The next-generation cryptographic platform for high-security products

RedFox Cryptographic Platform

Creating certified cryptographic products used to be a complex task, especially if you require a certification for government use. Not only must the products provide unsurpassed levels of security, but they must also undergo lengthy evaluations by various certification bodies. This often leads to a very long time to market. A lot of time, and thus money, is spent before the end-user benefits from your cryptographic solution.

Fox-IT has developed the RedFox carrier module in close cooperation with the Dutch government. The RedFox allows for swift certification of products based on it. The RedFox offers very high levels of security, both logical and physical. Cryptographic algorithms are implemented in hardware and provide high-performance throughput up to 800 Mbit/sec. Integrating the RedFox into new high-security products is a straightforward task using the SDK and reference implementations, thereby allowing time to market to be reduced significantly.

FOX-IT
FOR A MORE SECURE SOCIETY

Many security products require strong cryptography. Providers of such products and their customers need to rely on a strong cryptographic core. This ensures that their products are truly secure. Examples of such high security products abound, both in government and commercial settings. These include VPN solutions, hard disk encryption and hardware security modules (HSMs).

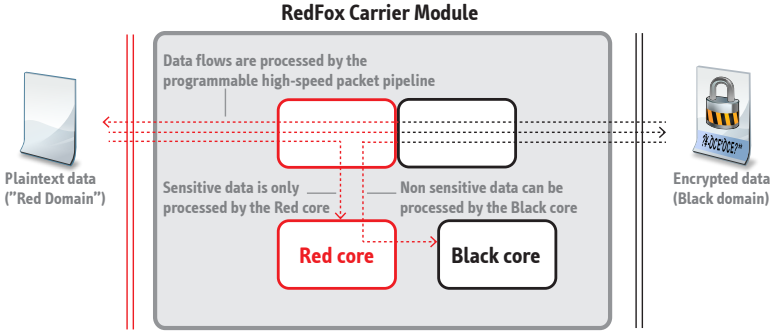
As cryptography lies at the heart of these products, government or commercial evaluations of such products focus heavily on the strength of the underlying cryptographic system. There are good reasons for this focus. Although modern cryptographic algorithms are theoretically strong, many mistakes can be made in their implementation.

A common solution to this problem is to offload cryptographic operations to a trusted external hardware security module (HSM). However, traditional HSMs cannot implement complex data processing logic, do not provide strict red-black separation, and do not offer flexible hardware interfacing. They must therefore be integrated into a host system that provides these features, thereby extending the scope of the security functionality to include the HSM and host system. That complicates the security design, makes it more difficult to ensure correct implementation, and increases the cost of certification and the time to market.

The RedFox Carrier Module (RF-CM) is a flexible HSM designed to be used as a building block in a wide variety of products. It can run complex data processing logic and provides strict red-black separation in hardware. The RF-CM was developed in close cooperation with the Dutch National Communications Security Agency (NL-NCSA). As such, it is designed to be used at the highest levels of Dutch, EU, and NATO security. The RF-CM is available in two editions to suit both government and enterprise customers.

Architecture

The RF-CM contains two separate processor cores to ensure very strong red-black separation (see figure). The red core handles sensitive data, such as keys or unencrypted data, while the black core processes non-sensitive data. This ensures that even if the black core is compromised, both key material and sensitive data remain secure.



Aside from the red and black cores, a programmable packet processing pipeline allows high-speed cryptographic operations. This pipeline, known as the hardware fast-path, can be programmed to process and encrypt data packets at high speed (up to 800 Mbit/second). Each packet is initially matched and assigned to a certain flow. Known flows can then be automatically decrypted or encrypted in hardware, without the need to query the red or black cores. Flows that require further processing can be offloaded to the red or black core, depending on the sensitivity of the data. As this process is highly flexible, the hardware fast-path can be used for a wide range of applications, including network-based products, hard disk encryption, key management and more.

Shortening time to market for certified security products

Due to its flexible nature, the RF-CM can be used as a solid base for security products requiring cryptography or secure storage. It is well-suited for NATO, EU and NL national markets.

The RF-CM has been developed in close cooperation with the NL-NCSA. This ensures that the certification of end-products based on the RF-CM can be performed much more cost-effectively than a fully custom solution. The RF-CM comes with approved pre-certification documentation, ensuring that the most complex parts of end-product certification can be performed rapidly.

Challenges in high-security products

Creating high-security products is a challenging task. A single flaw in either design or implementation can have catastrophic consequences for the system's security. Especially challenging aspects include the secure implementation of cryptographic logic, multiple layers of strong physical defenses, and perhaps most of all the protection of sensitive (red) data and processing logic and separation thereof from the non-sensitive, untrusted (black) domain.

The modern computing platform generally provides a single processor on which software runs, and it is the software's responsibility to provide data protection. This design has significant weaknesses and, as the software becomes more complex, can make certification very difficult. Software bugs can lead to breaches of security and data loss because the hardware doesn't enforce security domain separation. Unexpected hardware behavior can make well-written software vulnerable to specialist attacks, such as cache timing or other side-channel attacks.

Even many existing high-security products contain only a single processor and cannot run red and black software separately. That leads to highly critical security logic and more complex noncritical support logic being mixed, thereby complicating the certification process and increasing the chance of undetected flaws.

The RF-CM provides a complete package containing thoroughly evaluated high-performance cryptographic hardware and distinct red and black processing cores for running application-specific software in both domains without breaking the strict hardware-enforced domain boundary. All of this is wrapped in multiple layers of strong physical protection.

Unsurpassed levels of security

The RF-CM contains a large number of security and anti-tamper measures at the physical, electrical, and software levels (see highlight: Security in Depth). The security is active and, on detection of an attempt to tamper with the device, all sensitive material within the device is immediately cleared.

To ensure that the software on the system can be trusted, every step of the software chain can only run if it has a correct digital signature. The system is a trusted platform, ensuring that malicious code cannot be executed. Further security measures include support for a Crypto Ignition Key (CIK) which is stored on a hardware device that, when removed, renders the device unclassified. Keeping the CIK and the RF-CM separate ensures additional security during transport and storage.

Security in Depth

Strong security consists of multiple layers, ensuring that even if several countermeasures fail, an attacker cannot access the sensitive material contained in the device. The RF-CM contains many state-of-the-art security measures at the physical, electrical and logical levels.

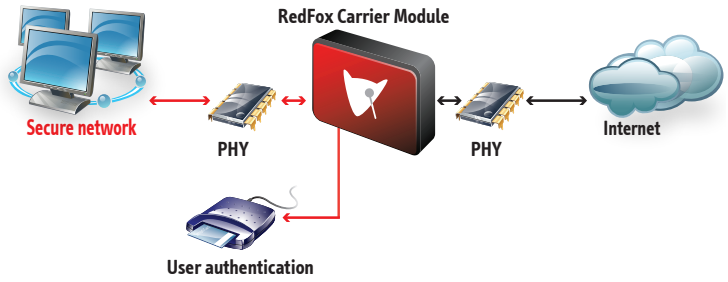
Red-Black separation

The RF-CM's security philosophy is based on a clear boundary between a sensitive (red) domain and a non-sensitive (black) domain. The red domain handles sensitive information such as key material, authentication and unencrypted data. The black domain only handles non-sensitive information, such as encrypted data. The boundary between the red and black domains is enforced in hardware, with crossings strictly controlled and kept to a minimum.

Example: VPN solution

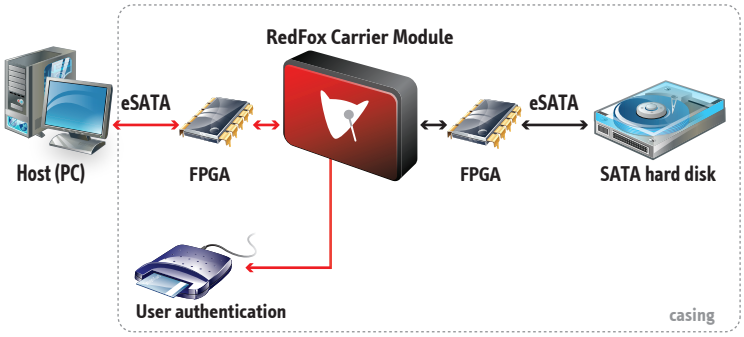
The red and black Gigabit Ethernet interfaces and the design of the hardware fast-path make the RF-CM a perfect fit for network encryption. A high-security Virtual Private Network (VPN) requires minimal extra hardware besides the RF-CM due to the built-in red and black processor cores. Only an interface for user authentication and the physical Ethernet drivers for fiber or copper media are required to complete the hardware design for a VPN appliance.

The VPN endpoint software that runs on the RF-CM's red and black cores can be cost-effectively built on top of the !RedFox SDK, thereby minimizing software development effort necessary for creating a fully functional VPN solution. The system's flexibility allows software to be written for both local management using a simple user interface and remote management over the wire from a management station.



Example: Hard disk encryption

The flexible design of the RF-CM also allows other uses than high-speed network encryption. One particular example is the use of the RF-CM for hard disk encryption.



The diagram above illustrates the concept of a transparent eSATA hard disk encryption device that is 'seen' by the host as a normal hard disk. The RF-CM is placed in the SATA data path. Surrounding FPGAs encapsulate eSATA frames in Ethernet frames, and vice versa. Two separate FPGAs are used to guarantee the red-black separation. The hardware fast-path is programmed to encrypt or decrypt the eSATA frames inside the Ethernet frame's payload at high speed.

FOX-IT
FOR A MORE SECURE SOCIETY

Technical Overview

Technical facts

Dimensions	144.5 x 109.0 x 22.5 mm (lxwxh)
Weight	0.4 kg
Power supply voltage	5 V
Power consumption	3 W (typical), 7.5 W (max)
Interfaces red	Gigabit Ethernet (GMII/MII), UART, GPIO
Interfaces black	Gigabit Ethernet (GMII/MII, UART, GPIO, USB, I2C, SPI

Performance

Crypto performance	800 Mbit / sec (AES + SHA, all key sizes)

Crypto algorithm support

RF-CM Edition:	Government	Commercial
AES (128, 192, 256-bit)	Yes	Yes
Classified algorithms	Yes	No
Camellia (128, 192, 256-bit)	No	Yes
SHA (224, 256, 384, 512-bit)	Yes	Yes
Public key operations, including RSA and ECC	Yes	Yes

Further information

Please contact Fox-IT if you would like a more detailed data sheet, a demonstration, proof-of-concept or integration details and SDK-information.

FOX-IT
FOR A MORE SECURE SOCIETY

RedFox Carrier Module

- Offers unsurpassed levels of security, both logical and physical.
- Flexible and versatile cryptographic module.
- Shortens time to market for certified security products.
- Can be easily integrated into security products using development kit.

Fox-IT

Fox-IT specializes in cyber defense, IT Security, lawful interception and digital forensics solutions, providing completely secure, easy-to-use and automated products for data transport, interpretation and archiving to dozens of government defense and intelligence agencies, systems integrators and commercial organizations worldwide. Fox-IT solutions maintain the security of government systems up to “state secret level” sensitivity, critical infrastructure and process control networks and other highly confidential data. The company also provides services including IT security audits, digital forensic investigations, training programs and managed security services. Established in 1999, Fox-IT is based in the Netherlands and works with trusted partners in more than 20 countries.

Fox-IT
Olof Palmestraat 6
2616 LM Delft
The Netherlands

P.O Box 638
2600 AP Delft

t +31 (0)15 284 79 99
f +31 (0)15 284 79 90
e fox@fox-it.com

www.fox-it.com