SODAT software spol.s r.o.

Sedlákova 33
602 00 BRNO
tel./fax: 05-43236177(8)
mobil: 0602-702781
http://www.sodatsw.cz
e-mail:tomas@sodatsw.cz

NABÍDKA BEZPEČNOSTNÍHO HW A SW

Úvod

Firma SODAT software spol. s r.o. se věnuje oblasti vývoje bezpečnostních SW řešení již od roku 1997. V dnešní době má k dispozici systém AreaGuard®, jehož cílem je chránit ON-LINE šifrováním data uživatele. Dalšími vlastnostmi je implementace elektronického podpisu a lokální i vzdálená autentizace uživatele do operačního systému.

Podmínky implementace

Nabízené řešení využívá vlastností operačního systému MS-WINDOWS 2000 (NT 4.0), MS-OFFICE 2000, MS Internet Explorer 5.0 a implementace systému AreaGuard® Notes. Výhodou navrhovaného řešení je maximální využití již implementovaných služeb uvedených systémů s použitím šifrovacích funkcí AreaGuard® Notes. Jako HW prostředek (token) k uložení šifrovacích klíčů a certifikátů k autentizaci a digitálnímu podpisu lze použít HW token iKey 1000 nebo libovolný jiný prostředek dle požadavků uživatele (čipová karta, IR security box nebo jiný token podporující PKCS#11, MS CAPI a CSP).

Hardware – iKey 1000

SODAT software doporučuje nasazení autentizačního HW tokenu **iKey 1000** od firmy Rainbow USA (http://www.rainbow.com). iKey 1000 se připojuje přes USB rozhraní a je plně kompatibilní s čipovými kartami.

Funkce iKey 1000:

- Identifikace a autorizace uživatele ke stanici – autentizace uživatele ke stanici a doméně na základě certifikátu uloženého v tokenu a vydaného firemní certifikační autoritou (součást WINDOWS 2000 SERVER). Není nutná implementace dalšího SW.
- Audit činnosti uživatele – auditní služby operačního systému WINDOWS 2000 (NT). Není nutná implementace dalšího SW.
- Uživatelská oprávnění – služby operačního systému WINDOWS 2000 (NT). Není nutná implementace dalšího SW.
- Počet uživatelů na stanici není omezen.
- Připojení přes USB. Identifikace a autentizace uživatele pomocí certifikátu X.509 uloženého v tokenu včetně uživatelských šifrovacích klíčů (symetrické i asymetrické).
- Není zapotřebí žádné čtecí zařízení. Součástí iKey 1000 je prodlužovací kabel k USB rozhraní.

Vlastnosti iKey 1000:

- 8 kB vnitřní EEPROM paměti, která je rozšiřitelná na 32 kB
- tři režimy přístupu do paměti podle ISO 7816-4 (anybody, user, administrator)
- ochrana paměti pomoci PIN (32bit) a SO (Security Office) PIN (64bit)
- nastavitelný maximální počet pokusů pro zadání PIN
- unikátní sériové číslo (64 bit)
- uložení certifikátů dle X.509
- podpora RSA 1024-bit v rámci knihovny PKCS#11 a MS CAPI
- podpora autentizace HMAC a CHAP pomocí MD5 (tajná hodnota nikdy neopustí iKey)
- hardwarová podpora algoritmu MD5
- generátor náhodných čísel

Každý uživatel vlastní token iKey 1000, ve kterém je uložen certifikát a jeho soukromý klíč. Použití tokenu je podmíněno zadáním PIN s nastavitelným počtem chybných pokusů. PIN je možné obnovit pomocí SO-PIN, který má k dispozici bezpečnostní administrátor. Do tokenu s pamětí 8 kB je možné uložit 3 certifikáty s příslušnými privátními klíči a minimálně 20 symetrickými klíči pro ON-LINE šifrování souborů systému AreaGuard® Notes.

Software – AreaGuard® Notes

AreaGuard® Notes je bezpečnostní ON-LINE šifrovací software určený pro operační systém WINDOWS 2000 (NT 4.0). Software AreaGuard® Notes dokáže ON-LINE šifrovat soubory na disku (lokální, vzdálený, výměnný). Pokud je nastaven soubor jako šifrovaný, pak při čtení souboru probíhá transparentní dešifrování a při uložení souboru šifrování. Šifrovaný soubor může být uložen na libovolném místě adresářové struktury a v žádném případě nemůže dojít k jeho dešifrování bez vědomí uživatele. AreaGuard® Notes poskytuje možnost nastavit adresáře, ve kterých se budou všechny soubory automaticky šifrovat. Každý soubor, který se bude do takovéhoto adresáře ukládat bude automaticky zašifrován. Šifrované soubory je možné zaslat e-mailem, zálohovat na výměnná média a sdílet mezi více uživateli. Pokud dochází k načítání souborů ze vzdáleného disku, pak je soubor po síti přenášen v zašifrovaném tvaru. Šifrované soubory lze uložit jako samodešifrovací EXE soubor, který může být dešifrován na počítači, kde není AreaGuard® Notes instalován. Při mazání šifrovaného souboru se automaticky provádí nevratné mazání. Šifrovací klíče může uživatel zadávat z klávesnice nebo z tokenu (čipová karta, iKey, ...). AreaGuard® Notes používá k šifrování standardizovaných algoritmů 3-DES, IDEA, RC4 a v polovině roku 2001 nový standard RIJNDEAL s délkou klíče 128-bitů. Jejich implementace splňuje všechny požadavky moderní kryptografie. Na návrhu implementace se podílel přední český kryptolog Dr. Ing. Petr Hanáček z VUT Brno.

Během veletrhu INVEX 2000 získal AreaGurad® Notes ocenění The Best Of Invex 2000, udělovaného redakcemi odborných časopisů.

Bližší informace o systému AreaGuard® Notes naleznete na adrese:
http://www.sodatsw.cz/oa7.htm

Současně se systémem AreaGuard® Notes a tokenem iKey 1000 dodáváme podporu silné kryptografie pro WINDOWS 2000, MS Internet Explorer 5.0 (5.5) a MS-OUTLOOK 2000 s délkou klíčů 128 bitů pro symetrické šifry a 1024 bitů pro asymetrické šifry. Certifikáty a soukromé klíče uživatele lze automaticky využít v prostředích MS Internet Explorer a MS-OUTLOOK 2000 k šifrování a digitálnímu podpisu, autentizaci uživatele k počítači a doméně.

Záruka

Na token iKey 1000 poskytujeme záruku 6 měsíců. U SW je neomezená záruka na média. U funkčnosti SW je záruka funkčnosti neomezená při dodržení přesného specifikovaného prostředí.

Technická podpora

Oddělení technické podpory je dostupné ve všední dny mezi 8.00 a 17.00 hodinou, pokud není smluvně stanoveno jiným způsobem. Technická podpora u zákazníka se řídí ceníkem SODAT software. Všechny produkty můžeme zákazníkovi bezplatně zapůjčit a zajistit bezplatnou pomoc při základní ukázkové implementaci.

Způsob a termín dodání

Termín dodání je 14 dnů od doručení objednávky. Způsob dodání na příslušných médiích poštou, osobním doručení nebo vyzvednutí na našem obchodním oddělení.

Cenová kalkulace a způsob úhrady

AreaGuard® Notes na 1 PC .....1.499,- Kč
Množstevní ceny viz. ceník http://www.sodatsw.cz/cenik.htm
HW token iKey 1000, 1ks .....1.890,- Kč

1 hodina práce u zákazníka (implementace, školení, technická podpora ...)
.....1.200,- Kč
Doprava k zákazníkovi, 1 km ..... 7,- Kč

Veškeré ceny jsou uvedeny bez DPH dle platných předpisů.

Závěr

Veškeré informace o aktivitách SODAT software, popisu systému, historii a seznam referencí najdete na http://www.sodatsw.cz.