White Paper

Freescale Trust Computing and Security in the Smart Grid

By Meera Balakrishnan

freescale.com

Abstract

With the increasing deployment of automated technical solutions in the implementation of automated metering reading (AMR), advanced metering infrastructure (AMI) and smart grid infrastructure, possibilities of security attacks like data hacking, introducing malware in the system and cyber attacks are on the rise as well. Vulnerabilities in AMI devices include non-secure data buses, serial connections or remote access to debug port. The question arises: how can data security and customer privacy in smart meters and smart energy gateways be ensured? This paper talks about how trusted computing helps resolve security issues in implementing the smart grid by providing a clear idea of what elements of the system are trusted—and to what level and why. Freescale solutions that embed trusted computing are also covered.

Smart Grid Domain Interaction

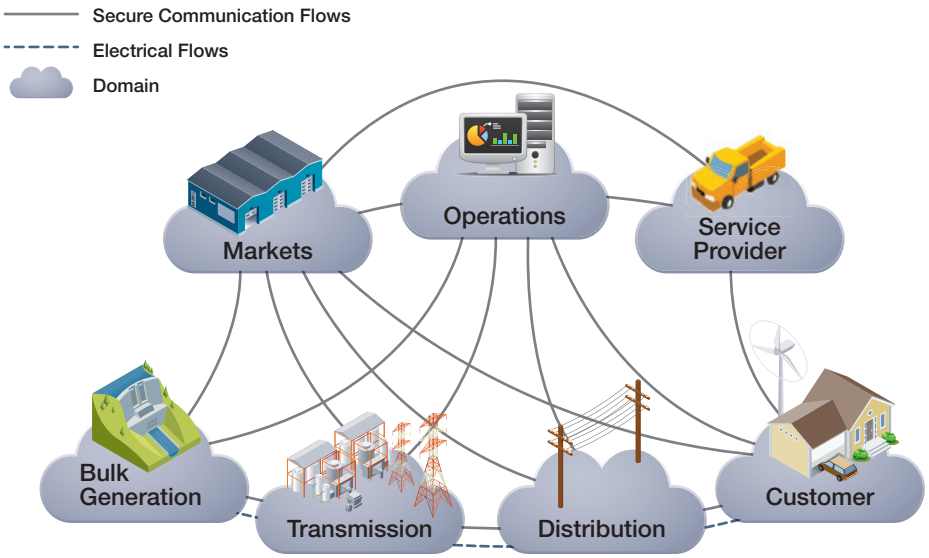


Figure 1: The interactions of different smart grid domains through secure communication and electrical flows. (Source: NIST Smart Grid Framework 1.0, January 2010).

Need for Improved Grid Security

Attacks on computer systems through viruses, root kits, Trojans, worms, keyloggers, bots and other malicious software have been the focus of hackers and cyber security experts for many years. With historically isolated industrial controls such as supervisory control and data acquisition (SCADA) systems and programmable logic controllers (PLCs) connected to the same networks, loss of service as well as physical damage can be caused from unauthorized access. But the goal of the smart grid is network connectivity, so network security is fundamental to its successful implementation.

Recently, the global electricity grid infrastructure has experienced a rapid increase in the number of vulnerabilities. As one of the key assets of any nation, protection from the increasing number of attempted and successful attacks on the grid and its metering systems is a rising priority.

Increasingly, more dangerous attacks have occurred from a variety of sophisticated attackers, including foreign governments. Attackers include state run and financed attacks, hackers, cyber terrorists, organized crime, industrial competitors, disgruntled employees and careless or poorly trained employees. The bottom line is the cost impact can be significant. At the 2011 London Conference on Cyberspace, British Prime Minister David Cameron reported that cybercrime cost the UK an estimated 27 billion pounds a year, and with several other nations as much as $1 trillion a year globally.

As a result, governments around the world are taking steps to ensure increased security and reduce the cost of cybercrime. In the U.S., organizations active in standards and other areas include the North American Electricity Reliability Corporation (NERC) and the National Institute of Standards and Technology (NIST). In Europe, organizations like ENISA, EC-DG SGCG are currently supporting the creation of a smart grid framework and standards which are being developed based on inputs from standards bodies like CEN/CENELEC/ETSI SGCG, ISO and IEC.

Designed to ensure the reliability of bulk electric systems in North America, NERC's Critical Infrastructure Protection (CIP) includes standards development, compliance enforcement, assessments of risk and preparedness. NIST developed and issued NISTIR 7628, Guidelines for Smart Grid Cyber Security and NIST Special Publication 1108: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.

Standards Developed to Provide Improved Grid Security

ANERC's CIP Reliability Standards require compliance with specific requirements to safeguard critical cyber assets. CIP-002 through CIP-009 address physical as well as cyber security requirements for responsible grid entities. They provide the benchmarks for utility companies' measurements and certifications. Cyber aspects include:

- Identifying critical assets
- Identifying and training cyber security personnel
- Developing and implementing security management
- Defining methods, processes and procedures
- Securing the systems identified as critical cyber assets
- Reporting and response planning
- Establishing recovery plans

NIST's cybersecurity objective of confidentiality, integrity and availability (CIA) impacts the interactions of several entities as shown in figure 1. The basis of the interactions are the Internet, enterprise buses, wide area networks (WANs), substation local area networks (LANs), field area networks and premises networks. While confidentiality is least critical for power system reliability, it is increasingly important with the availability of online customer information and privacy laws that impose strict penalties for breach of privacy. The integrity for power system operation addresses requirements of:

- Authentication of the data
- No modification of the data without authorization
- Implementation of NISTIR 7628
- Known and authenticated time stamping and quality of data

Impact Levels for Smart Meters

	C	I	A
15	L	M	M
17	L	H	M
18	L	H	L

Table 1: CIA impact levels for smart meters. (Source: NIST 7628)

In addition to establishing the requirements, NIST existing and developed standards identify critical security aspects such as data encryption and definitions for common understanding and implementation of solutions.

The following use cases exemplify the implementation of NIST requirements through silicon solutions.

Use Case 1: Smart Meters

Smart meters or the AMI have two-way communications between field area networks in the smart grid. As such, they can be a weak link in overall network security. In the NERC CIP assessment, critical smart meter areas are:

15 - Interface between systems that use customer site networks such as home area networks (HANs) and building area networks (BANs)

17 - Interface between systems and mobile field crew laptops/equipment

18 - Interface between metering equipment

The NIST CIA impact level of low (L), medium (M) or high (H) for these critical areas is shown in table 1. The high-level security aspects with unique technical requirements include:

- User identification and authentication
- Device identification and authentication
- Security function isolation
- Denial-of-service protection
- Software and information integrity

To meet these requirements, the silicon solution must provide:

- Crypto support
- Secure key
- Random number generator (RNG)
- Secure clock
- Trusted execution/hardware firewall
- Tamper detection
- Secure debug

ANEAMI system functions include measuring, communicating and using data. Encryption techniques are defined for specific aspects of these functions. Smart meter encryption techniques include advanced encryption standard (AES) and elliptic curve cryptography (ECC) that are even more stringent than techniques used in the banking sector. NIST applies additional requirements for smart meters including unique credentials, a key management system (KMS) that supports an appropriate lifecycle of periodic rekeying and revocation, and more. The successful implementation of smart meter security is based on a hardware root of trust.

Use Case 2: Data Concentrator

In the AMI architecture, a data concentrator collects meter information and data for transmission to the utility. Figure 2 shows the process.

Mechanisms for the interface between the data collection system and the electricity meter (or a data concentrator and the electricity meter) include:

- Trusted execution
- Authentication of all command messages
- Encryption (AES 128) to ensure confidentiality of metering data using block ciphering and a unique symmetric encryption key for each meter
- Message authentication for meter data integrity provided via AES Galois message authentication code (GMAC) algorithms

Each smart meter has a unique and secret unicast AES key with its default value set in the factory. When the meter has been installed and commissioned, a new operational key replaces the default value. A unique and non-modifiable master key encryption key (KEK) in each smart meter provides added security. The master key is used during the transportation of a new working key, during the commissioning or during the operational life of the meter.

In the above use cases, one of the major criteria for security is trusted execution of code, which is accomplished though use of trusted computing.

Smart Meter and Utility Security

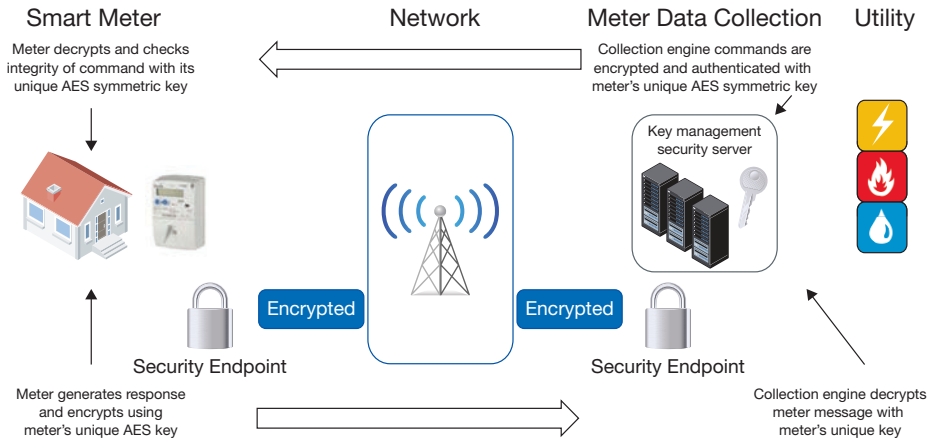


Figure 2: End-to-end security between the smart meter and the utility. (Source: Freescale)

Trust Architecture Threat Types

Threat Type	Threat Definition
Theft of Functionality	Loss of control of the system's functionality such that legitimate users enable unauthorized features or unauthorized parties exploit the system's features to the detriment of legitimate users
Theft of Third-Party Data	Loss of third-party data to an unauthorized party, where the system's users had a reasonable expectation that such a loss would not occur, resulting in regulatory or reputational loss to the OEM
Theft of Uniqueness	Loss of product differentiation through reverse engineering, duplication and unapproved interoperability

Table 2: Threat types against which trust architecture protects

Trusted Computing: Root of Trust (RoT), Trusted System and Architecture

The fundamental step towards establishing a secure or trusted component or entry point to a network is an RoT. The RoT verifies that the component is performing in an expected manner in the initial operation or engagement of the component or system. This established trust provides the first step towards improving security. In the Aberdeen Group report, "Endpoint Security: Hardware Roots of Trust," the analyst notes that over a twelve-month period, companies that utilized a hardware root of trust in their approach to security had 50 percent fewer security related incidents and 47 percent fewer compliance/audit deficiencies.

A trusted system is a system that does what its builder (OEM) and users expect it to do and does not do what the developers and users consider harmful. The trust architecture provides the tools to create a trusted system. Developers who properly leverage the hardware hooks in the silicon solution can trust that the software they loaded into the system during manufacturing or authorized software updates is the software that executes following system boot. Once trusted software is in control, the developer can leverage additional trust architecture features to keep the trusted code in control of the system and to defend against the extraction of system secrets or the introduction of malicious software.

Objectives of the Trust Architecture

The trust architecture relies on a combination of trusted hardware and software to support a wide range of OEM-defined security policies, including confidentiality, integrity and authentication of system assets such as data traffic, control traffic, system configuration data, cryptographic keys, and system and application software. The security mechanisms within the trust architecture protect these assets against three main threats, which are defined in table 2.

Freescale Security Solutions

Security Features	QorIQ MPU	i.MX MPU	Vybrid MPU	Kinetis MCU
Trusted Execution	Hypervisor secure and normal processor modes Memory management: No execute feature. Memory pages can be marked as non executable	Non MMU: Security supported with memory protection unit	Non MMU: Security supported with memory protection unit	Non MMU: Security supported with memory protection unit
High Assurance Boot	Secure boot process supported by: Security fuse processor Internal boot ROM Security monitor	Authenticated boot, encrypted boot (i.MX6)	Authenticated boot/ encrypted boot	X
Secure Storage	X	Off-chip crypto protection On-chip self-clearing RAM (i.MX25, i.MX5x, i.MX6)	On-chip zeroizable Secure RAM	256-bit secure storage erased by tamper
HW Random Number Generation Ensures strong keys and protects against protocol replay	X	X	X	X
Secure Clock Provides reliable time source On-chip, separately powered real-time clock Protection from SW tampering		On-chip separately powered real-time clock monotonic counter	On-chip separately powered real-time clock	Secure real-time clock with monotonic counter
Secure Debug	Permanent JTAG or challenge/response access	Three security levels plus complete JTAG disable	Three security levels plus complete JTAG disable	Multiple secure debug levels
Tamper Detection	Runtime integrity checker	Runtime integrity checking (not on i.MX6) Physical tamper detection	Runtime integrity checking Physical tamper detection	Runtime integrity checking Physical tamper detection
Cryptography	H/W acceleration AES, MD5, SHA1/256	H/W acceleration for AES, DES, 3DES, MD5, SHA1/256	H/W acceleration AES, DES, 3DES, MD5, SHA1/256	H/W acceleration AES, MD5, SHA1/256
Deep Packet Inspection Intrusion detection and prevenion using signature detection and filtering techniques	X			

Table 3: Freescale security solutions features at a glance

Freescale Security Solutions

As a leading supplier of MCUs and MPUs for control and monitoring applications, Freescale has over 44 years of experience developing information security solutions. This includes:

- Over 150 security patents
- Over 5,000 man years and $1.7 billion invested to date
- Over 125 major equipment projects developed and produced

In addition, dedicated Security Technology Centers of Excellence and an extensive portfolio of cryptography and platform assurance intellectual property (IP) provide Freescale a distinctive position to address smart grid security issues. To meet NERC and NIST requirements, four different solutions address security in smart grid and other industrial applications. (Refer to table 3.)

QorIQ Family

Freescale has implemented the trust architecture on devices in the P1–P5 QorIQ processor families, however, not every member of each family implements the trust architecture.

The single-core QorIQ P1010 processor's trust architecture platform helps protect against software intrusion and software cloning with its advanced end-to-end code signing and intrusion prevention capabilities. Implementing the NIST 7268 system trust model, figure 3 shows the trust features in the QorIQ P1010. Based on the e500 core, the P1010 has security accel, security fuses, security monitor, internal boot ROM and external tamper detect blocks. These blocks and others combine to provide users a variety of security options.

The trust architecture mitigates the threats listed in table 2 by providing the following SoC capabilities:

- Unauthorized modifications to OEM software and system configuration information (such as device trees or certificates) in the manufacturing chain and in deployed systems are detectable. Such modified software and configurations can be prevented from executing on the QorIQ CPU.
- Confidential code, factory installed private and session keys, and other system secrets are protected against extraction or exposure.
- Session keys negotiated during the normal operation of the system are protected against extraction or exposure.
- Multicore QorIQ CPUs enforce strong barriers between partitions so that the private resources of one partition cannot be accessed by another partition.
- Once authenticated (trusted) software is running on a partition, the QorIQ CPU can prevent (or quickly detect) modifications to this code. QorIQ CPUs also offer significant immunity to buffer overflow attacks through configuration of data memory as non-executable.

Figure 4 shows the QorIQ CPU's trusted boot process. The QorIQ CPU uses an RSA public key to decrypt the signed hash and simultaneously recalculates the SHA-256 hash over the system code. If the decrypted original hash matches the calculated hash, the code is authenticated.

P1010 Block Diagram

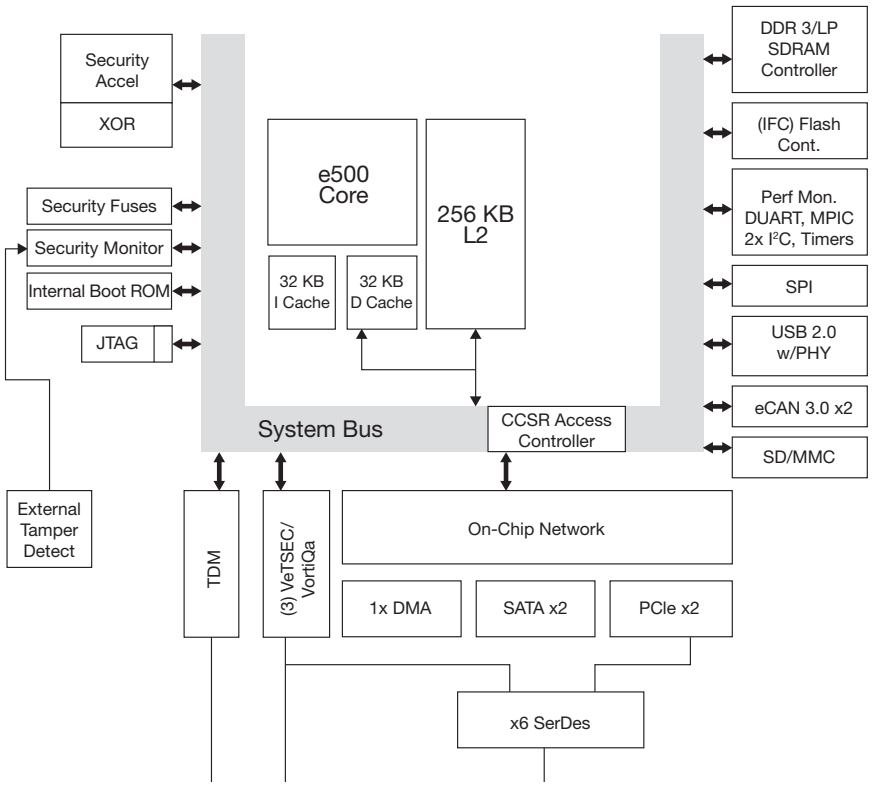
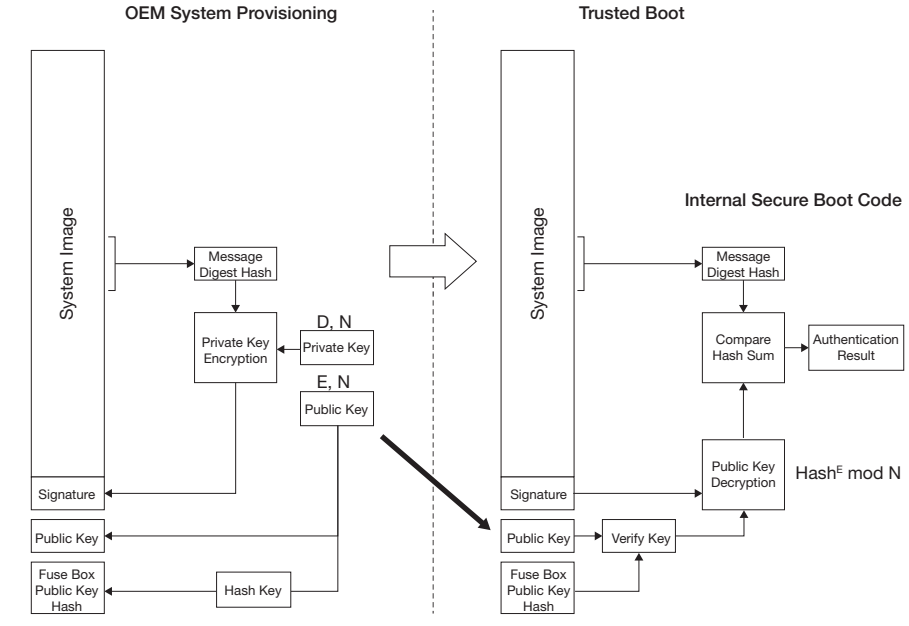


Figure 3: QorIQ P1010 trust features

Trusted Boot Process



Note: Program and signature may also be encrypted for IP protection
Private key has to be carefully managed and protected

Figure 4: Code integrity through the trusted boot process

Trust Architecture Defenses

	Malicious Action	Trust Architecture in Operation
Defense Against System Modification OEMs and service providers want protection from loss of functionality due to malicious actions	Theft of functionality, escalation of privilege, crashing the system by unauthorized code execution (booting an alternate image or changing boot location)	QorIQ secure boot will detect a fraudulent image and refuse to execute, as long as attackers do not have OEM's image signing key
	Modification of system code after boot through use of buffer overflows, debug interfaces and "mod chips"	Power Architecture® technology CPU provides enforcement of non-executable memory regions, hypervisor and PAMU memory access control, runtime integrity checking and secure debug
	Exploiting a remote management interface, firmware update facility	Perform a two-way authentication of remote management server, using protected credentials
		Use IPsec, SSL or SSH for privacy and integrity of firmware updates over the network
		Verify digital signature of new firmware before allowing it to execute
Denial of Service as Theft of Functionality Attackers could deliberately activate the trust architecture defenses to deny service and functionality to legitimate users	Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks attempt to crash a system by flooding it with connection setup requests, malformed packets and other spurious traffic	The QorIQ Data Path Acceleration Architecture supports fast flow classification and policing, used to rate limit floods of connection setup request packets and similar protocol exploits Many QorIQ processors include a 10 Gb/s pattern matching engine, to accelerate identification of malware
Defense Against Theft of Third-Party Data QorIQ processors are often used in systems that forward third-party or user data, or store said data within the system for extended periods of time: end-user system credentials, certificates, passwords, session keys, files and user packets	The objective of code modification attacks is often to extract end-user data. Theft of certificates, data and keys by running software on the system	The trust architecture on QorIQ helps protect data through strong access control and encryption. PAMUs enforce memory access control policies, preventing external chips from using peripheral interfaces The hypervisor can be used to enforce privacy between software partitions in a virtual machine environment Encryption can be used to protect third-party data and other private information both short and long term
Defense Against Theft of Uniqueness Theft of uniqueness is a loss of product differentiation suffered by an OEM due to reverse engineering, duplication (cloning), or unapproved interoperability by a competitor	**Counterfeit Clones** A counterfeit clone is an exact (or as exact as possible) copy of a system	Using trust architecture to validate and decrypt the code achieves significant resistance to this type of attacker as, the driver modification causes secure boot to fail By including a Freescale unique ID in code signature, even cloners with unprovisioned QorIQs cannot create systems capable of booting the OEM's code
	Functional Clones A functional clone is a reverse-engineered system intended to compete with the original	The trust architecture cannot prevent reverse engineering, but can raise the cost of the attack If system must work out of the box, all code is resident in NV RAM when system leaves factory. Trust architecture methods for protecting long-term secrets must be exploited to their fullest. If system leaves the factory with minimal functionality, remote provisioning can be used to raise the cost of attack

Table 4: How trust architecture protects agains various malicious acts

Trust Architecture in Operation

Table 4 shows the defenses provided by trust architecture against various malicious attacks.

The QorIQ family is ideally suited to solve the use cases mentioned earlier and many more. For example, the P1025 QorIQ data concentrator includes:

- P1025 QorIQ processor 667/800 MHz dual-core device
- Capabilities for IEEE® 1588 time stamping and security acceleration

The P1025 also has many additional features that address connectivity and security requirements in data concentrator applications.

The QorIQ platform's trust architecture provides OEMs with the hardware anchor points they need to develop a trusted system. Freescale's hypervisor and other reference software provides OEMs with the ability to supervise the multiple CPUs running independent OSes and to demonstrate a chain of trust from the internal secure boot code to the OEM's own code.

Other Freescale security solutions for the smart grid include the i.MX and Vybrid MPUs and the Kinetis ARM® Cortex™-based MCU. Vybrid MPUs do not have the deep packet inspection of the QorIQ but include a secure clock for a reliable time source. The on-chip, separately powered real-time clock provides protection from software tampering.

The i.MX processor includes TrustZone® technology secure and normal processor modes as well as a secure clock but does not have deep packet inspection. Finally, the Kinetis ARM Cortex-based MCU does not have a memory management unit (MMU), but supports security with a memory protection unit and other security features.

Freescale security solutions include robust tools and solid ecosystem partner solution support. This includes:

- Extensive tool suite of hardware and software available for customer evaluation
- VoritQa software tool suite for control center, monitoring control and home gateway applications
- Certified, third-party software suite

Securing the Grid and More

Increased grid infrastructure networking requires increased grid security. With efforts from organizations such as NERC and NIST, the specific requirements for increased grid security have been well defined. As a result, enabling technologies from many companies will help ensure high security levels as smart grid systems, including smart meters and data concentrators, are implemented. With proven leadership in processing, control and security, Freescale security solutions provide the trusted, hardware-based foundation for a secure grid with comprehensive systems and software support.

Appendix

Anti-cloning provides a unique device ID and digital signing support and encryption

High assurance boot is a security library embedded in tamper-proof on-chip ROM that prevents unauthorized SW execution

Secure clock provides reliable time source

Secure communications ensure the integrity of data and information

Secure debug protects against hardware (HW) debug (Joint Test Action Group (JTAG)) exploitation

Secure storage provides a programmable ARM TrustZone technology protected region within on-chip RAM

Trusted execution isolates execution of critical software (SW) from possible malware

TrustZone technology is a trusted execution environment for security-critical SW

AES: Advanced Encryption Standard

ECC: Elliptic Curve Cryptography

FIPS: Federal Information Processing Standards

Hash is any well-defined procedure or mathematical function that converts a large, possibly variable-sized amount of data into a small datum

RSA is an algorithm for public-key cryptography named for Rivest, Shamir, and Adleman who were first to publicly described it

For more complete acronyms and glossary, see Appendix I of NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References

References

INL/EXT-09-15500, “Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues,” **inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf**

NERC
nerc.com/files/CIP-002-1.pdf

Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security
smartgrid.gov/sites/default/files/pdfs/nistir_7628%20.pdf

NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements
csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid
csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References
csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

An Introduction to the QorIQ Platform’s Trust architecture
freescale.com/webapp/sps/site/overview.jsp?code=NETWORK_SECURITY_INT_SEC

How to Reach Us:

Home Page:

freescale.com

Email:

support@freescale.com

For more information, visit freescale.com

Document Number: TRCMPSCSMRTGRDWP REV 1