

SPYRUS TrustedFlash®

Rosetta microSDHC™ Products for Secure Mobility

Table of Contents

Table of Contents	i
Introduction to Mobile Device Security	1
The Threat is Real	2
SPYRUS TrustedFlash Rosetta microSDHC Overview	4
Rosetta microSDHC Architecture	4
SPYRUS TrustedFlash and Rosetta microSDHC PKI Features	6
SPYRUS TrustedFlash Rosetta microSDHC PKI Security Features	8
Rosetta Hardware Security Module – An Anchor of Trust	8
Entropy – The Soul of Security	9
Multiple Contexts and Separation	9
Rosetta microSDHC Separation in a Mobile Host Platform	11
SPYRUS TrustedFlash and Rosetta microSDHC PKI Applications	13
Security Applications Using Rosetta microSDHC	13
Rosetta microSDHC as a Secure Element for RES4Office™	15
Rosetta microSDHC as a Secure Element for Android Application Container	16
Summary	17
Appendix – SPYRUS Product References	18

Introduction to Mobile Device Security

Today, we live in an IT world comprised of what appear to be opposing corporate forces. On one hand, we have enormous demands to increase worker productivity and support an ever-changing, distributed and mobile workforce...which due to changing worker sensibilities and lifestyles, have increasing demands for the use of their own preferred mobile devices, mobile networks, and user interfaces. On the other hand, we are being asked to secure our corporate network access and our underlying corporate data ... and all of this, while managing our overall spending and retaining the new mobile workforce which places job satisfaction near the top of all employment metrics.

The BIG question: Is it really possible to manage a distributed and mobile workforce, secure corporate data, and maintain network integrity while at the same time managing costs?

The simple answer: YES. In this white paper we will cover the SPYRUS TrustedFlash Rosetta microSDHC offering as well as a full in-depth discussion of our family of related products and services that offer your organization not just mobility and cost savings, but also provide enhanced levels of data and network security for those users employing Bring Your Own Devices (BYOD) and Bring Your Own Networks (BYON).

How do the two universes coexist?

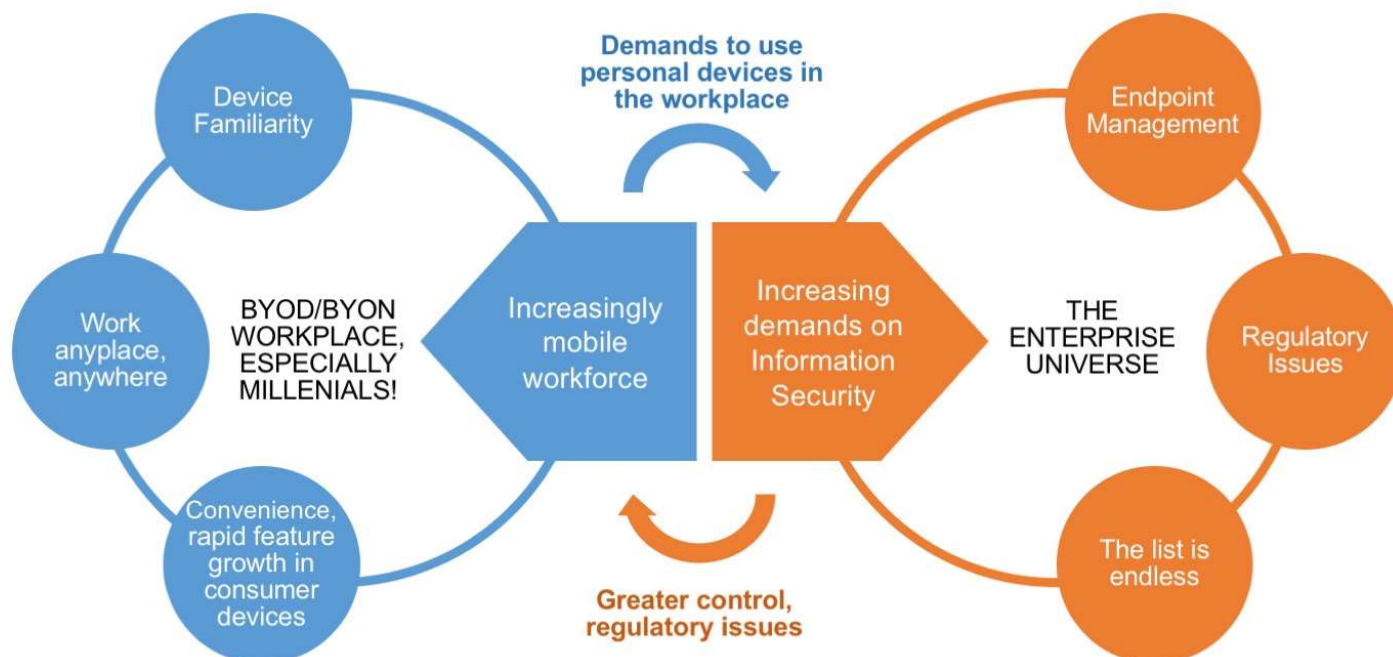


Figure 1: Coexisting Operational Environments

BYOD devices are overwhelmingly based on personal preference. A recent study indicates that 65% of tablets, 70% of “smartphones” are chosen outside enterprise standards and purchasing, giving significant credibility to the “urban legend” of “Ghost IT” departments and networks. Conflicting with these statistics are the growing requirements for security compliance with standards such as HIPAA, Sarbanes-Oxley, FDA 21 CFR 11, and major issues related to globally sponsored hacking, malware, and other intrusions into mobile device architectures. How does the enterprise enforce an Acceptable Usage Agreement (AUA) for BYOD devices with corporate data?

Another major issue is the monitoring and control of what applications are acceptable/denied during corporate use of BYOD including the following:

- “Personal” or networked ad hoc clouds such as YouSendIt, DropBox
- Social Networking
- Games, shareware, open access networks in public venues
- What data is collected from BYOD devices, either inadvertently via cookies, etc., or more importantly “hidden” monitoring sponsored by device manufacturers and service providers?

The Threat is Real

With this ever increasing use of portable computing and storage capability comes a liability. Information exploitation in the world today is at an all-time high. In our modern computing environment, classified government data, sensitive corporate data, personal identity & financial information, and other personal data are all under attack from a variety of assailants. There exists a wide variety of threats to your sensitive information from both casual and sophisticated adversaries. Since 2005, over 1 **Billion** records containing Personally Identifiable Information (PII) have been reported as breached in the United States alone¹. But there is no single cause for this loss of data. 25% of these data compromises are attributed to lost or stolen media, 25% to external hacking from outside a device or network, and a full 50% are attributed to a trusted user’s negligence or malicious activity. And the problems are not confined to the loss of sensitive data. Mobile devices are being exploited more and more as a means for malware infiltration into host computers and, ultimately, into enterprise networks.

The SPYRUS family of Rosetta microSDHC products has been designed with this kind of threat environment in mind. In particular, the addition of the internal SPYCOS 3.0 hardware security module as a FIPS 140-2 Level 3 certified hardware based “Root of Trust” for storage of critical information, certificates and keys has provided built in safeguards and countermeasures for a wide variety of attacks including:

- Exploitation of weak key generation
- Password Guessing Attacks (a vulnerability increased with weak passwords)
 - Offline password attack
 - Online password attack
- Identity Masquerade & Spoofing attacks
- Cryptographic Side Channel attacks

¹ From: <http://www.PrivacyRights.org> (as of 15 November 2014)

- Fault induction attacks
- Physical penetration attacks
- Unauthorized access to critical security parameters
- Replay attacks
- Hijacking attacks (“BadUSB” Exploit translated to mobile devices)

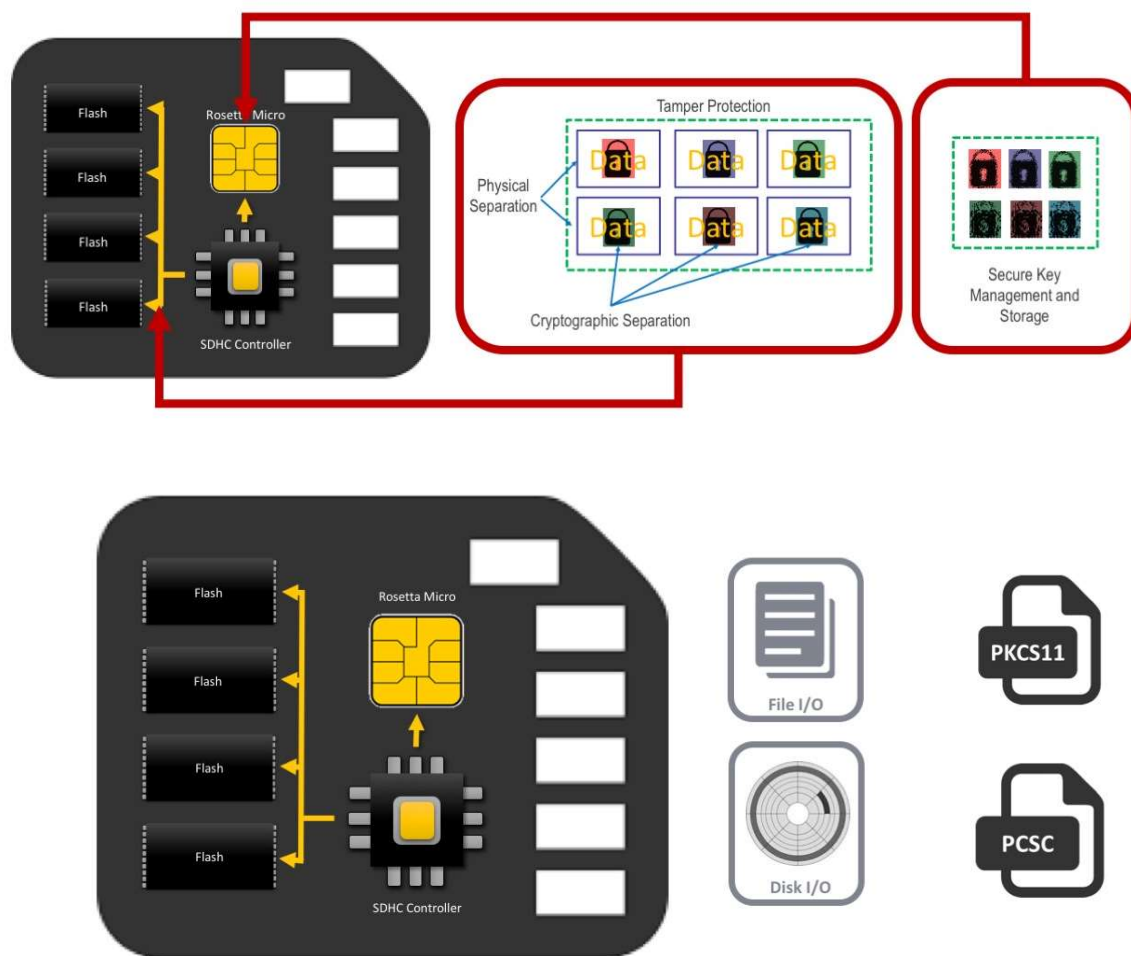
So, the threat is real; and it is naive to think that any particular person or organization is not vulnerable. In fact, there is a whole new industry of “Data Brokers” that has arisen in the last few years, collecting any and all information they can squeeze out of the digital world. And all this information is for sale. Some of these are legitimate activities and others are malicious. But at present there is little or no regulation on these activities. And the fact that these activities can and do take place from almost anywhere in the world makes monitoring and controlling them virtually impossible. Hence the need to determine if and how you want to protect your sensitive information.

This White Paper is intended to provide a technical overview that will allow you to see how the SPYRUS TrustedFlash Rosetta microSDHC products help you address this threat environment.

SPYRUS TrustedFlash Rosetta microSDHC Overview

Rosetta microSDHC Architecture

The unique design of the Rosetta microSDHC card combines secure digital (SD) technology with an integrated AES 256-bit hardware encrypting core and a secure element with public key infrastructure (PKI) technology in a standard microSDHC form factor. The Rosetta microSDHC card provides flash storage memory and a comprehensive suite of security features, implementing the strongest cryptographic algorithms and key lengths commercially available. It is designed to be a hardware trust anchor for a wide variety of mobility platforms and to provide high assurance security solutions for both commercial and classified applications functioning as a non-CCI (Controlled Cryptographic Item) device.



The PKI mode configures the file system as a standard non-encrypting flash file system.

Figure 2 Rosetta microSDHC Architecture, internal Rosetta SPYCOS[®] HSM module architecture (upper right), application architecture (lower panel).

As shown in Figure 2 (upper left), the Rosetta microSDHC card integrates the Rosetta Micro security controller with an SD memory controller with AES hardware crypto core to create a seamless microSDHC package. The Rosetta Micro is a secure element that contains the FIPS 140-2 Level 3 certified SPYRUS Cryptographic Operating System (SPYCOS®) 3.0 within a highly tamper resistant crypto processor that manages all the critical key management functions use by the SD controller and PKI functions used by public key enabled applications. This is the same cryptographic OS embedded in the Rosetta Smart Card and SPYRUS USB security devices, such as the Hydra Privacy PC® USB file and media encryption drives, the Secure Pocket Drive™, the SPYRUS Windows To Go, Linux2Go™, and Xtreme live drives, and the PocketVault™ P-3X USB 3.0 encrypting storage drives. The Rosetta Micro security controller provides a hardware trust anchor for use in security devices, applications, and processes. It also makes available a comprehensive set of cryptographic capabilities for use in existing and yet to be developed security applications as shown in the callout in Figure 1 (upper right). The SD Controller can be configured with encryption disabled to provide full access to the flash memory configured on the Rosetta microSDHC card making it available for use as supplemental, removable, and configurable secure memory for use by applications running on the host platform. When encryption is enabled, the SPRUS TrustedFlash hardware encryption mode protects access to the flash contents until the user is successfully authenticated to the Rosetta security controller.

This capability is intended to provide support for multiple platforms incorporating the Rosetta microSDHC such as mobile devices, secure digital surveillance cameras, medical diagnosis platforms, or even Internet of Things (IoT) gateways and sensor nodes. Security is assured by combining the TrustedFlash encrypted data container with Rosetta's ability to bind the authentication and key derivation process. Rosetta will establish a FIPS 140-2 Level 3 encrypted channel through the various layers of software in the local operating system, protecting the password or other authenticators from exposure within intermediate layers in addition to the secure channel created to communicate with the AES engine in the SD Controller. This encrypted channel can be established within the application as well as all the way back to a server or other cloud based execution environment via unsecured or unencrypted links.

For mobile or other devices requiring authentication to a specific user as a digital proxy, the Rosetta microSDHC's combination of TrustedFlash encrypted flash storage and strong Suite B authentication capabilities provide a secure environment for the storage of biometric templates for authentication, their verification, and the separation of processing in the final matching and verification within the trusted boundaries of the internal Rosetta SPYCOS PKI HSM.

Because SPYRUS is first and foremost a security company, the SPYRUS TrustedFlash Rosetta microSDHC devices have been designed and architected with security in mind. Figure 2 (bottom panel) is a snapshot of application interfaces. They provide some of the strongest military-grade hardware encryption commercially available. The on-board hardware security infrastructure includes AES-256, ECDH (and ECDSA with defaults of ECC P-384), and SHA P-384, which together make up the US Government's Suite B cryptography, and extends the capabilities to ECC P-521 and SHA-512 which exceed the Suite B requirements. But strong crypto is only one part of a high assurance solution. To be effective, cryptography needs to be implemented and applied in a manner that effectively addresses the threat environment described earlier in this paper. The Rosetta strong hardware trust anchor within the microSDHC is shared by other members of the SPYRUS token family, including SPYRUS Windows To Go live drives, P-3X encrypting USB 3.0 smart drives, and Hydra PC file encryption drives. Rosetta NcryptNshare™ applications leverage this capability by using Rosetta as a strong

hardware trust anchor and build on this to not only protect data-at-rest but also to provide a high assurance processing environment while your data is in use.

[Note: Details on the FIPS certification of the SPYCOS 3.0 package, including the security policy used and all certified algorithms, can be found on the NIST web site for FIPS Certificate 2390 at:
<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2015.htm>.]

SPYRUS TrustedFlash and Rosetta microSDHC PKI Features

The Rosetta SPYCOS security controller is the hardware trust anchor within the microSDHC providing a comprehensive suite of cryptographic features and capabilities. As cryptographic requirements have changed and evolved over time, SPYRUS has remained a demonstrated leader in the industry. As our customers require new algorithms and longer key lengths, SPYRUS has supported algorithms to include 2048-bit RSA, AES-128/192/256, XTS-AES 256-bit two key, ECDH, and SHA-224/256/384/512 key lengths advocated by industry and the U.S. Government. SPYRUS also supports elliptic curve cryptography (ECC) using the NIST approved high-strength P-256, P-384, and P-521 curves that meet or exceed U.S. Government Suite B standards. The ECDSA digital signature standard and the EC Diffie-Hellman key establishment schemes are supported in accordance with NIST SP 800-56A Key Establishment Guidelines.

SPYRUS TrustedFlash hardware based full disk encryption of the flash memory on the Rosetta microSDHC PKI is available. Additionally, sector based virtual vault encryption (i.e. full disk encryption) is available when Rosetta microSDHC is configured with the optional Rosetta NcryptNshare (RES) Disk application. RESDisk™ is a full volume encryption application with a hybrid key management scheme that merges hardware key management with XTS-AES 256-bit symmetric encryption in software to create any number of encrypted disks that can be shared with other RESDisk users. In addition, the RES2Go™ application can be used to uniquely encrypt each file saved within the flash memory on the microSD card and target it for secure sharing with a specified set of trusted recipients. These security applications can be used individually on the Rosetta microSDHC or they can be combined for an even higher assurance memory or network storage solution.

SPYRUS TrustedFlash and Rosetta microSDHC PKI devices are currently available in 4 GB, 8 GB, and 16 GB capacities, with 32 GB available in 2016. Specialized versions with a minimal amount of memory, e.g. 128 Mbytes, are available for large volume, cost sensitive applications requiring high assurance PKI authentication capabilities coupled with minimal flash storage such as telematics, vetronics, electronic payments, telemedicine and related applications. Selected models are available in extended temperature ranges for austere industrial and defense environments with 100% device functionality testing.

The following table is a summary of the high level features of the current Rosetta microSDHC family.

Table 1: Rosetta microSDHC Features

Rosetta microSDHC Parts	Available Flash Sizes	AES-256 Hardware Encryption	Integration with NcryptNshare family of products	Full Cryptographic Functionality	Extended Temperature Range*
PKI, no hardware encryption of flash	4GB, 8GB, 16GB	Available	Yes	Yes	No
PKI, TrustedFlash hardware encryption of flash	4GB, 8GB, 16GB, 32GB, 64GB	Ask for information	Yes	Yes	Yes
PKI, limited size flash	Custom Sizes	Ask for information	Yes	Yes	No

(*) - 25° C to + 85° C 100% device testing

SPYRUS Trusted Flash Rosetta microSDHC PKI Security Features

Rosetta Hardware Security Module – An Anchor of Trust

Enforcement within any strong security solution must be anchored in some point of trust. There must be something you trust to hold up to and defend against the threat environment within which you are trying to establish a secure solution. Within every Rosetta microSDHC there is a FIPS 140-2 Level 3 certified Rosetta SPYCOS security controller to which all security is anchored. As a hardware trust anchor this controller provides superior protection to any software trust anchor that can be provided. The cryptographic security boundary of this controller is the die itself, so that it can be embedded in other products for specialized applications. This is the trust anchor embedded in all the various form factors of the Rosetta microSDHC product family.

The main advantage of hardware based security is its ability to implement robust, built in counter measures to address a variety of physical and logical attacks commonly leveled against security applications and processes. The goal of most of these attacks is to access, expose, and/or exploit the critical security parameters (such as cryptographic keys) that must be kept secret if the security of a process is to be maintained. Protecting these within a hardware security boundary provides an isolated environment in which strong protection mechanisms can be employed. Many of these security features within the Rosetta SPYCOS security controller are built into the processor chip on which SPYCOS runs. This chip provides an enhanced level of on-chip security features to fulfill the strong security requirements of a Common Criteria evaluation at an EAL-5 level. These countermeasures include a wide variety of hardware tamper detection circuits and physical protection shields. Advantage is taken of all these within the SPYCOS firmware to enhance the overall security profile of the device. When tampering is detected, countermeasures are employed to protect the critical security parameters within the processor.

In addition to taking full advantage of the hardware tamper alarms and physical protection mechanisms in the chip, the SPYCOS firmware takes a variety of its own steps to assure a high level of security in its operation. SPYCOS *never* stores the password or other authentication factors on the device. The user password is only one of multiple factors used to derive a Master Key Encryption Key (MKEK) used for validation. The MKEK is not a password-based key generated using an algorithm such as PBKDF2, nor is it ever stored in static memory. The MKEK is generated by the full entropy FIPS 140-2 Level 3 certified Random Bit Generator (RBG) onboard the device and is re-derived each time an authentication takes place using a provably secure multi-factor algorithm. All keys and other critical security parameters are stored within the hardware secured and hardware encrypted internal EEPROM with an additional layer of software encryption using AES 256-bit encryption with this MKEK. SPYCOS also has carefully implemented its algorithms to minimize their vulnerability to sophisticated side-channel exploitation techniques. Finally, SPYCOS employs a variety of built-in tests and evaluation processes to make sure its cryptographic operations and protection mechanisms remain fully operational.

Altogether, these features enable a highly secure, hardware protected processing and storage environment which provides a superior trust anchor for Rosetta microSDHC secure operations.

Entropy – The Soul of Security

The degree to which cryptographic keys and other critical security parameters can be trusted is inversely related to how easily they can be revealed, predicted, or guessed by an adversary. If your cryptographic keys are known, you have no security. As a result, the very core of security in a cryptographic system rests on how random (or unpredictable) its critical security parameters are. In a cryptographic system, this lack of predictability is loosely referred to as entropy.

[Note: This is a gross over-simplification of the issue but for the purposes of this paper, it will serve for a working understanding. In actuality, entropy is a measure of unpredictability of information content. Claude Shannon did much of the foundational work on the concept of entropy and many cryptographers and information theorists have added to this body of knowledge. Much can be gained from an understanding of this, but for the purposes of this paper, that will be left for an independent exercise by the reader.]

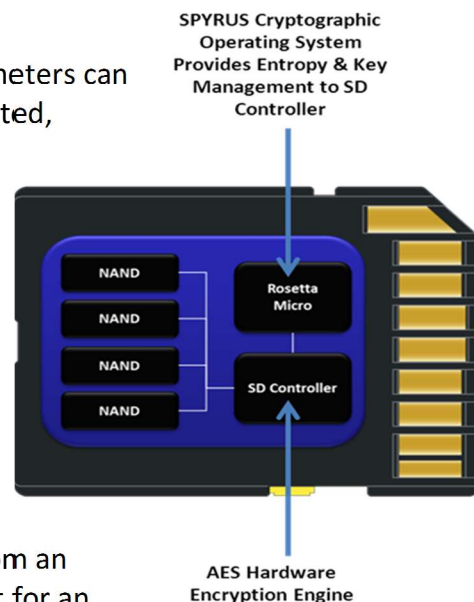
The Rosetta microSDHC uses the FIPS 140-2 Level 3 certified Random Bit Generator (RBG) on the Rosetta SPYCOS security controller for the generation of keys and other critical security parameters. It conforms to the SP800-90 series of DRBG specifications using the Hash DRBG mixing algorithm. At factory initialization time it is instantiated with entropy from both external and internal (from a true hardware NDRNG embedded in the processor chip) sources. The goal is to maximize the entropy in values generated by the RBG on board the Rosetta SPYCOS security controller.

When generating and using cryptographic keys, special care is taken to assure that they are strong (high entropy) and that they are protected against most attacks. Whenever a private key is generated the RBG is re-seeded from the entropy pool stage of the DRBG. In addition, RSA keys are generated in accordance with the latest SP800-90A DRBG specification, as required for FIPS 140-2 Level 3 certification. In addition particular care is taken with all cryptographic operations performed within the processor to defend against possible penetration and side-channel exploitation attacks.

Multiple Contexts and Separation

In most mobile platform environments it is common practice to operate more than one application at the same time. And with the increasing number of BYOD/BYOC devices operating in enterprise environments, security concerns demand that these applications perform in their own application contexts with strong operational separation between them. When those applications are concerned with security and protecting both the user's PII data and the enterprise IP, the issues of "sandboxing" and strong firewalling within a single operational platform become even more critical. The Rosetta microSDHC was designed with this type of working environment in mind.

Each application context within the Rosetta security controller operates within its own application directory and maintains its own, cryptographically unique environment. Each of these is strongly firewallled from the others to maintain its own operational sandbox. The separation methodologies used by SPYCOS include



logical, cryptographic, tamper protection, and physical separation. Figure 3 depicts the multiple layers of the security topology used within the Rosetta microSDHC.

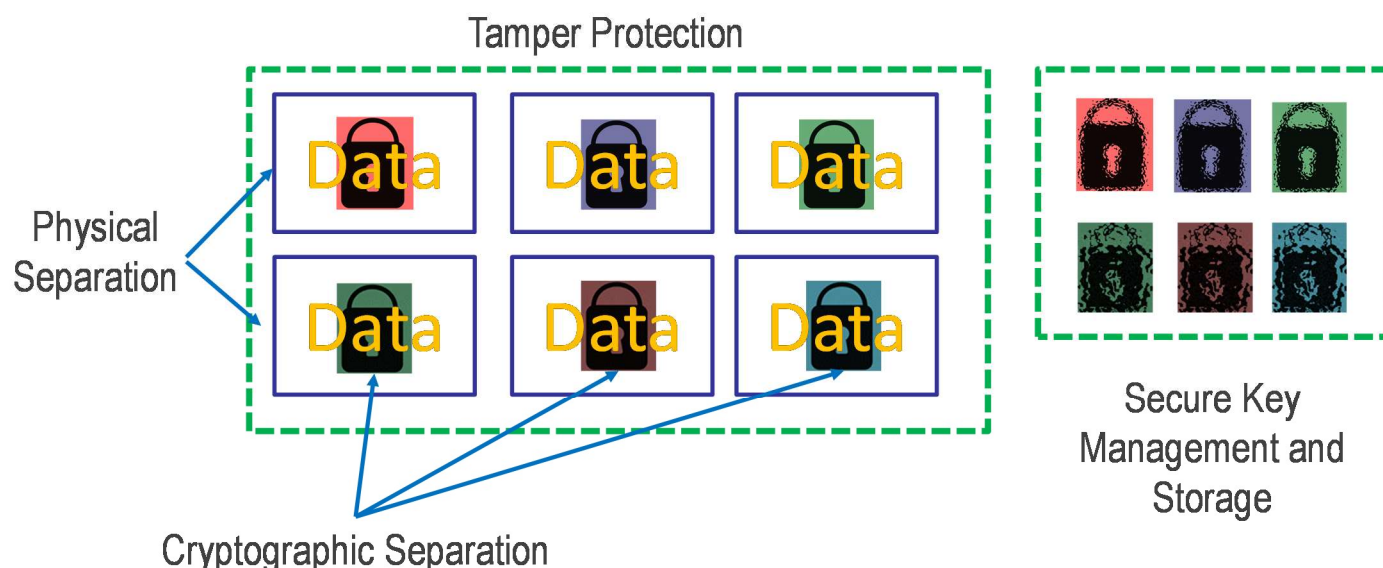


Figure 3: Anti-Tamper. Physical, Cryptographic Separation and Secure Key Management Protection Context Separation in Rosetta microSDHC

When an application directory is created, it contains its own MKEK and authentication factors. The operational application contexts are also mutually exclusive – no two can be activated and in use on the module at the same time. This way, critical security parameters are never exposed to the wrong security context.

Through the use of a dedicated security module implementing state of the art hardware anti-tamper mechanisms within the Rosetta security controller, keys maintained within the security boundary are kept secure. All of the applications cryptographic keys are protected safely within the tamper-resistant and temper-evident hardware in the Rosetta SPYCOS controller. They are not accessible by reading the FLASH chips and are not accessible via hardware hacks such as enabling a JTAG interface. Physical separation in this context refers to the storage of critical security parameters in secure memory dedicated to preventing unauthorized access separate from the main system. Furthermore, the strong physical protection of all the critical security parameters is also maintained between applications, even though one of those applications may be authenticated to the drive.

But physical separation from the host processor in a separate hardware controller is only one of the protection mechanisms employed. In the event of a physical attack against the Rosetta module and its contents, all cryptographic keys and data within the module are deleted. This level of tamper protection is a key discriminator for a Rosetta-based secure element as compared to the built-in TrustZone features of some mobile chipsets.

For logical separation, mandatory access control is applied to objects stored in a hierarchical file system. In this way, the keys and data are sandboxed based upon successful authentication to the security context. When the context is changed by selecting a different application directory, the data objects contained in the previously selected application directory are no longer accessible.

Finally, cryptographic separation is also enforced since each application context has a unique set of authenticators and a unique MKEK, providing a completely independent cryptographic environment. All of these are generated using the FIPS approved RBG within the Rosetta security controller and are never exposed outside of the security boundary of the Rosetta chip. This way, the application keys and other critical security parameters encrypted by an application's unique MKEK are unrecoverable without explicitly logging on to that application. In addition, the context can be bound to a user or to a user and additional security contexts outside of the Rosetta parameters through the use of multiple authentication factors. Authentication to an application directory can be configured to use a standard user logon requiring a user to supply up to a 128 octet authenticator, usually a password. Every bit is used during the authentication process. Alternatively, multi-factor authentication may be used to bind the logon to up to two other external entities. These entities may be the devices into which the Rosetta microSDHC is inserted, the machine to which the device is connected, the network to which the device is connected, etc.

Each of these layers of protection provides a level of assurance for securing access to keys and other critical security parameters that is unsurpassed by any other similar commercial solution.

Rosetta microSDHC Separation in a Mobile Host Platform

Most current Windows and Linux operating systems support access to an external security module such as the Rosetta microSDHC using standard or readily available drivers. Applications in these environments can easily make use of the security resources available in the Rosetta microSDHC using the available mini-driver or PKCS #11 interfaces.

Android, however, does not yet support, in the standard branch, external security modules. Some applications that run on Android have added support for smart cards but not for crypto-modules to support system level services. Adding support for a FIPS 140-2 level 3 certified RNG, key store, crypto-engine or secure storage could be added but requires a custom ROM. Key libraries could be written to replace or augment native cryptographic services used by the kernel and offered to the application by the Android runtime environment. This approach also requires significant expertise to customize and to maintain a custom ROM. It requires rooting a device and replacing the custom ROM, typically voiding the manufacturer's warranty. This requires a significant tradeoff between high assurance and high maintenance and cost.

Rosetta microSDHC provides an interface that makes integrating into applications easy and can be done without requiring changes to the ROM, does not require root privilege, and can be incorporated easily into applications installed from Google Play or from an enterprise MDM framework. Examples of applications that can be modified to use the Rosetta microSDHC as an application secure element are:

- SPYRUS TrustedFlash
- SPYRUS NcryptNshare Applications
- SPYRUS Security in a Box® SDK for Android
- E-Mail

- VPN
- File Sharing
- SMS
- Voice
- Instant Messaging
- Any application requiring PKI credentials for authentication and encryption

For example, the stock email client supporting IMAP/POP/Exchange mail can be modified to use Rosetta microSDHC rather than the native Android keystore which may or may not be rooted in hardware. Even if it is rooted in hardware, it is not protected to the degree it is within the Rosetta microSDHC.

Separation between applications can be enforced by using different security contexts within the Rosetta microSDHC. This allows logical and cryptographic separation between the keys and credentials in different contexts. It is also possible for applications to share a context and therefore share all data within it.

With this type of integration of a secure element on Android, each application “containerizes” its data within the FIPS certified module. The separation is on an application-by-application basis. An enterprise application can be installed alongside a personal application but is protected using a different set of credentials and is separated physically and cryptographically from each other. The enterprise application can make use of multi-factor authentication requiring access to the data by an authorized user and while accessing an authorized computer or network. Access to the secure element can also be bound to secure device measurements on platforms that support such operations (like TrustZone on Samsung Galaxy phones).

SPYRUS TrustedFlash and Rosetta microSDHC PKI Applications

Security Applications Using Rosetta microSDHC

TRUSTED MOBILITY SOLUTIONS: ROSETTA NCryptNShare™ FAMILY OF APPLICATIONS




Built on Rosetta hardware and software security platform



Figure 4: Rosetta NcryptNshare Applications Using Rosetta microSDHC. Other members of the SPYRUS hardware token family supporting Rosetta NcryptNshare are shown for completeness.

The SPYRUS TrustedFlash features in the Rosetta microSDHC family has been integrated with the Rosetta NcryptNshare file sharing product line. End-to-End Encryption between senders and recipients protects data at rest and data in transit with FIPS 140-2 Level 3 hardware assurance, the most comprehensive multifunction security solution available today for collaborative workflow processing. The Rosetta NcryptNshare is the only available product that integrates the four essential transaction security processes --- military-grade encryption for confidentiality, digital signature for file integrity, certified time-stamping of document existence and non-repudiation of owner identity --- and uniquely protects these processes from cyberattacks by enveloping the critical security parameters within the SPYRUS Rosetta FIPS-140-2 Level 3 Hardware Security Modules (HSMs). The presence of all these factors enables files to be qualified as forensic evidence for transaction records of all types, and to be protected over decades of storage or use. A summary of the secure storage and file sharing applications include:

- **SPYRUS TrustedFlash microSDHC** is a PKI secure element integrated with hardware-encryption to protect all data stored on the embedded flash of the Rosetta microSDHC card. Public key enabled applications can use the Rosetta microSDHC when combined with the SPYRUS PKI libraries.

- **RESDisk** is an encrypted Virtual Volume application that uses Rosetta for key management in combination with the SPYRUS XTS-AES 256 crypto library to create multiple encrypted virtual volumes on Rosetta microSDHC devices, other storage media, or network share drives that can be shared among other RESDisk users. 
- **RES Pro™** is a Windows Explorer Extension application that provides encryption and decryption “in place”. RES Pro works with any Rosetta FIPS 140-2 Level 3 SPYCOS 2.4 or 3.0 device as hardware root of trust and files can be securely shared with other RES Pro users. The software license is bound to a computer and does not support Touch screens. 
- **RES4Office™** is an add-on application for Microsoft Office 2010, 2013, 2016, and Office 365. Once installed to Word, PowerPoint, Excel, Visio, or Project, an NcryptNshare ribbon is enabled to encrypt, decrypt or share the enabled Office applications using any Rosetta enabled device. Sharing is supported using Outlook, Skype for Business, Skype, Sharing, and popular cloud collaboration solutions. 
- **RES2Go** is a standalone application that is licensed to a SPYRUS encrypting storage device, which can be moved across computers and does not require any installation of software on the host. RES2GO uses a “VAULT” concept meaning that all encrypted content will be added to “VAULT” and stored on the SPYRUS device. RES2GO is designed to work with any Rosetta SPYCOS 2.4 and 3.0 storage hardware (P-3X/WSP/WS/PocketVault/Rosetta microSDHC) device.

Organizations can realize cost and efficiency savings in their choices of networks and cloud services because each file is separately encrypted with its own key and protected as it flows from sender to collaborative recipients over unsecured networks and public cloud services. This allows organizations to select the most economic IT resources without compromising the security of information exchange and also eliminates the overhead of maintaining separate encryption key management vaults for combinations of these services. IT operations can be simplified because the cloud services and network transport of recipient and sender organizations can be different, and the same shared-file level protection is maintained even when multiple copies of a transaction are sitting on different vendor cloud servers.

SPYRUS Rosetta NcryptNshare file encryption and secure sharing features provides superior confidentiality through the use of Elliptic Curve Cryptography with key size of P-384 together with AES-256 symmetric encryption that is ideal for use for forensic records and transactions. Secure storage of encryption keys, password protection and authentication and system integrity testing are implemented by an internal Rosetta Hardware Security Module.

As shown in Figure 4, files can be shared with other RES users whether encrypted files are stored on the SPYRUS WorkSafe Pro, P-3X, Rosetta microSDHC, SharePoint, or in the Cloud. Each file or RESDisk encrypted disk created by the sender is protected using a unique key that is encrypted (wrapped) with a key encryption key derived from the originators Rosetta HSM along with each recipient’s public/private key pair using an EC Diffie-Hellman key agreement. The sender’s and receivers keys are conveyed in a RES Sharing Certificate that is stored in a local RES Contacts Folder. For secure data recovery, a RES Recovery Agent may be implemented

for organizations concerned about file recovery if the RES equipped device is lost or stolen. The RES Recovery Agent configures a backup RES device can be defined as a Recovery Agent so that every file that is encrypted will automatically include the Recovery Agent's RES Sharing Certificate. Depending on security policy, the Recovery Agent can optionally be set up to require two-person control and kept securely locked in a safe or a vault offsite.

Rosetta NcryptNshare Bring Your Own Key Applications

FIPS 140-2 Level 3	Intelligent detection	Sender verification	Network, mobile or cloud	Compliance
FIPS 140-2 Level 3 defense in depth security protection at the file level	Files can detect file alternation without decryption	File recipients can verify the sender to prevent masquerading	Files can be encrypted and shared on corporate networks, mobile devices, or cloud systems	SPYRUS security helps enterprises meet regulatory and compliance requirements

Rosetta microSDHC as a Secure Element for RES4Office

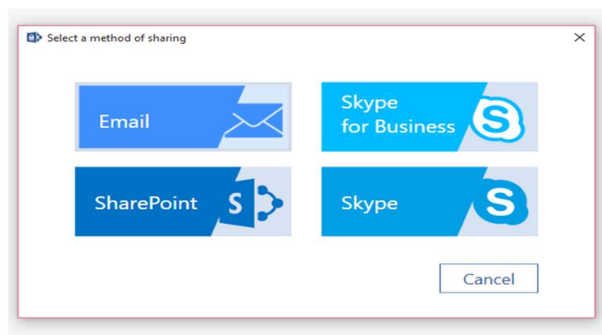
Many customers appreciate the content protection features of RES but have expressed a desire for tighter integration with Microsoft Office software, particularly Office365. The RES architecture allowed SPYRUS to easily create an additional RES application for Microsoft Office, named RES4Office, and available in Office 2010, 2013, 2016, and Office365.

RES4Office uses the same core encryption functionality used in all NcryptNshare applications. The RES4Office software application is an add-on for Office applications which will display a specific SPYRUS NcryptNshare "ribbon" on the main Office "ribbon" as displayed below for Word, Excel, PowerPoint, Project, and VISIO.



The main buttons on the SPYRUS 'ribbon' are defined to be:

1. Encrypt and Save
2. Encrypt and Share with email, SharePoint, Skype for Business, and Skype
3. Decrypt and Open
4. Manage Contacts
5. Settings



Rosetta microSDHC as a Secure Element for Android Application Container

Application container solutions for Android implement separation by combining standard and custom technologies. The application container is simply an application that “contains” other applications. This is achieved on Android by signing the application with the same code signing credential. It makes use of Android’s discretionary access control (file system permissions) and mandatory access control (Security Enhanced Linux/Android) to restrict access to objects held within the container – signed by the same key. It also adds a filtered layer of middleware between the application and the Android runtime environment so that all system calls can be mitigated. The container achieves encrypted storage by intercepting file system calls for file input and output and adds encryption. The container adds management of container and application functionality by adding remote services for setting policies that dictate what the middleware will allow the application to do.

Container solutions distinguish themselves based upon the management services they provide and the degree to which they are integrated with the platform. Since some platforms provide stronger protection from unlocking and rooting, the same container installed on different platforms will have different security profiles. Only those platforms that have a demonstrated ability to not be unlocked or rooted can be considered a secure environment. Integrating Rosetta microSDHC into the wrapper middleware of the container provides an exceptional security element for protecting all container cryptographic keys and credentials.

In a similar manner the file system interface calls are shimmed to add encryption and the key container, and other cryptography API’s can be shimmed to use the Rosetta microSDHC rather than the Android container. This approach provides a known FIPS 140-2 Level 3 validated security profile for securing keys and other critical security credentials when the implementation across various platforms is not consistent.

Summary

SPYRUS's family of Rosetta microSDHC devices and applications provide contractors, remote workers, and telecommuters with a complete operating environment and security functions for mobile devices that includes extensive FIPS 140-2 Level 3 rated authentication coupled with a variety of secure storage and sharing solutions for securing the mobile device of choice for the BYOD/BYON enterprise user. All Rosetta microSDHC versions feature superior security defense of the operating system, documents, and identity credentials from tampering and theft with layered hardware and software encryption depending on the particular model.

Technical leadership, SPYRUS TrustedFlash hardware security, onboard FIPS 140-2 Level 3 PKI capabilities, and the integration with new mobile device applications including payment systems, VOIP, collaboration, and interactive data analytics applications make the SPYRUS Rosetta microSDHC family the choice for secure mobile device platforms.

The entire family of devices is intended to also maintain compatibility with the optional SPYRUS Enterprise Management System (SEMS™) in 2016. Combining a public key with a smart card-enabled ecosystem and SPYRUS security applications extends a true end-to-end security approach for enterprise smart card and PKI infrastructure to mobile users for authentication to applications and networks.

Typical use cases of the Rosetta microSDHC product line is to protect email, sensitive personal or corporate information, video recordings of body cameras and surveillance systems, Office files, pictures, tax and banking information, images captured on medical imaging systems, voice, text, and more.

Please visit the SPYRUS website at www.spyrus.com to find out more or contact a sales representative at info@spyrus.com or sales@spyrus.com.

Appendix – SPYRUS Product References

A link to the data sheet for the Rosetta microSDHC family as well as related SPYRUS Windows To Go products has been included with this paper for easy reference and comparison. In addition, a link for the SPYRUS Enterprise Management System datasheet is included to provide a more comprehensive overview of how the drives would operate within a managed enterprise environment. Altogether, datasheets for the following products are included:

- Rosetta microSDHC <http://www.spyrus.com/wp-content/downloads/400-313001-14DSRosettaSDHCCard.pdf>
- Rosetta Micro Series II and Series III
<http://www.spyrus.com/wp-content/downloads/400-100035-17DSRosettaMicro.pdf>
- Rosetta Series II and Series III USB and Smart Card
http://www.spyrus.com/wp-content/downloads/400-100000-17DSRosettaSeriesIISC_USB.pdf
- Rosetta NcryptNshare RES Disk
<http://www.spyrus.com/wp-content/downloads/400-520001-02RESDisk.pdf>
- PocketVault™
<http://www.spyrus.com/company/literature/SPYRUSdatasheets/DSPVEPro.pdf>
- WorkSafe and WorkSafe Pro
<http://www.spyrus.com/wp-content/downloads/400-451001-05WorkSafe and WorkSafe Pro.pdf>
- Portable Workplace and Secure Portable Workplace
<http://www.spyrus.com/wp-content/downloads/400-450002-04DSPW-SPW.pdf>
- Windows To Go XTreme
<http://www.spyrus.com/wp-content/downloads/400-530001-01WTG Xtreme.pdf>
- SPYRUS Enterprise Management System
http://www.spyrus.com/wp-content/downloads/400-420001-11_DSSEMS.pdf

Additional information and technical details for these products can be obtained from SPYRUS, Inc. following the execution of an appropriate Non-Disclosure Agreement.