the Data Management Platform in the Cloud

While data acquisition and communications are important factors for running a highly operational IoT program, neither of them deliver any real benefits until all devices are connected and data is brought seamlessly and quickly to a centralized platform. It doesn’t matter how fast the platform can receive, process, and share. If the security behind the platform is weak, the return of every IoT investment is lost the moment a breach of any kind occurs.

From access control management of data acquisition to session management of data communications, a successful IoT platform features multi-layer security and support for data integrity, auditing, and validation. Businesses selecting a cloud platform to support IoT devices should consider features such as:

- **Widespread connectivity management**: Optimize data consumption and cost by implementing a broad range of critical attributes including IoT connection provisioning, data management and auditing, and analytics across wireless networks.

- **Centralized device management**: Manage and secure devices once they are installed in the field, connected through a reliable wireless network, and enabled to operate remotely. Device management from one central location allows dynamic remote configuration, provisioning, and firmware updates of installed IoT devices – all based on parameters defined by the business.

- **High-performing data management**: Ensure the integrity and confidentiality of your intellectual property with advanced data encryption technology and a broad range of functions related to data collection, transport, storage, and delivery.

- **Strong administration and security**: Invest in comprehensive administrative functions from a single, intuitive cloud-based management portal. Businesses can provide multiple security layers to safeguard data, devices, applications, and the platform against external and internal cyber threats. Also, they can manage authenticated access with role-based permissions for all user types and control how and when your staff logs in with smart-session ID and expiration timeout management.

- **Flexible application development**: Innovate multiple approaches to creating dashboards, developing web-based and mobile apps, and integrating with enterprise systems or cloud-based big data analytics to provide input for flexible connectivity and device management functions.

---

US$2 trillion

Global cost of IoT-related cyber crime in 2019, compared to $400 billion in 2015

WHY TELIT

Turn IoT Devices into Effective, Secure Business Outcomes

Protect your IoT data, devices, and infrastructure from any internal and external threat with powerful connectivity, modules and platforms from Telit. Long before the Internet of Things emerged as a buzzword phenomenon, we have been pioneering the world’s most comprehensive portfolio around it for over 20 years.

Demonstrating our commitment to undisrupted IoT operation and innovation, we designed Telit simWISE. Our module-embedded SIM technology allows our customers to give more value to their customers, while reducing the total cost of ownership and improving the connection lifecycle of their IoT deployments worldwide.

Telit simWISE alleviates some of today’s top priorities around IoT-connected devices by helping businesses:

- Overcome design constraints and increase the reliability of next-generation SIM technology
- Reduce logistics costs associated with control, stock, and shipping of pre-provisioned SIM cards
- Utilize remote provisioning to avoid costs of physically swapping of SIM cards
- Enable out-of-the-box management of data and connectivity for distributed devices remotely
- Leverage the latest integrated cryptographic capabilities for superior device security
- Provide a new generation of devices with personalization capabilities through secure state-of-art manufacturing infrastructure
- Facilitate simple global connectivity solutions by collaborating with world-recognized partners and vendors

By combining Telit simWISE with our innovative spirit and over 20 years of experience, deep industry insights, and unmatched IoT technology expertise, your business can ignite and sustain your own vision of profound, secure, and IoT-driven digital transformation.

LEARN MORE

Explore how Telit module-embedded SIM technology can secure your IoT device network and platform. Call your Telit representative today or visit us at www.telit.com/simwise.
ABOUT TELIT

Telit offers the world’s most comprehensive portfolio of high-performance IoT modules, connectivity services, and software. Our innovative spirit, decades of experience, deep industry insights, and unmatched IoT technology expertise is the foundation of everything we do.

We help customers and partners who require best-in-class performance with our uncompromising engineering practices and design methodologies that exceed stringent environmental requirements and industry standards. Our IoT experts have pioneered a successful end-to-end system approach that assures that all the pieces work together seamlessly when connecting “things to apps” – from device management to connectivity and data management and everything in between.

Want to see the next evolution of the SIM?

Telit simWISE™

EXPLORE IT NOW →