BUILDING BLOCKS FOR EMBEDDED SECURITY

Developers can rely on Digi TrustFence for built-in security without having to design features from scratch.

While it is well-known today that security for connected devices is critical, and security breaches are occurring at epidemic proportions, many companies still fail to properly implement embedded security or make the right up-front design decisions. The issues stem from lack of knowledge about how to properly integrate security into design and present a multi-faceted level of defense against intrusion.

The largest enterprises often have dedicated security teams that are responsible for ensuring device security throughout the product lifecycle. But many smaller organizations don’t have this expertise in house, and may not even know how to approach device security, leaving them vulnerable to attacks. These companies are at the mercy of their collective suppliers’ security knowledge and implementation. This is where Digi TrustFence® comes into play.

WHAT IS DIGI TRUSTFENCE?

Digi TrustFence is a security framework designed with the realities and constraints of real world business operations in mind, so that regardless of an organization’s size, resources and security knowledge, they can implement proper device security in their products.

Cryptography and information security are complex concepts. Putting them into practice can be an even more daunting task, but it doesn’t have to be. Digi engineers have worked through these problems and combined the most important security features into one easy-to-implement package. Digi TrustFence is an industry-leading security framework that combines hardware and all layers of software to simplify the process of securing connected devices.

The Digi TrustFence framework combines hardware and all layers of software to simplify the process of securing connected devices.

DIGI TRUSTFENCE AND EMBEDDED DESIGNS

Digi TrustFence is integrated into a broad range of Digi products, from Digi cellular routers to embedded systems like Digi XBee® RF modules, Digi XBee cellular modems, and Digi ConnectCore® System-on-Modules (SOMs). In this brief, we specifically address how Digi TrustFence supports robust security for products built with Digi ConnectCore SOMs, which are based on the NXP® i.MX® series of application processors.

Embedded devices often require a device security approach that supports 10+ year product life cycles. Just like software developers rely on trusted software libraries, embedded developers can rely on Digi TrustFence to provide a sound security approach without having to design features from scratch.

Digi TrustFence addresses the unique challenges involved in securing embedded devices that make IoT the low-hanging fruit for attackers:

- Irregular security updates due to widespread and remote deployment
- Easy attack replication across thousands of identical embedded devices
- High-value targets such as utility, transportation and communication systems
- Long device lifecycles of 10 years or more
- Industrial protocols outside the security layers provided by enterprise tools[1]

To combat these issues, Digi TrustFence supports the classic information security model, which requires three equally important data protection objectives: confidentiality, integrity and availability. For a device to be truly secure, developers must account for all three factors.

- **Confidentiality** means that only people who are authorized to do so can access your information or your device.
- **Integrity** is the certainty that nothing has been altered and that the information or device can be trusted to be genuine.
- **Availability** means ensuring that users have reliable access, but only if they have been authenticated.

Digi TrustFence is a complete embedded security solution that simplifies the process of securing connected devices. So what does built-in security look like?

BUILDING ON THE NXP I.MX SECURITY FEATURES

NXP i.MX applications processors feature advanced security capabilities at the system level, such as High Assurance Boot (HAB), a True Random Number Generator, and multiple hardware-accelerated cryptographic algorithms, which provide the perfect foundation for implementing a secure embedded system.

To develop a fully secure product involves building on NXP's security features to ensure a complete, secure embedded system that provides multi-layer defense against intrusion.

Digi TrustFence enables developers to build a solution that accesses on the value of those built-in features without requiring expertise in security/cryptography, low-level hardware and embedded software. Digi complements and extends these building blocks to form a secure subsystem from the ground up teams can develop secure systems on top of this foundation with product-specific requirements.

The Digi ConnectCore family of SOMs also includes hardware and software security features that do not rely on i.MX components. These include digital and analog tamper pins and Secure Element, which are handled by Digi Microcontroller Assist™ (MCA), as well as FIPS 140-2 certification. **This foundation offers a major head start, saving months of developer time and reducing security risk.**

The longevity of embedded products means that software maintenance and future availability are crucial. Digi maintains the Digi TrustFence security framework with this in mind; we understand that the functionality you rely upon must be there throughout the life of the product.

The steps for securing Digi ConnectCore modules with Digi TrustFence are well-documented, with instructions and graphics explaining core security concepts and describing how Digi TrustFence protects your devices.

This documentation is a comprehensive resource written for users who are not security experts, with in-depth topics covering the full product lifecycle, including development, production and deployment. You can find the Digi TrustFence technical documentation in the Digi Embedded documentation portal.

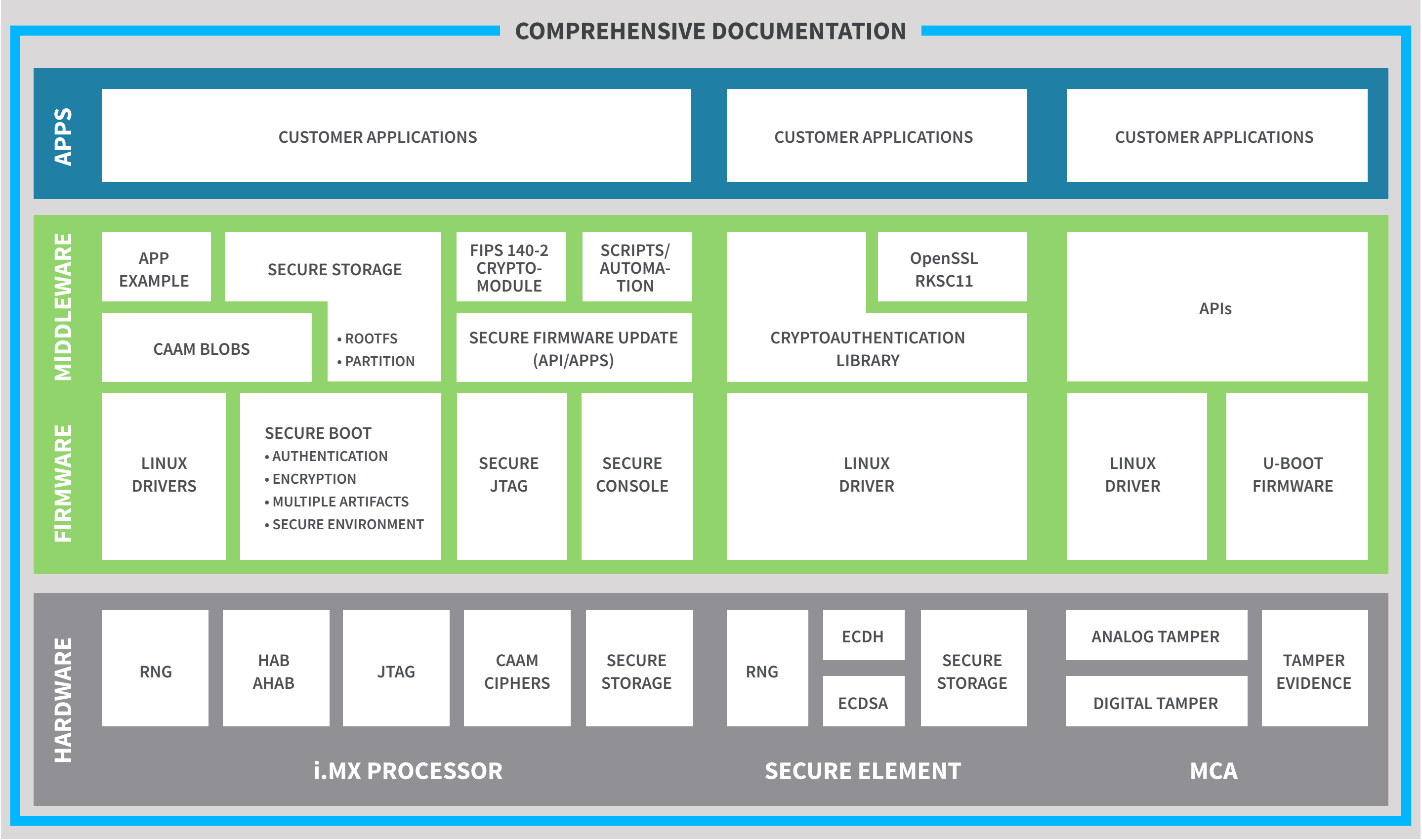

Diagram 1: Digi TrustFence security stack

SECURITY FEATURES IN DIGI CONNECTCORE MODULES

In the connected world, it is important to build in security from the ground up, following a “secure by design” approach that thwarts intrusion into your product, data and intellectual property at multiple levels. Here are the features Digi builds into the ConnectCore module family.

Secure Boot

On most modern embedded systems it is critical to ensure that the device only runs legitimate firmware, preventing the execution of malicious software. Secure boot ensures that a basis of trust is established in the system from startup. The foundation of a secure boot implementation relies on **digital signatures**, which certify the authenticity of the firmware stored in the memory before starting its execution.

The secure boot support provided by modern microprocessors guarantees that the first firmware executed — the bootloader — is authentic. However, the software of a modern embedded system is formed by multiple artifacts. Depending on the operating system, the boot process involves loading multiple binaries into memory, for instance the Linux kernal and device tree. Therefore, a true secure boot implementation must ensure integrity and authenticity of all the software elements, from the bootloader to the user space applications.

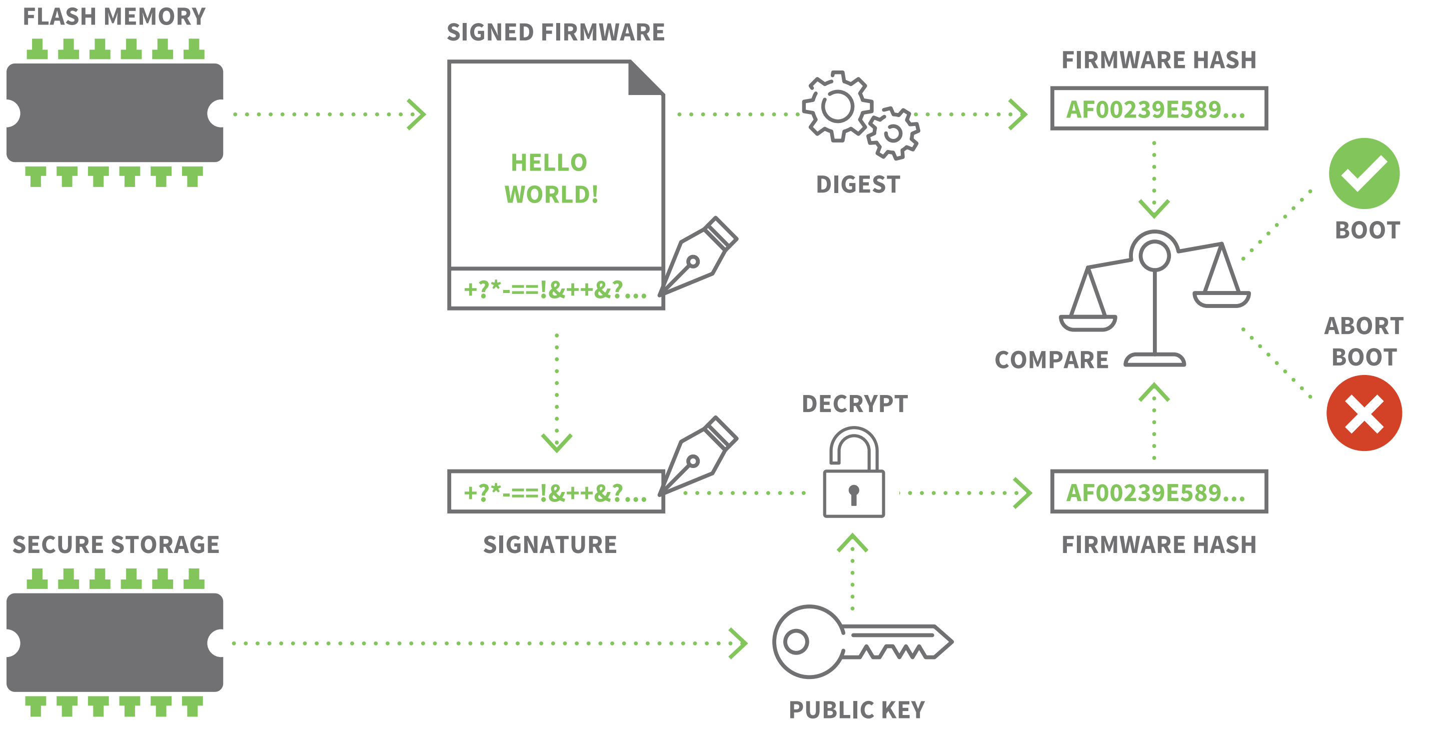

Diagram 2: Firmware verification process

It's up to the device developer to protect the integrity of the boot process by ensuring the system is booting only what has been authenticated. Digi has wrapped these complexities in a tested solution. Digi TrustFence offers a complete secure boot solution by extending the i.MX secure boot mechanism to authenticate (and optionally encrypt) the Linux kernel, device tree blobs, bootscripts and initramfs. This simplifies signing and encrypting any of these artifacts, requiring only a couple lines of code in the Digi Embedded Yocto or Digi Embedded Android configuration file. Digi also provides standalone scripts for this function so that the process can be isolated in a secure server outside of the development environment.

The encryption of the filesystem prevents tampering of the device and insertion of malware on the user-space applications. It also provides **intellectual property** and **user data protection**.

In cases where additional security is required, the Secure Element on Digi ConnectCore SOMs goes beyond traditional secure boot and implements **multi-factor authentication** using infrastructure provided by the crypto-authentication chip, also included on the SOM.

Protected Ports

Once secure boot is enabled in the system, the standard boot flow will authenticate all the firmware before running it on the system. But what if the standard boot flow is altered using JTAG, or the U-Boot console during boot? To mitigate this attack vector, you can secure other ports that could allow access to the device. Digi ConnectCore modules offer several options to secure these ports and access to the system.

Oftentimes, a supposedly secure system still has unprotected serial interfaces that provide full access through a command shell. Enabling Digi TrustFence forces you to consider and set up these important protections.

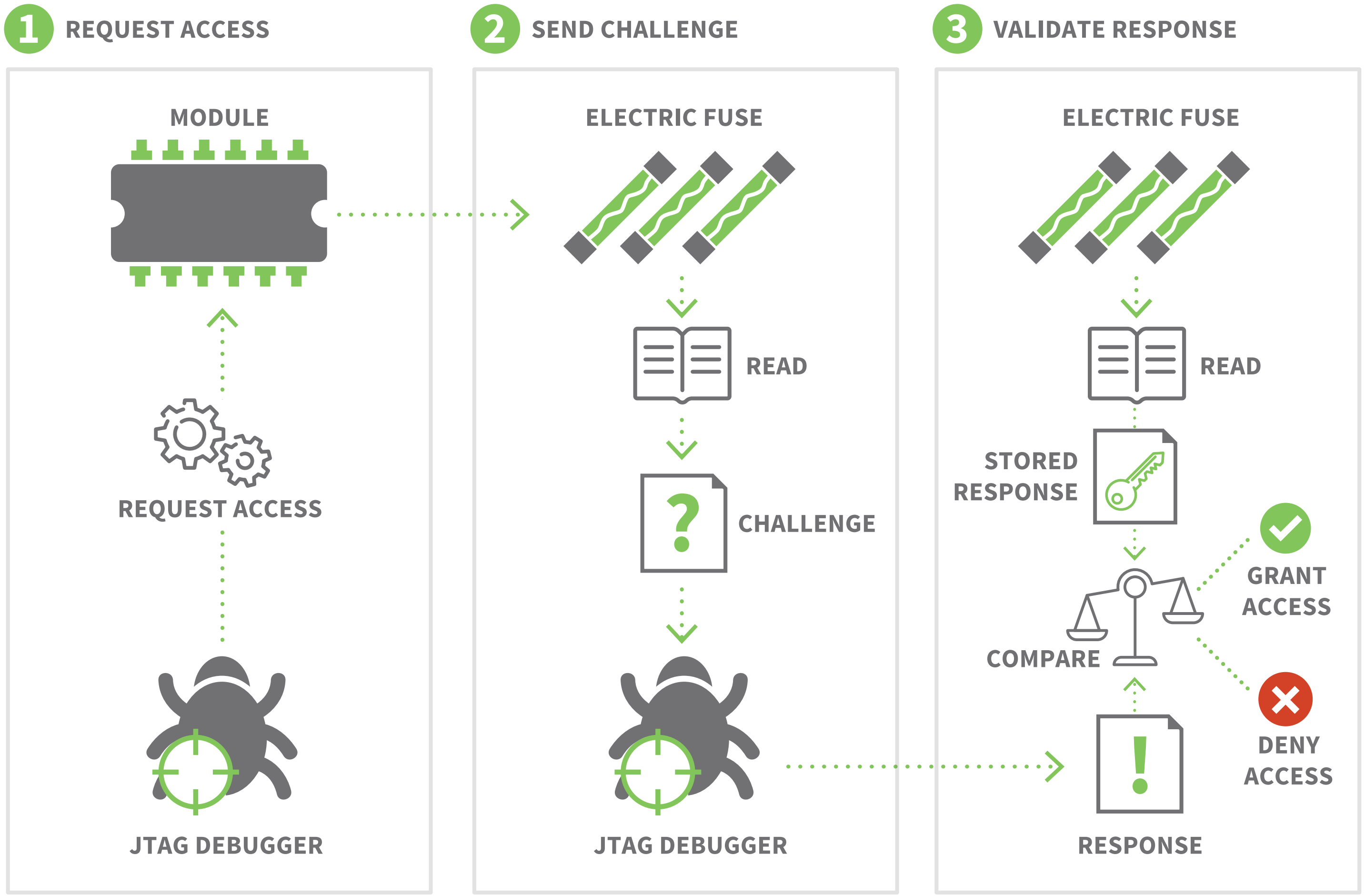

Diagram 3: Secure JTag process

Secure JTAG

Most embedded devices provide a JTAG interface for debugging purposes. However, if left unprotected, this interface can become a critical attack vector on the system. JTAG allows halting and debugging of the processor at any point, even during boot in the authentication steps, which means an attacker could interrupt and bypass authentication. Digi TrustFence allows you to change the secure JTAG mode to prevent any attacks with a hardware debugger.

Secure Console

The console can be a vulnerable point of attack on an embedded product. One of the first things an attacker will try on a device is to look for the debug UART pins, hoping to discover a root shell to the device. Digi recommends you completely disable the system console both in U-Boot and in Linux for the highest level of security. If they are mandatory on the final system, Digi TrustFence also offers ways to enable them to use a password or a GPIO pin. With Digi TrustFence, developers can adapt security settings to meet specific product requirements by simply defining a set of variables.

Tamper Detection

The tamper interface provides a mechanism for detecting unauthorized attempts to gain physical access to or make unauthorized modifications to a system or device. You can use the tamper interface to detect events in all power modes, including power off with battery backup (coin cell). All events are saved into non-volatile memory and the system is notified as soon as execution resumes. You can also program customized counter measures, such as instructing the system not to boot if it detects unauthorized access to the system. The Digi Embedded Yocto Board Support Package provides the necessary firmware to easily detect tamper events and perform the corresponding response actions.

Secure Storage

Another fundamental aspect of security is confidentiality. Many applications require the embedded device to keep sensitive data. The standard solution to this problem is to use encryption to protect the data and ensure that only authorized users have access to the encryption key. When a user interacts directly with a system, the encryption key can be protected with a password, pin code or fingerprint that is provided by the user. However, many embedded devices work without user interaction, so this is not an option in those cases.

This problem is commonly solved in embedded systems with a hardware-protected key that is used to encrypt and decrypt data but that cannot be accessed directly. With this key, applications can protect content and save it in the flash memory, with the assurance that it can only be decrypted by the i.MX processor that encrypted the data. In this way, all data is protected when the system is offline.

Using this advanced and specific i.MX operation is not simple, but the Digi TrustFence framework provides easy ways to deploy this feature and securely encrypt your system at any level:

- System encryption: The most secure setting (and default mode in Digi TrustFence) is to encrypt the complete root filesystem. In this mode, the complete rootfs partition is encrypted and all files and metadata are protected. Note that on-the-fly encryption and decryption does introduce a small performance penalty in read and write speeds.
- Partition encryption: To protect some sensitive files but not pay the cost of encrypting the complete rootfs, you can keep the rootfs partition unencrypted and set up a specific encrypted partition where the sensitive files will be stored.
- File-specific encryption: For the most specific use cases, Digi provides a method of encrypting and decrypting specific files using the internal i.MX encryption key. The artifacts used in this process are known as CAAM blobs.

> Data confidentiality is commonly solved in embedded systems with a hardware-protected key that is used to encrypt and decrypt data but that cannot be accessed directly.

Secure Firmware Update

Due to the connected nature of devices, security vulnerabilities are more widespread than ever before, and new threats are discovered by the security community daily. Security requirements change often, and it is therefore important to make sure your system is ready to be securely updated so new vulnerabilities can be patched or functionality can be added to the product. A secure firmware update process involves more than safely updating a device. It also verifies that the delivered image is coming from a known source and that the image was not modified to introduce malware.

Enabling Digi TrustFence in your project automatically enables the secure firmware update mechanism. The software that validates and programs the new firmware is a signed artifact that is validated, loaded to RAM, and launched by the bootloader so it cannot be tampered with. Since the software runs completely from RAM, it can update any part of the system, including the firmware update software itself. Digi TrustFence makes it easy to securely update device firmware on an ongoing basis; once Digi TrustFence is enabled in a project, the resulting build artifacts are ready to perform secure firmware updates.

Secure Element

Digi ConnectCore SOMs include a crypto-authentication chip, or Secure Element, that complements and extends the cryptographic capabilities of the main processor. The Secure Element integrates the ECDH (Elliptic Curve Diffie Hellman) security protocol along with ECDSA (Elliptic Curve Digital Signature Algorithm) authentication, widely used in Internet of Things (IoT) use cases for medical, industrial networking, home automation and more. The chip provides hardware-based cryptographic key storage, saving you the effort of managing and storing device certificates and encryption keys.

The keys are securely saved in the chip and never exposed during the cryptographic operations performed by the device. The device also provides a high-quality FIPS Random Number Generator that can help improve the total system entropy. But hardware is nothing without software. Digi Embedded Yocto integrates a library that simplifies access to all these features from your custom applications. In addition, the library can interface with OpenSSL via a PKCS#11 API to exchange cryptographic tokens.

The combination of different hardware cryptographic devices allows you to implement more secure solutions – like multi-factor authentication – where the security of the system cannot be compromised by a single point of failure.

Random Number Generators (RNGs)

Many cryptographic operations, such as the generation of session keys, rely on random numbers generated by the system. A poorly designed strategy for RNG can leave a good cryptosystem vulnerable to attacks. To ensure that generated keys are unpredictable, they must be totally random; otherwise, the security of the system is compromised.

There are two main strategies to generate random numbers:

- The first is based on the measurement of a physical parameter that is inherently random, such as quantum phenomena or thermal noise. These generators are known as True Random Number Generators (TRNGs) or Hardware Random Number Generators (HRNGs). The advantage is that they produce “true random” values. On the other hand, generation is quite slow compared to other methods. They are also difficult to analyze, if not impossible, due to the randomness of the physical process.
- The second strategy uses deterministic algorithms that produce sequences of random numbers that depend only on a short initial value, typically referred to as a seed. These generators are called Pseudo Random Number Generators (PRNGs). The main advantage of PRNGs is their rapid generation and ability to be analyzed and tested, thanks to the deterministic nature of the algorithm. They must be seeded with a truly random value; otherwise, the resulting sequence of numbers is predictable. Since the 1980’s, several PRNGs have emerged with properties that make them suitable for cryptographic systems. This class of PRNGs—studied deeply by experts in information theory—is called Cryptographically Secure Random Number Generators, or CSPRNGs.

In modern cryptography, it is common to combine both approaches: using a TRNG or HRNG to collect a pool of data with high entropy and then processing it through a CSPRNG to obtain a more uniform stream of data.

Digi TrustFence provide a dual TRNG – one included in the applications processor and a second in the Secure Element. This allows the system to combine the randomness of multiple independent sources, resulting in a more secure implementation by not relying on a single source of entropy. The combination of high-quality entropy with the multiple available choices of CSPRNG, either in hardware or software, provides a secure solution via random bit generation.

FIPS Certification

The Federal Information Processing Standards (FIPS) 140-2 level 1 standard is an information technology security approval program for cryptographic modules. It is geared toward private-sector vendors who seek certification for products used in government departments and regulated industries (such as financial and healthcare institutions) that collect, store, transfer, share and disseminate sensitive but unclassified information.

Select Digi ConnectCore modules with TrustFence have been certified to FIPS 140-2 level 1, enabling companies to leverage existing certifications instead of performing their own FIPS integration and validation at a certified lab, which is a very costly and resource-intensive process often exceeding $100,000. The National Institute of Standards and Technology (NIST) will issue a FIPS 140-2 certificate in your company's name by rebranding Digi's certificate.

DIGI TRUSTFENCE FEATURES BY PLATFORM

The following table lists Digi TrustFence security features by ConnectCore platform:

		ConnectCore 8M Nano*	ConnectCore 8X*	ConnectCore 6UL	ConnectCore 6+	ConnectCore 6
Enhanced secure boot	Authentication	✓	✓	✓	✓	✓
	Encryption	Planned	Planned	✓	✓	✓
Random number generation	CAAM TRNG	✓	✓	✓	✓	✓
	TRNG	✓	✓	✓	✓	X
Secure storage	Rootfs encryption	✓	✓	✓	✓	✓
	Partition encryption	✓	✓	✓	✓	✓
	CAAM blobs	✓	✓	✓	✓	✓
Protected ports	Secure JTAG	✓	✓	✓	✓	✓
	Secure console	✓	✓	✓	✓	✓
	Tamper pins (MCA)	✓	✓	✓	X	X
Secure element	Cryptochip	✓	✓	✓	✓	X
FIPS certification	FIPS 140-2 level 1 for Yocto Linux	Planned	Planned	✓	✓	✓

*Some features may be in development

SUMMARY

Cryptography and information security are complex concepts. Putting them into practice can be an even more daunting task, but it doesn't have to be. Digi engineers have worked through these problems and combined the most important security features into one easy-to-implement package.

Digi TrustFence is a security framework designed with the realities and constraints of real world business operations in mind, so that regardless of an organization's size, resources and security knowledge, they can implement proper device security in their products. It helps developers create a multi-layer defense against intrusion without requiring expertise in cryptography, low-level hardware and embedded software, saving months of developer time and reducing security risk. Just like software developers rely on trusted software libraries, embedded developers can rely on Digi TrustFence to provide a sound security approach without having to design features from scratch.

Digi is keenly aware of the risks developers face in bringing a product to market, and for this reason security is front and center in all we do. We developed Digi TrustFence as a multi-pronged solution to support the most robust security requirements in the connected device space. Digi TrustFence is designed to empower your team to produce secure products that hold up to evolving security threats throughout the complete product lifecycle.

For detailed Digi TrustFence information and implementation instructions, visit the Digi Embedded documentation portal by clicking here.
From there, select a Digi ConnectCore platform to see security content specific to that platform.

[1] eInfochips, An Arrow Company: 6 Critical Challenges Facing the Embedded Systems Security, August 20, 2018

Digi International Worldwide Headquarters
9350 Excelsior Blvd. Suite 700
Hopkins, MN 55343

PH: 877-912-3444
www.digi.com