

ProtectToolkit M

Cryptographic API/Toolkit



ProtectToolkit M is a Cryptographic Service Provider (CSP) that seamlessly integrates with the Microsoft CryptoAPI (CAPI). As an Application Programming Interface (API), it enables easy incorporation of hardware-based cryptographic security into Microsoft CAPI-enabled security applications.



The CryptoAPI (CAPI) is Microsoft's Cryptographic Application Programming Interface that allows developers to add cryptography and certificate management functionality to their Win32 applications. It contains functions that allow Windows-based applications to encrypt or digitally sign data in a flexible manner, while protecting sensitive private key data. Independent modules known as Cryptographic Service Providers (CSPs) perform all cryptographic operations and form the cornerstone for Microsoft-based PKI cryptographic services.

All cryptographic keys within the Microsoft CAPI are saved within a CSP key database that can be stored either in a default software configuration on a host server, or alternatively within the superior confines of a tamper-protected Hardware Security Module (HSM).

Software-based cryptography entails several flaws, the most predominant being the storage of sensitive data on the server itself. The algorithms, cryptographic keys, clear text and cipher text reside in unprotected memory on the server, controlled by standard Microsoft software and susceptible to malicious attack, such as duplication, modification, or substitution. The most susceptible element is the cryptographic key. Compromising a key allows an adversary to recover encrypted data, falsely generate digital signatures, or intercept and change payment transactions.

ProtectToolkit M is a Microsoft CAPI CSP supplying a complete set of cryptographic operations to allow Microsoft-based applications to call cryptographic functions in the secure environment of a HSM. Such requests may include encryption, key exchange, and Message Authentication Codes (MACs).

ProtectToolkit M facilitates the ability to achieve physical and logical secure key management, generation of digital signatures, message authentication, protected communications and powerful cryptographic processing acceleration — all within the Microsoft programming environment.

BENEFITS AT A GLANCE

- Seamless out-of-the-box integration of Hardware Security Modules (HSMs) with leading software applications from global and regional software vendors that implement security solutions to Microsoft Cryptographic API (MS CAPI) standards
- Call cryptographic functions in the Microsoft Cryptographic API (Microsoft CryptoAPI or Microsoft CAPI) and have these requests passed through the physical and logical FIPS 140 certified security of a HSM, rather than the host system
- Securely generate, store and use cryptographic keys within the secure environment of a FIPS 140 certified HSM, avoiding the risk of exposing sensitive keys as clear text in working memory when performing cryptographic operations
- Strengthen Microsoft Certificate Services (PKI) and Information Security Server (IIS), two of the most popular commercial Microsoft applications, with no-compromise, HSM-based root key and SSL Web Server private key protection
- Benefit from stronger security through support of higher key lengths (up to 4096 bit RSA) compared to the default Microsoft "Base", "Strong", or "Enhanced" cryptographic providers, which offer a maximum of 1024 bit RSA security
- Speed up CPU-intensive cryptographic operations that typically impede host server performance. **ProtectToolkit M** enables cryptographic processing to be offloaded to dedicated HSMs removing processing bottlenecks and relieving the Microsoft-based host application to concentrate on other critical application processing tasks
- Choose from a variety of HSM form factors (PCI card or external, network-attached module) and performance options

PRODUCT DATA SHEET

SEAMLESS OUT-OF-THE-BOX INTEGRATION

As a plug-in CSP, **ProtectToolkit M** seamlessly adds the hardware-based physical and logical security of a HSM to cryptographic API-compliant Windows applications. Integration requires only the installation of the HSM and selection of the relevant CSP via the configuration setup of the Windows application. Windows GUI-based key management and device management utilities simplify the process of integration and deployment.

SafeNet constantly monitors, tests and upgrades its CSP to ensure its interoperability and integration with leading cryptographic API-enabled Windows applications and third-party integrations. This ensures an extensive suite of technologies are available, such as Microsoft PKI, IIS, and ISA Server, and third-party applications utilizing these technologies. For example, **ProtectToolkit M** is compliant with the latest version of the Windows 2003 PKI, providing seamless support for extended features such as the Microsoft key recovery scheme.

ACCELERATE DEVELOPMENT OF CUSTOMIZED APPLICATIONS

The entire cryptographic development environment, including APIs, tools, sample code and documentation needed to develop Microsoft CAPI applications is provided directly by Microsoft as part of their standard Windows operating system environment and additional development facilities, e.g. MSDN. Developers already familiar with Microsoft CAPI development experience no additional learning curve and can be immediately productive with **ProtectToolkit M**.

ENHANCED SYSTEM SECURITY AND PROCESSING PERFORMANCE

The strength of a cryptosystem is dependent on the storage and management of the cryptographic keys. All keys within the Microsoft CAPI are saved within a CSP key database, generally located within software on a host server. **ProtectToolkit M** allows Windows-based applications that call the Microsoft Cryptographic API (CAPI) to integrate with HSMs to achieve the highest levels of physical and logical secure key storage.

The dedicated Digital Cipher Processor within the HSM offloads CPU-intensive cryptographic processing from the host server facilitating an increase in overall system performance. This is achieved using the **ProtectToolkit M** "RSA FULL" and "RSA SChannel" CSP in place of the corresponding Microsoft CSPs.

KEY FEATURES

- Rich choice of cryptographic algorithms, including 3DES, RC2, RC4, RSA (up to 4096 bit)
- Provision of two Microsoft CAPI provider types in one package (RSA FULL and RSA SCHANNEL)
- Remote client/server operation for exporting Microsoft CAPI services across a TCP/IP network
- Scalability and high availability by supporting multiple HSMs in Work Load Distribution (WLD) mode
- Secure Channel/Trusted Path between the API (host library) and HSM (both PCI and network-attached modules)
- Dedicated Windows GUI-based HSM administration utility including functionality for:
 - HSM device management and security
 - Policy configuration (e.g. FIPS mode)
 - Firmware upgrade
 - Multi-adapter management
 - Keyset creation and space allocation/de-allocation
- Dedicated Windows-based keyset management utility providing:
 - Keyset password access management
 - Key container creation and removal
 - Key pair generation (SIGN or EXCHANGE) and deletion
 - Management of key properties (e.g. EXPORTABLE)
 - Seamless integration with Microsoft's CA
 - Key back-up and recovery and private key archiving and recovery scheme
 - Full integration with Microsoft Certificate Services (PKI) and Internet Information Server (IIS)



HSM PLATFORM OPTIONS

The protection of keys and other valuable data within a physically secure tamper-resistant HSM is paramount to achieve strong cryptographic security. The storage of keys within a software-only solution greatly diminishes the security against malicious attack due to a hacker's ability to infiltrate and compromise keys from the file system or working memory.

ProtectToolkit M operates seamlessly with the HSMs listed below.

PROTECTHOST ORANGE

ProtectHost Orange is a FIPS 140 - 2 level 3 certified network-attached HSM that connects to a single machine or a complete network as a central cryptographic subsystem to perform symmetric and asymmetric cryptography.



PROTECTSERVER ORANGE EXTERNAL

ProtectServer Orange External is a FIPS 140 - 1 level 3 certified network-attached HSM that connects via TCP/IP to a single machine or complete network (LAN) as a central cryptographic subsystem to perform symmetric and asymmetric cryptography.



PROTECTSERVER GOLD

ProtectServer Gold is a FIPS 140 - 2 level 3 certified PCI adapter-based HSM that can be installed in server systems as a cryptographic subsystem to perform symmetric and asymmetric cryptography.



PROTECTSERVER ORANGE

ProtectServer Orange is a FIPS 140 - 1 level 3 certified PCI adapter-based HSM that can be installed in server systems as a cryptographic subsystem to perform symmetric and asymmetric cryptography.



PLATFORMS

- Windows 2000, XP, 2003
- Other platforms on request

All platforms are continuously updated, please check with SafeNet for the latest additions.

TECHNICAL SPECIFICATIONS

SUPPORTED ALGORITHMS

- Public Key Encryption - RSA (up to 4096 bits)
- Digital Signatures - RSA (up to 4096 bits)
- Symmetric Ciphers - DES, DES3, RC2, RC4
- Message Authentication Codes (MAC) - DES-MAC, DES3-MAC, RC2-MAC
- Message Digests - MD2, MD5, SHA-1
- True Random Number Generator (RNG)

CRYPTOGRAPHIC PROVIDER TYPES

- "RSA FULL" for cryptographic operations as implemented by the CSPs
 - Microsoft Base Cryptographic Provider
 - Microsoft Strong Cryptographic Provider
 - Microsoft Enhanced Cryptographic Provider
- "RSA SChannel" for SSL and TSL client authentication as implemented by the CSP - Microsoft RSA/SChannel Cryptographic Provider



ABOUT SAFENET

SafeNet (SFNT:Nasdaq) is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, digital identities and intellectual property, and offers a full spectrum of products including hardware, software, and chips.

ARM, Bank of America, Cisco Systems, the Departments of Defense, and Homeland Security, Microsoft, Samsung, Texas Instruments, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. For more information, visit www.safenet-inc.com.

Corporate: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: +1 410 931 7500 or 800 533 3958 Email: info@safenet-inc.com

WORLDWIDE OFFICES

SALES OFFICES

Australia +61 3 9882 8322
Brazil +55 11 3392 4600
Canada +1 613 723 5077
China +86 10 8266 3936
Finland +358 20 500 7800
France +33 1 47 55 74 70
Germany +49 18 03 72 46 26 9
Hong Kong +852 3157 7111
India +91 11 2691 7538
Japan (Tokyo) +81 45 640 5733
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore +65 6297 6196
Taiwan +886 2 2735 3736
U.K. +44 1276 608 000
U.S. (Massachusetts) +1 978 539 4800
U.S. (New Jersey) +1 201 333 3400
U.S. (Virginia) +1 703 279 4500
U.S. (Irvine, California) +1 949 450 7300
U.S. (Santa Clara, California) +1 408 855 6000
U.S. (Torrance, California) +1 310 533 8100

Australia +61 2 9906 2988
Brazil +55 21 2215 5765
Czech Republic +420 2 2423 6833
Germany +49 2151 3630 20
India +91 80 5110 0600
Italy +39 02 7729 7599
Netherlands +31 20 311 6540
Singapore +65 6559 3449
Switzerland +41 61 462 2010
U.S. (Roseville, California) +1 916 677 2450

Distributors and resellers located worldwide

www.safenet-inc.com