

ProtectToolkit C

Cryptographic API/Toolkit



ProtectToolkit C delivers one of the most comprehensive PKCS#11 implementations available on the market. It consists of a powerful set of utilities to assist in managing all cryptographic solutions for PKCS#11-enabled applications.



PKCS#11 (also known as Cryptoki) is the specification most relevant to current public key-based application software. It defines a technology-independent programming interface for cryptographic applications such as smart cards, authentication and validation, certificate generation and management, and for the support of emerging cryptographic services.

ProtectToolkit C is a cryptographic provider that enables secure applications to be constructed using the industry-standard PKCS#11 Application Programming Interface (API). It facilitates the ability to seamlessly integrate PKCS#11-compliant security applications into the secure confines of a SafeNet HSM to establish the highest levels of PKI cryptographic security.

The high quality API design and construction, directly in line with PKCS#11 standards, coupled with SafeNet's deep understanding of real-world cryptographic applications, facilitate ease of implementation.

The Software Development Kit (SDK) includes application building tools, libraries, sample source code and a graphical PKCS#11 token browser. It is ported to a wide range of operating systems and consists of a range of both 'C' and Java language callable functions.

Additional functionality such as certificate request generation, certificate generation, time stamping and advanced key management are all supported by SafeNet's extensions.

BENEFITS AT A GLANCE

- Seamless out-of-the-box integration of HSMs with leading software applications from the most important global and regional software vendors that implement security solutions to PKCS#11 standards
- Apply the most comprehensive PKCS#11 implementation on the market to security applications required to meet the PKCS#11 standard
- Call PKCS#11 cryptographic functions and have these requests passed through the physical and logical security of a SafeNet FIPS 140 certified HSM
- Securely generate and store symmetric and asymmetric cryptographic keys within tamper-resistant HSMs
- Speed up CPU-intensive cryptographic operations that typically impede server performance.
ProtectToolkit C enables cryptographic processing to be offloaded to dedicated HSMs removing processing bottlenecks and relieving the host system to concentrate on other critical application processing tasks
- Choose from a variety of HSM form factors (PCI card or external network-attached modules), performance options, and PKCS#11 run-time modes
- Coupled with Work Load Distribution (WLD) support and the widest server operating system coverage, **ProtectToolkit C** enables the highest flexibility in terms of scalability and availability
- A customization Software Development Kit (SDK) enables you to create your own application, or extend a SafeNet application, and operate these within the secure boundaries of a HSM

PRODUCT DATA SHEET

SEAMLESS OUT-OF-THE-BOX INTEGRATION OF PKCS#11

As a plug-in crypto provider, **ProtectToolkit C** seamlessly integrates with the leading software applications of the most important global and regional software vendors that implement security solutions to PKCS#11 standards. SafeNet constantly monitors, tests and upgrades its PKCS#11 providers to ensure interoperability, integration and compatibility with an ever-growing suite of software applications.

ACCELERATE DEVELOPMENT OF CUSTOMIZED APPLICATIONS

ProtectToolkit C provides application developers with the necessary environment and tools to facilitate accelerated development of proven and secure Cryptoki-compliant cryptographic services. The toolkit enables these cryptographic functions to be seamlessly incorporated into existing security applications designed to conform to PKCS#11 standards. Best practice tips and walk-through tutorials provide invaluable help in quickly mastering the learning curve.

The Software Development Kit (SDK) provides the software libraries, header files and reference documentation required to compile and link a program that uses the Cryptoki interface. In addition, numerous sample programs with source code and build instructions assist application development.

HSM software emulation functionality enables initial development and testing using the software-only variant of **ProtectToolkit C**. This delays the need to install the HSM into the development environment until the final testing phase (i.e. after the application is debugged and fully tested). This significantly reduces the development system setup time since no hardware and associated device drivers are required to allow testing and debugging on the development machine. This enables the developer to focus exclusively on the programming task at hand.

Next to the default ANSI 'C' API, **ProtectToolkit C** is also available with a Java PKCS#11 interface by wrapping the industry-standard PKCS#11 interface in a set of comprehensive Java classes.

In addition, the PKCS#11 functionality provided by **ProtectToolkit C** can be fully customized as a Functionality Module (FM) developed with the **ProtectProcessing** customization SDK. This also enables the existing PKCS#11 functionality to be patched, i.e. modified by some form of pre- or post-processing.

ENHANCED SYSTEM SECURITY AND PROCESSING PERFORMANCE

ProtectToolkit C enables developers to perform PKCS#11 cryptographic services on the trusted, tamper-protected, physically secure hardware security environment of a SafeNet HSM. Not only is much greater security delivered over host-based software systems, but also increased cryptographic processing performance due to the use of dedicated cryptographic hardware processors (digital cipher processors).

KEY FEATURES

- Rich choice of cryptographic algorithms, including 3DES, AES, RSA (up to 4096 bits), Elliptic Curve Cryptography (ECDSA) and SHA-2
- Additional software-only implementation in HSM emulation mode for rapid, low-cost application development
- Remote client/server operation for exporting PKCS#11 services across a TCP/IP network
- Secure Channel/Trusted Path between API (host library) and HSM (both PCI and network-attached modules)
- Software Development Kit (SDK) including application building tools, libraries, sample source code and graphical PKCS#11 token browser
- Debugging version (logger library) of **ProtectToolkit C** library supports convenient monitoring and debugging of all PKCS#11 calls
- Support of a host key storage scheme by implementation of an external token (ExtToken) library version of **ProtectToolkit C**
- Advanced key management utility offering extensive functionality including:
 - Split key entry and creation
 - Split key backup and restore
 - Smart card key back-up and restore (supporting an n-of-m secret sharing scheme)
 - Both graphical and console versions available
- GUI-based token browser offers the capability to create, delete, examine, test and modify tokens in a convenient, user-friendly environment. This is accomplished by graphically showing PKCS#11 tokens along with cryptographic information and services in a hierarchical directory tree. The split window display features a representation of the slots and tokens in the first panel, and service/operations buttons in the other panel. Drag 'n' drop and right click context-based processing support provides the highest degree of convenience and efficiency



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 security against malicious attack due to a hacker's ability to infiltrate and compromise keys from the file system or working memory.

ProtectToolkit C 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.



PROTECTSERVER BLUE

ProtectServer Blue is an ITSEC certified PCI adapter-based HSM that can be installed in server systems as a cryptographic subsystem to perform symmetric and asymmetric cryptography.



PLATFORMS

- Windows WIN32, NT 4.0, 2000, XP, Server 2003
- Solaris (SPARC), 2.7, 2.8, 2.9
- Linux kernel 2.2, 2.4, 2.6 (Intel), Red Hat, Fedora and SuSE
- SCO UnixWare 7, OpenServer 5
- HP-UX 11i (PA-RISC and Itanium)
- AIX 5.2, 5.3
- Remote PKCS#11 client easily portable to support other operating system environments
- Other platforms on request

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

MECHANISMS

The PKCS#11 standard defines a mechanism as "a process for implementing a cryptographic operation". In short, it is a cryptographic algorithm, a sequence of algorithms, or a protocol. The mechanisms currently supported by **ProtectToolkit C** include:

- Public key encryption - RSA up to 4096 bit
- Key agreement - Diffie Hellman (DH) up to 4096 bit
- Digital signatures - RSA (up to 4096 bit), Digital Signature Algorithm (DSA, 1024 bit), ECDSA (NIST reference curves, e.g. P-224, P-384, P-521)
- Symmetric Ciphers - AES, DES, 3DES, IDEA, CAST-128, RC2, RC4, SEED, PKCS#5 Password Based Encryption (PBE)
- Message Digests - MDC2, MD2, MD5, SHA-1, SHA-256, SHA-384, SHA-512, RIPEMD-128, RIPEMD-160
- Message Authentication Codes (MAC) - AES-MAC, DES-MAC, 3DES-MAC, X 9.9, X9.19, CAST-128-MAC, IDEA-MAC, HMAC-MD2, HMAC-MD5, HMAC-RIPEMD128, HMAC-RIPEMD160, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, SEED-MAC, SSL3-MD5-MAC, SSL3-SHA1-MAC
- Certificate handling - PKCS#10, X.509, PKCS#7 decode, PKCS#12 key and certificate import
- Key management - Random generation, Split custody key entry, N-of-M secret sharing
- Key derivation - XOR, concatenation, DH Derive, ZKA MDC2 Derive
- Miscellaneous - SSL mechanisms



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