certicom™
securing innovation

Security Builder® IPSec™ 3.2

virtual private network (VPN) module for IPv4 and IPv6 networks

Provide your customers with efficient, standards based and secure VPN access: Based on the award-winning movianVPN technology, Security Builder IPSec 3.2 is a cross-platform IPSec module that enables developers to easily embed standards-based VPN access into resource-constrained devices. With the smallest code size and widest support for industry-leading VPN gateways, Security Builder IPSec 3.2 provides efficient security and enables better performance than is normally achievable with traditional IPSec implementations.

Security Builder IPSec 3.2's support for the latest industry standards, including IPv6, IP Key Exchange version 2 (IKEv2) and MOBIKE, enables developers to use it for advanced applications such as Unlicensed Mobile Access (UMA), Internet Multimedia Subsystems (IMS), Fixed Mobile Convergence (FMC) and other emerging third generation partner project (3GPP) services. When configured with Security Builder GSE, a FIPS 140-2 Validated cryptographic module, it also provides government-approved security.

smaller and faster

Security Builder IPSec 3.2 builds on Certicom's expertise with constrained platforms and can be used to secure communication on a variety of devices. Compile the code to provide only those features you need for compact implementations and gain better performance than is normally achievable with traditional IPSec. Elliptic Curve Cryptography (ECC)-based algorithms—supported by industry leading VPN Gateways—enable faster key exchanges, while IKEv2 provides for greater standardization and faster IPSec tunnel negotiations

comprehensive security

IPSec has matured into the leading VPN protocol. This maturity allows Security Builder IPSec 3.2 to support a variety of cryptographic algorithms including 3DES, AES, ECDH, RSA, Diffie-Hellman, SHA-1, SHA-2, MD5 and EAP. Security Builder IPSec 3.2 also provides authentication support for one-time-password tokens (i.e. SecurID or Safeword). This can be further extended to provide support for smartcards and cryptographic hardware acceleration.

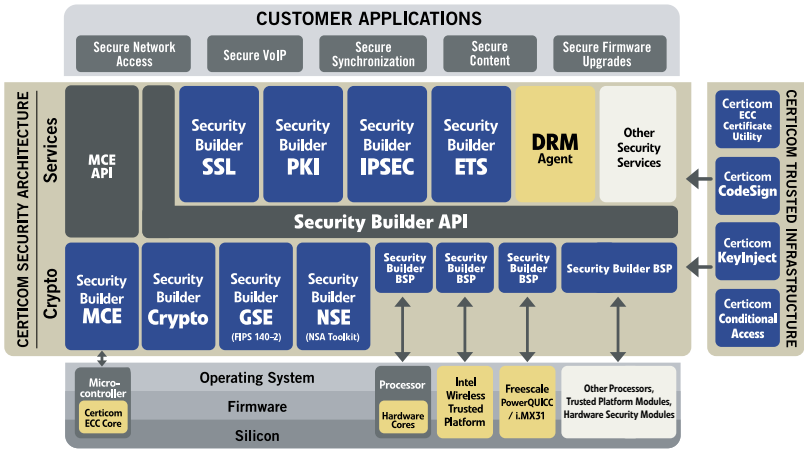
immediate VPN compatibility

With most other IPSec toolkits, a developer must test and create a compatible implementation with each individual VPN gateway vendor. Security Builder IPSec 3.2 includes pre-defined profiles that allow immediate compatibility with most leading VPN gateway vendors , including support for IPv6 networks. Certicom continually monitors VPN compatibility and adds new features regularly so that developers can focus on their primary development goals, not VPN updates.

part of a comprehensive architecture

Security Builder IPSec 3.2 is one of the security protocol modules that form the Certicom® Security Architecture™ – a comprehensive, portable and modular solution designed to allow developers to quickly and cost-effectively embed security into applications and across multiple families and generations of devices.

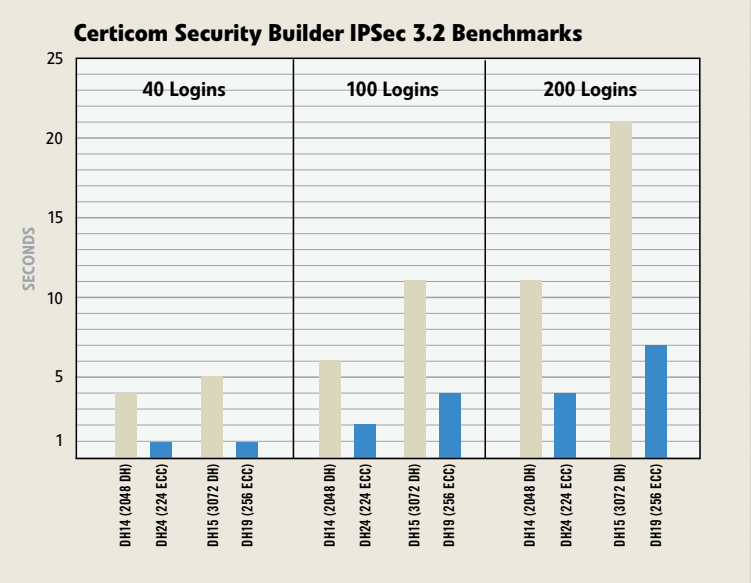
Security Builder® IPSec™ 3.2 is part of the Certicom Security Architecture, a comprehensive, portable and modular security platform that includes: software cryptographic providers that offer FIPS 140-2 Validation and meet NSA guidelines for ECC; security services like SSL, IPSec, PKI, DRM and Embedded Trust Services (ETS); hardware security cores and board support packages (BSP) that expose cryptographic functionality available in hardware.



Features

	Security Builder IPSec 3.2
Programming Language	C
IPSec Features	
IPv4	✓
IPv6	✓
IKEv2	✓
MOBIKE	✓
Mobile IP Interface	✓
IKE Aggressive Mode	✓
IKE Main Mode*	✓
IKE ModeConfig*	✓
EAP-SIM	✓
EAP-TLS	✓
EAP-AKA	✓
EAP-MD5	✓
NAT-T Support*	✓
Perfect Forward Secrecy	✓
IPSec ESP	✓
Tunnel and Transport Mode	✓
Multiple Tunnels	✓
Rekeying	✓
Dead Peer Detection	✓
IPSec Authentication	Password or Pre-Shared Key, Extended Authentication (XAUTH)*, One-Time Passwords (RSA SecurID)*, RSA SecurID Software Token*, Hybrid Authentication*, RSA Certificates*, ECDSA Certificates*, EAP-SIM*, EAP-TLS*, EAP-AKA*
IPSec Policy Features	
Dynamic IP Allocation*	✓
DNS Server download*	✓
DNS Suffix download*	✓
Manual Keying	PF_KEY
Symmetric Encryption Algorithms	AES128,192,256, 3DES, DES
Key Agreement/Key Transport	DH768 (Group 1), DH1024 (Group 2), DH1536 (Group 5), ECDH K-163 (Group 7), ECDH B-283 (Group 8), ECDH K-283 (Group 9), ECDH B-409 (Group 10), ECDH K-409 (Group 11), ECDH B-571 (Group 12), ECDH K-571 (Group 13), DH2048 (Group 14), DH3072 (Group 15), DH4096 (Group 16), DH6144 (Group 17), DH8192 (Group 18), ECDH P-256 (Group 19), ECDH P-384 (Group 20), ECDH P-521 (Group 21), ECDH P-192 (Group 22), ECDH B-163 (Group 23)
Hash Functions	SHA-1, SHA-2, MD5, AES-XCBC-MAC-96
UI Samples	Windows Mobile 5 for Pocket PC, Windows Mobile 5 for SmartphoneWindows, Mobile Pocket PC 2003, Palm OS 5.x, Symbian 9.x
Driver Samples	Windows Mobile 5 for Pocket PC, Windows Mobile Pocket PC 2003, Windows Mobile 5 for Smartphone, Windows Mobile Smartphone 2003, Palm OS 5.x, Symbian 9,x, Linux Kernel 6.x, Windows XP
Platform Support	Linux ARM, Linux x86, WinCE 3.4 (Smartphone and PocketPC), Windows Mobile 5 (Smartphone and Pocket PC), Windows XP, Symbian 9.1, Palm OS 5.

*requires matching support from VPN gateway



Supported VPN Gateways

- Alcatel 7130 Secure VPN Gateway Family
- Avaya VSU™ Series
- Check Point™ Software Technologies VPN-1
- Cisco VPN Concentrator 3000 Series
- Cisco Secure PIX Firewall VPN
- Cisco ASA
- Cisco IOS Routers (with Easy VPN server)
- Cylink Nethawk
- Hewlett-Packard VPN SA 3000 Series
- Intel® Netstructure™ 3100 Series
- Lucent Firewall Brick Family
- Netscreen Systems
- Nortel Networks Contivity VPN Switch Series
- ReefEdge Connect Server
- Secure Computing Sidewinder™ Firewall
- Symantec Raptor Firewall and PowerVPN

A proven solution deployed worldwide

Certicom IPSec technology is already in wide use in many devices, including those developed by Motorola, Sierra Wireless, Sony Ericsson, Nortel, RIM and Samsung. To learn more about the Certicom Security Architecture, visit **www.certicom.com/csa**.

Engage Certicom Professional Services to create an end-user application.

Using Security Builder IPSec, manufacturers can develop a complete end-use application that enables secure network access from a variety of devices. Certicom Professional Services can help you create a user interface (UI), build drivers, port the toolkit to a new platform or round out other functionality to create a VPN solution tailored to your application.

about certicom

Certicom protects the value of your content, applications and devices with security offerings based on Elliptic Curve Cryptography (ECC). Adopted by the National Security Agency (NSA) for classified and sensitive but unclassified government communications, ECC provides the most security per bit of any known public-key scheme. Visit www.certicom.com.

certicom™

North America **1.800.561.6100**
EMEA **+44.20.7484.5025**
International **+1.905.507.4220**
E-mail **info@certicom.com**
www.certicom.com