IDProtect

Athena, con su amplia experiencias en el estandar de smart card, ha lanzado ID Protect con soporte PKI para proyectos de identidad que requieran un Token USB JavaCard con una memoria de 72kb certificados FIPS y IP58/68.

Soporte para MS CAPI/CNG, PKCS#11 y ILM - Listo para PKI

Al ser el ID Protect un Token USB, compatible a través del middleware IDProtect Client, con PKCS#11, Microsoft CAPI/CNG y opcionalmente Microsoft ILM, permite una integración sencilla con soluciones de seguridad y PKI líderes.

Con soporte para Cryptography API de Microsoft (CAPI) y Cryptography API: Next Generation (CNG) a través del Athena Crypto Service Provider (CSP) o Minidriver, IDProtect se integra sencillamente con aplicaciones de Microsoft Windows incluyendo Outlook, Internet Explorer así como otras aplicaciones en Windows 10, 8/8.1, 7, Vista, XP, Windows Server 2003/2008 / 2008R2 / 2012 / 2012R2, Smart Card Logon, VPN y Remote Terminal Services.

IDProtect es compatible con PKCS#11 y TokenD en LINUX y MacOS (incluyendo 10.5 y 10.6 TokenD para plataforma Intel y PPC).

IDProtect puede ser utilizado 'off the shelf' o utilizado con otras aplicaciones para satisfacer requerimientos de los proyectos más demandantes.

Opciones tecnológicas

IDprotect soporta opcionalmente las últimas tecnologías biométricas Match-On-Card y arquitecturas ILM/FIM.

Tome ventaja de la arquitectura multi-aplicación de IDProtect al cargar de manera segura aplicaciones pre o post emisión utilizando herramientas de carga ampliamente disponibles.

Adicionalmente se puede añadir soporte para IDL (ISO 18013), ICAO, IAS ECC, NIST PIV o aplicaciones de pago para expandir aún más las funciones del Token USB.

Aspectos técnicos destacados

- 72k EEPROM
- ISO 7816
- ISO IP58/68 certificado
- Full Speed USB 2.0
- Java Card™ 2.2.2
  - GlobalPlatform™ 2.1.1
  - FIPS 140-2
  - ICP Brasil
  - Soporte para Security Domain
  - Administración de memoria
  - DES y 3DES
  - RSA
  - Curvas Elípticas (EC_FP, EC_F2M)
  - AES
  - GOST 28147-89
  - SHA-1, 256, 384 y 512
  - GOST 3411
  - MS-CAPI/CNG
  - PKCS# 1,7, 10 y 11
  - X.509
  - Middleware
  - Soporte para Windows, LINUX y Mac
  - Soporte para Microsoft ILM/FIM (Opcional)
  - PKI
  - IDL (ISO 18013), ICAO, IAS ECC, PIV y Payment (Opcional)
  - Biometría Match-On-Card (Opcional)

athena

Características del dispositivo

- Full speed USB 2.0
- ISO IP58/68 certificado
- Protección contra el polvo
- Protección contra inmersión continua en agua
- Tamper Evident
- Arquitectura Secure single chip
- LED de actividad
- Dimensiones: 3.65 x 1.70 x 0.70
- Peso: 5g
- Temperatura operativa: 0°C - 70°C
- Temperatura de almacenamiento: -40°C— 85°C
- Humedad:0-100% sin condensación

Silicon Memory

- 72K EEPROM
- Típicamente más de 500.000 ciclos de Escritura/Borrado a una temperatura de 25º
- Retención de datos por 10 años

Silicon peripherals

- ISO 7816 Controller (compatible con los protocolos T=0 o T=1)
- Programmable Internal Oscillator (Hasta 40 MHz por CPU y Crypto Accelerator)
- Random Number Generator (RNG)
- Hardware DES y Triple DES DPA/DEMA Resistant
- Checksum Accelerator
- 32-bit Cryptographic Accelerator para Public Key Operations con GF(2n)

Silicon Security

- Hardware dedicado para Protection contra ataques SPA/DPA
- Protección avanzada contra ataque físicos, incluyendo Active Shield
- Sistemas de protección ambiental
- Monitores de voltaje, frecuencia y temperatura
- Protección a la luz
- Secure Memory Management/Access Protection (Supervisor Mode)

Silicon Certification

- CC EAL4+
- VISA
- CAST

Especificaciones del sistema operativo

- ISO/IEC 7816
- Sun Microsystems Java Card 2.2.2
- Global Platform 2.1.1

Protocolos de Señal y Transmisión soportados

- ISO/IEC 7816-3 y ISO/IEC 7816-4 T=0 y T=1 (default)
- Mejora de velovidad PPS
- Multiple Logical Channels (base+3)

Funcionalidades Global Platform soportadas

- Gestión del ciclo de vida
- Security domains (incluyendo verificación DAP, Delegated Management y Supplementary Security Domains)
- Protocolos de canal seguro (soporte para SCP 01 y 02)

Seguridad del sistema operativo

- Llave y valor del PIN encriptado almacenado en memoria
- Integridad de llave y PIN verificada en memoria
- Borrado de llave y PIN en terminación del Token USB

Manejo de memoria del sistema operativo

- Recolección de basura
- Optimizador de memoria

Criptografía soportada

- AES (128, 192, 256 bits)
- DES y 3DES (2 y 3 claves)
- RSA (JC 2.2 hasta 2048)
- Curvas Elípticas (EC_FP)
  - JC 2.2 longitudes de claves: 160, 192
  - JC 3.0 longitudes de claves: 224, 256, 384
  - Longitudes de claves propietarias: 521
- Curvas Elípticas (EC_F2M)
  - 163, 167, 173, 179, 191, 233, 257, 307, 367, 431
- GOST 28147-89
  - CFB, CNT, ECB, MAC 256 bits
- Generación de claves On-card
  - RSA
  - EC_FP
- Key Agreement
  - DH
  - ECDH
- Hash Computation
  - GOST 3411
  - SHA-1
  - SHA-256, 384, 512

Certificaciones

- FIPS 140-2 #1750 y #1711
- ICP Brasil

Soporte PKI

- Microsoft Crypto API (CAPI)
- Microsoft Crypto API : Next Generation (CNG)
- Microsoft ILM/FIM (opcional)
- PKCS# 1, 7, 10 y 11 (2.20)
- PKCS#15 opcional
- X.509 versión 3

Soporte PKI - Middleware

- Microsoft certified Cryptographic Service Provider (CSP) o Minidriver. Certificado (Minidriver disponible a través de Windows Update.)
- Librerías PKCS#11 y middleware para LINUX y MacOS disponibles (OSX >10.4)
- Windows10, 8/8.1, 7, Vista, XP, 2000/2003/2008/2008 R2/2012 /2012 R2
- Remote Terminal Services
- Soporte para biometría match-on-card (opcional)

Aplicaciones soportadas (lista parcial)

Windows Smart Card Logon, firma y encripción de correo en Outlook y Outlook Express (S/MIME), Microsoft Mail, Microsoft VPN, IIS SSL, OpenSSL, almacenamiento del certificado raíz de una CA Microsoft, Adobe Acrobat, Checkpoint VPN, Cisco VPN, Citrix, Lotus Notes, Novell, PGP, Netscape, IE, Google Chrome, Firefox, Mozilla Thunderbird, SSH

Aplicaciones On-card

- PKI

Aplicaciones biométricas opcionales

- Algoritmo de biometría match-on-card disponible

Aplicaciones opcionales

- IDL (ISO 18013)
- ICAO
- IAS ECC
- PIV
- Payment

Asia
1-14-16,
Motoyokoyama-cho
Tokyo, 192-0063
Tel: +81 426 607 555
Fax: +81 426 607 106

North America
16615 Lark Ave, Suite 202, Los Gatos,
CA 95032, USA
Tel: +1 866 359 2273
Fax: +1 408 608 1818

LATAM & Iberia
CL. Padre Jesús Ordoñez 5 1-B, 28002,
Madrid, Spain
Tel: +34 915 644 651
Fax: +34 915 644 651

EMEA & International
45 Beech Street
London EC2Y 8AD
UK.
Tel: +44 20 9753 9792
Fax: +44 20 9753 9792

Poland & Central Europe
ul. Kasprowicza 8a/4
31-523, Kraków, Poland
Tel: +48 602 315 641
Fax: +48 123 414322

www.athena-scs.com
sales@athena-scs.com