

SafeNet eToken 5105

1. **Prezentarea produsului**
2. **Caracteristici**
3. **Avantaje**
4. **Servicii de securitate**
5. **Aplicatii compatibile**
6. **Logare la Windows pe baza certificatului**
7. **Specificatiile tehnice ale produsului**

1. Prezentarea produsului

SafeNet eToken 5105 asigura autentificare si non-repudiere pentru aplicatii precum eBanking, tranzactii bursiere, comert electronic si tranzactii financiare.

Operatiunile integrate (RSA 1024 si 2048 de biti) ale produsului SafeNet eToken 5105 permit integrarea in arhitecturile Infrastructurii Cheii Publice (PKI). SafeNet eToken 5105 genereaza si stocheaza chei private, parole si certificate digitale in insusi mediul protejat al chip-ului sau. Cheia privata a utilizatorului este generata si stocata in permanenta pe token, aceasta nu poate fi extrasa sau dedusa.

Eficient ca si cost si usor de folosit, SafeNet eToken 5105 este un adevarat smartcard fara cititor ce poate fi mutat cu usurinta de la un calculator la altul, poate fi purtat pe breloc sau in buzunar.

Folosind tehnologie avansata de criptare, SafeNet eToken 5105 ofera atat autentificare realizata de catre doi factori (dispozitivul detinut si PIN-ul stiut). Avand integrate procesoare criptografice avansate, certificate de securitate ITSEC nivel 4 si carcasa protectoare rezistenta la apa si la loviri accidentale, SafeNet eToken 5105 este alegerea cea mai buna pentru nevoile securitatii eBusiness.

2. Caracteristici

- Suport pentru tehnologia cheii publice (PKI), cu generare a cheii pe 1024 si 2048 de biti;
- Autentificare si semnare digitala RSA 1024-bit si 2048-bit integrate;
- Nivel inalt de securitate logica si fizica, certificat FIPS 140-2 Level 3, Common Criteria EAL4+;
- Conectivitate standard Crypto API si PKCS#11;
- Stocare securizata;
- Carcasa rezistenta la apa si la loviri accidentale;
- Conectivitate Plug-and-Play;
- Interfata USB standard.



3. Avantaje

- Non-repudiere, prin folosirea unei tehnologii PKI avansate de semnare digitala - datele sunt semnate pe chip-ul din interiorul eToken-ului, separat de mediul extern;
- Generare PKI on-board - cheile private nu parasesc niciodata eToken-ul;
- Nu este nevoie de integrare speciala - eToken Enterprise este compatibil cu interfetele standard de securitate si cu o gama larga de clienti de securitate;
- Instrumente flexibile folosite pentru integrarea in aplicatii;
- USB portabil -nu este nevoie de un cititor special;
- Autentificarea se realizeaza de catre doi factori - este nevoie atat de eToken, cat si de parola;
- Stocare securizata a cheilor utilizatorilor, precum si a altor informatii personale.

4. Servicii de securitate

- Servicii financiare online - autentificarea si semnarea tranzactiilor in cazul aplicatiilor de eBanking si a celor bursiere;
- Acces la extranet/intranet;
- Servicii guvernamentale online - inregistrarea autovehiculelor, servicii sanitare etc.
- Servicii de comert electronic B2B & B2C - autentificarea si semnarea tranzactiilor in cazul aplicatiilor de comert electronic;
- Solutii VPN - autentificare realizata de doi factori;
- Autentificare RAS (Remote Access Server);
- Logon la retea securizat;
- Comunicatii prin e-mail securizat - criptare si semnare;
- Securitate - protectie la pornirea calculatorului, semnarea si criptarea fisierelor.

5. Aplicatii compatibile:

- Windows 2000 Smartcard si NT logare la retea, client Check Point VPN, client Cisco VPN, RAS Dialup;
- PKI si CA: Baltimore , Entrust, Microsoft, Symantec, DST, RSA Keon si altele;
- Client de Securitate: Interoperabilitate Web Browser;
- Autentificare cu cheie publica pentru Microsoft Internet Explorer;
- Autentificare si semnare cu cheie publica pentru Netscape Navigator;
- Autentificare WAC;
- Microsoft Outlook/Outlook Express, Internet Explorer, Netscape Messenger, Lotus Notes, Mozilla, Google Chrome.

6. Logare la Windows pe baza certificatului

Logarea interactiva pe baza certificatului aflat pe un smartcard incepe cand un utilizator introduce smartcard-ul personal intr-un cititor care transmite catre sistemul de operare Windows 2000 (sau mai nou) o cerere de autentificare prin PIN in locul setului de date compus din username, nume de domeniu si parola. Introducerea card-ului este echivalenta cu pasul apasarii tastelor "Ctrl-Alt-Del" care sunt folosite de obicei pentru a initia log-on-ul pe baza de parola. PIN-ul folosit de utilizator este folosit numai pentru autentificarea pe smartcard si nu pe domeniu.



7. Specificatiile tehnice ale produsului

Sisteme de operare suportate	Windows Server 2003/R2, Windows Server 2008/R2, Windows Server 2012/R2, Windows 7, Windows XP/Vista, Mac OS, Linux, Windows 8, Windows 10
Suport standarde&API	PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPsec/IKE, MS minidriver, CNG
Memorie	72K
Algoritmi de securitate integrati	PKCS#11 V2.20, MS CryptoAPI and CNG (CSP,KSP), Mac Keychain (TokenD), Smart Card Minidriver, Java Card 2.2.2, GlobalPlatform Version 2.1.1, X.509 v3 certificate storage, SSL v3, IPsec/IKE, PC/SC
Nivelul de securitate al chip-ului	FIPS 140-2 Level 3, Common Criteria EAL4+
Dimensiuni	16.4mm X 8.4mm X 53.6mm
Suport pentru specificatiile ISO	Suport pentru specificatiile ISO 7816 1-4
Putere consumata	120mW
Temperatura la care trebuie folosit	De la 0 C la 70 C (de la 32 F la 158 F)
Temperatura de stocare	De la -40 C la 85 C (de la -40 F la 185 F)
Umiditate	0-100%, fara condens
Certificat de rezistenta la apa	IP X7 - IEC 529
Conector	USB tip A (Universal Serial Bus), suport pentru USB 1.1 si 2.0
Carcasa	Carcasa din plastic, rezistenta la lovituri accidentale
Retinere a datelor memorate	Cel putin 10 ani
Rescriere	Cel putin 500.000

