SODAT software spol.s r.o.

Sedlákova 33
602 00 BRNO
tel./fax: 543 236 177(8)
mobil: 602 702 781
http://www.sodatsw.cz
e-mail:tomas@sodatsw.cz

Nabídka bezpečnostního řešení AreaGuard® Solution.

Základní údaje o dodavateli:

1.1. Obchodní jméno : SODAT software spol. s r.o.
1.2. Sídlo: Sedlákova 33, 602 00 Brno
1.3. Statutární orgán: Tomáš Stranyánek-jednatel
1.4. Zmocněný zástupce: Tomáš Stranyánek
1.5. Bankovní spojení: eBanka 59372001/2400
1.6. IČ: 25323989
1.7. DIČ: 288-25323989
1.8. Tel./fax.: 543 236 177-8
1.9. Mobil 602 702 781
1.10. e-mail: tomas@sodatsw.cz

Detailní popis řešení a jeho vlastností

1. **Popis řešení a funkcionality řešení na klientské části**
   Předmětem tohoto technického popisu je řešení řady AreaGuard® Solution podpořené hardwarovými předměty.

   Softwarový systém AreaGuard® ve spojení s tokenem nebo čipovou kartou (hardwarovým předmětem) umožňuje rozšířit bezpečnostní mechanismy koncové stanice o následující funkce:
   - bezpečná autentizace uživatele k pracovní stanici a podnikové síti pomocí certifikátu uloženého v hardwarovém předmětu, případně pomocí hesla a jména, které se ukládá prostřednictvím AreaGuard® Gina do hardwarového předmětu
   - on-line šifrování souborů a adresářů pracovní stanice, podnikové počítačové sítě a to prostřednictvím AreaGuard® Notes
   - použití elektronického podpisu a šifrované e-mailové komunikace
   - u mobilních počítačů bezpečné navázání spojení prostřednictvím VPN klienta
   - kompletní správu symetrických a asymetrických šifrovacích klíčů jejich archivaci, vzdálenou distribuci a to prostřednictvím AreaGuard® AdminKit

   Pomocí systému AreaGuard® je možné zabezpečit počítače s operačním systémem MS-WINDOWS 9x, NT, 2000 a XP, pracující samostatně nebo připojených k serveru MS-WINDOWS 2000 s Active Directory. Řešení AreaGuard® Solution a všechny jeho části bezproblémově fungují na počítačích s výkonem postačujícím operačnímu systému na počítači instalovaném.

   1.1. **Bezpečná autentizace**
   Systém AreaGuard® provádí bezpečnou autentizaci k operačnímu systému a podnikové síti pomocí hardwarového předmětu. V tomto předmětu je uložen certifikát uživatele a uživatelův podpisový klíč, který je chráněn vnitřním procesorem předmětu a přístupný uživateli pouze po zadání uživatelova PIN. Uživatel se identifikuje uživatelským certifikátem a autentizuje se k operačnímu systému a podnikové síti pomocí elektronického podpisu, což je vyšší způsob autentizace oproti zadání uživatelského jména a hesla. Podmínkou pro implementaci bezpečné autentizace je existence domény v podnikové síti a podniková certifikační autorita.
   V případě, že zákazník nemá vybudovanou infrastrukturu, která podporuje autentizaci uživatele prostřednictvím certifikátu, lze použít přechodné řešení prostřednictvím AreaGuard® Gina, které zajistí uložení klasických přihlašovacích informací od hardwarového předmětu. AreaGuard® Gina dokáže generovat náhodná přihlašovací hesla, jejichž změna může být vynucena nastavením bezpečnostní politiky. V obou případech se uživatel identifikuje zadáním PIN.

   1.2. **Šifrování souborů**
   Soubory uložené na paměťovém médiu (pevný disk, síťový disk, výměnný disk, CD, CD-RW, disketa atd.) obsahují důvěrné (interní) informace uživatele a organizace. Z tohoto důvodu je zapotřebí zabezpečit tyto soubory proti možnému zneužití neoprávněnou osobou, která může tyto soubory získat např. krádeží příslušného paměťového média. Jedinou možnou ochranou proti této skutečnosti je použití kryptografických (šifrovacích) prostředků. Uživatelsky nejpříjemnějším a také vysoce účinným nástrojem je provádění on-line šifrování souborů ve specifikovaných adresářích (např. Dokumenty daného uživatele).
   On-line šifrování znamená, že při každém vytváření souboru nebo zapisování do souboru v šifrovaném adresáři jsou data automaticky šifrována nastaveným šifrovacím algoritmem a šifrovacím klíčem. Naopak při čtení dat ze šifrovaného souboru dochází k automatickému dešifrování v paměti pracovní stanice. Na disku jsou příslušné soubory vždy v zašifrovaném tvaru. Šifrovací klíče jsou uloženy v hardwarovém předmětu uživatele a jejich použití je podmíněno znalostí PIN k hardwarovému předmětu stejně jako při autentizaci uživatele.

Šifrované soubory se mohou nacházet na lokálním disku, výměnném nebo vzdáleném disku. Pokud je šifrovaný adresář sdílen více uživatelům, pak všichni uživatelé musí mít k dispozici šifrovací klíč, kterým jsou soubory v tomto adresáři šifrovány. K dešifrování dochází v paměti lokální stanice a proto je přenos dat po síti bezpečný.

Výhodou on-line šifrování prostřednictvím AreaGuard® Notes je naprosto nenápadný provoz, kdy uživatel neregistruje žádné byť sebemenší změny ve své práci s daty. Bezpečnostní správce může přesně definovat jaké ovládací prvky systému AreaGuard® Notes bude mít uživatel k dispozici. Lze docílit stavu, kdy běžný uživatel nebude moci nastavit šifrovanou oblast, definovat nový šifrovací klíč tedy i přešifrovat data jiným klíčem, případně klíč odstranit z hardwarového předmětu.

1.3. Elektronický podpis a šifrování e-mailů

Elektronický podpis a šifrování e-mailů je v podnikové síti důležité k zabezpečení utajení obsahu e-mailů před neoprávněnými uživateli (např. administrátory podnikové sítě) a k ověření odesílatele e-mailové zprávy. Stejně jako při autentizaci uživatele, tak při elektronickém podpisu je zapotřebí hardwarového předmětu, ve kterém jsou uloženy potřebné informace k vytvoření elektronického podpisu. Bez hardwarového předmětu nemůže uživatel e-mail digitálně podepsat nebo dešifrovat obsah jemu adresovaného a zašifrovaného e-mailu. AreaGuard® Solution zde plně využívá funkcí MS-Outlook případně Lotus Notes.

1.4. VPN klient

Při autentizaci uživatele k pracovní stanici a podnikové počítačové síti se velmi často aktivuje bezpečné spojení prostřednictvím VPN. Při aktivaci VPN dochází k ustanovení bezpečného šifrovaného kanálu, ve kterém se všechna data šifrují příslušným šifrovacím klíčem. Hardwarový předmět umožňuje ustanovení tohoto bezpečného komunikačního kanálu, kdy se využívá přihlašovacích informací, které jsou v něm uloženy.

2. Popis řešení administrace systému AreaGuard® prostřednictvím AreaGuard® AdminKit

V hardwarovém předmětu uživatele jsou bezpečně uloženy:

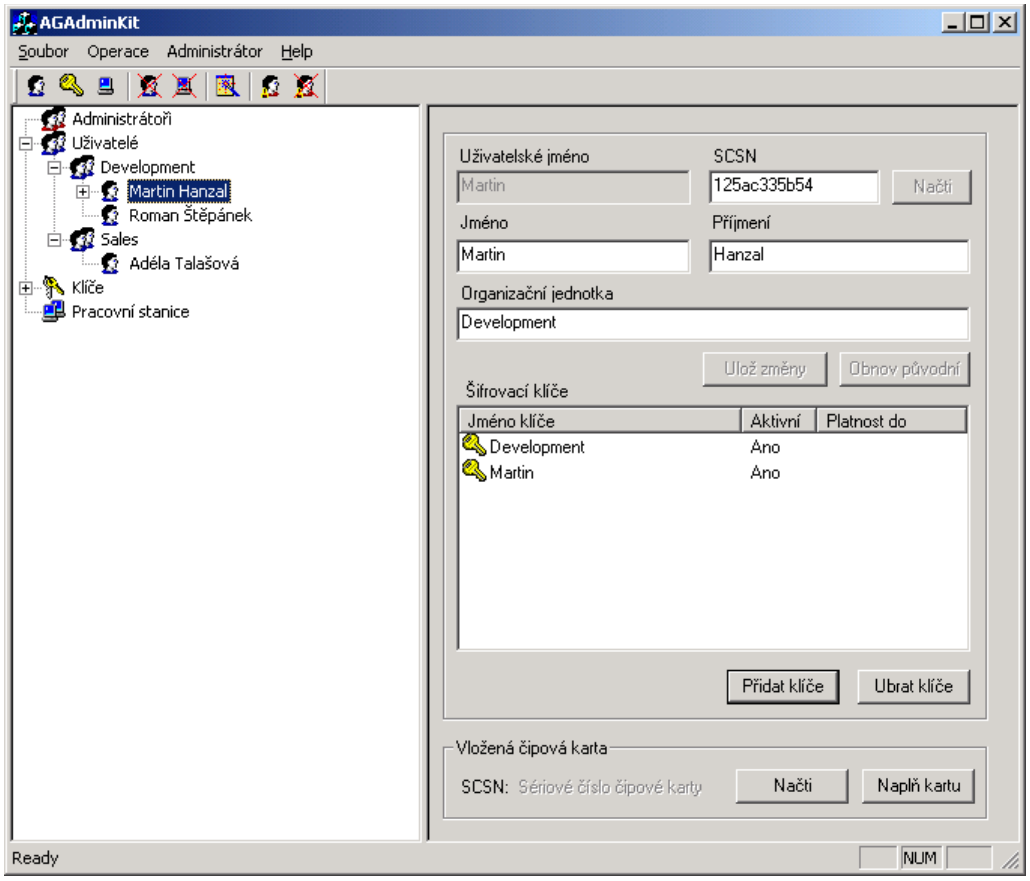
- certifikát uživatele a uživatelův podpisový klíč
- symetrické šifrovací klíče k šifrovaným souborům systému AreaGuard® Notes
- popř. další části kódu

Certifikát uživatele a uživatelův podpisový klíč slouží k autentizaci uživatele ke koncové stanici a podnikové síti (Active Directory serveru WINDOWS 2000). Hardwarový předmět je chráněn uživatelským PIN pro načtení informací z předmětu a Master PIN pro vytváření a mazání šifrovacích klíčů. Běžný uživatel nemůže obsah předmětu definovaný bezpečnostním správcem žádným způsobem změnit. K automatickému generování, správě, uchování a vzdálené distribuci uživatelských šifrovacích klíčů v hardwarových předmětech slouží aplikace AreaGuard® AdminKit.

1.1. Administrátorský nástroj AreaGuard® AdminKit

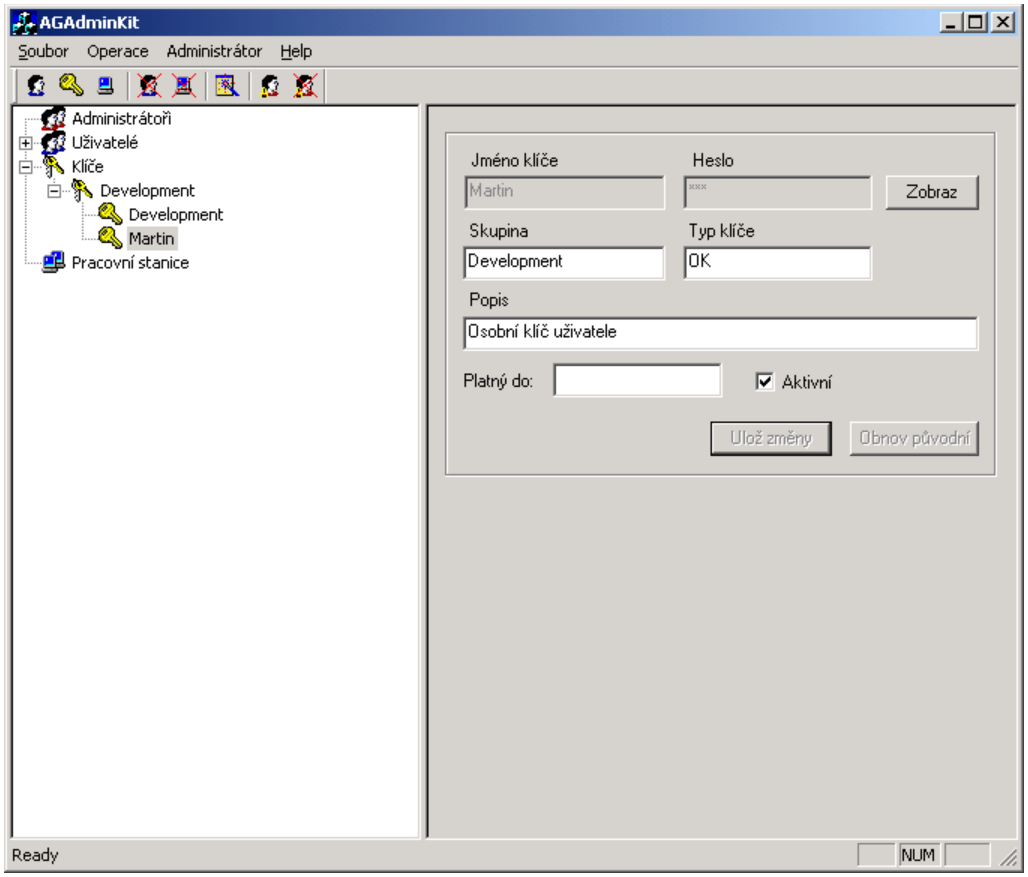
Nástroj AreaGuard® AdminKit ulehčuje práci bezpečnostním správcům systému AreaGuard® při správě a zvyšuje bezpečnost a dostupnost celého systému AreaGuard®. AreaGuard® AdminKit spravuje následující údaje:

- evidence uživatelů používajících hardwarový předmět
- evidence šifrovacích klíčů systému AreaGuard® a uživatelských certifikátů
- evidenci nastavení systému AreaGuard® na jednotlivých pracovních stanicích
- popř. správu dalších částí kódu

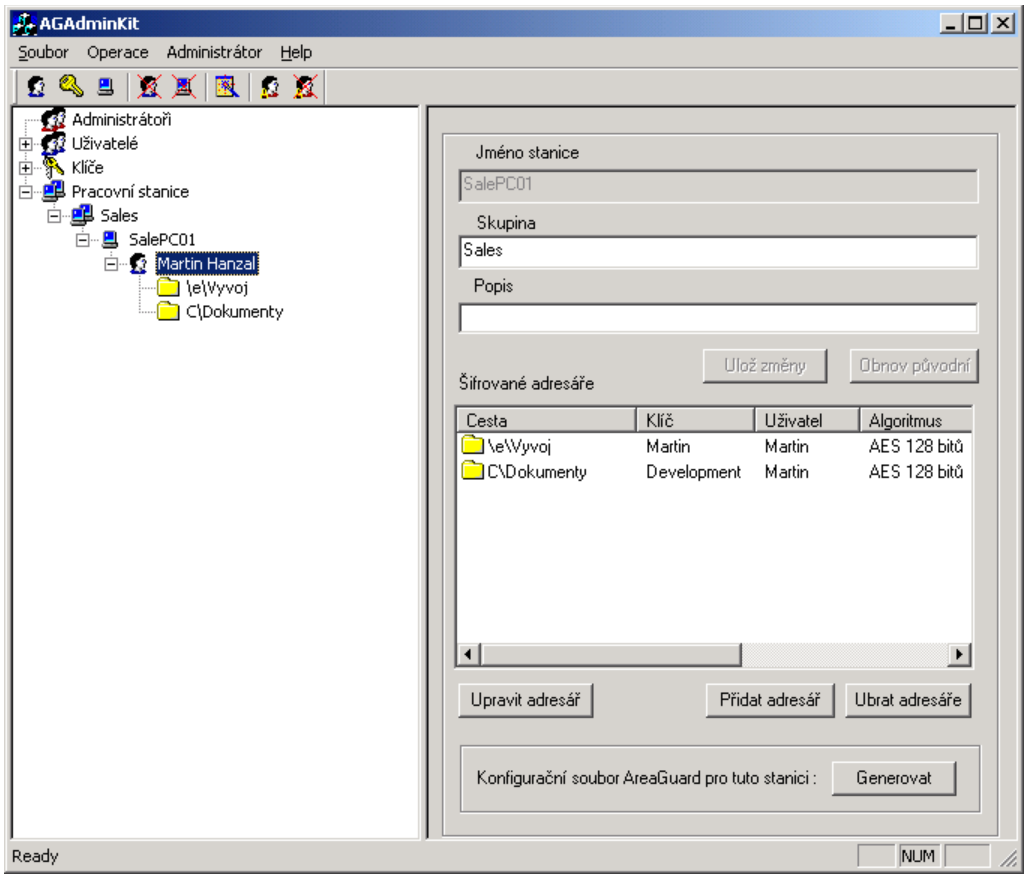


Evidence uživatelů
slouží k uložení informací všech uživatelů, kteří pracují se systémem AreaGuard®. Jednotlivým uživatelům lze přiřadit šifrovací klíče a příslušný autentizační certifikát. Kdykoli je možné nastavené šifrovací klíče uložit do hardwarového předmětu. V evidenci uživatele je uloženo sériové číslo předmětu, které se kontroluje při vkládání hodnot do předmětu.

Evidence šifrovacích klíčů
do systému AreaGuard® AdminKit lze ukládat veškeré uživatelské šifrovací klíče jednotlivých uživatelů a autentizační uživatelský certifikát s uživatelským podpisovým klíčem. Každému uživateli lze přiřadit šifrovací klíče, které má k dispozici. Uložení hodnot šifrovacích klíčů je zabezpečeno šifrováním pomocí systému AreaGuard®. S takto zašifrovanou databází má oprávnění pracovat pouze definovaný bezpečnostní správce, který zná heslo šifrovacího klíče této databáze. Toto heslo může být vloženo z klávesnice nebo může být uloženo v hardwarovém předmětu tohoto bezpečnostního správce. Lze zajistit nutnost přítomnosti více bezpečnostních správců, jejich autentizace je podmínkou pro vstup do systému AreaGuard® AdminKit.



Evidence nastavení systému AreaGuard®
AreaGuard® AdminKit eviduje veškeré pracovní stanice, na kterých je nainstalována jakákoli část systému AreaGuard®. U každé pracovní stanice jsou uloženy informace o šifrovaných adresářích a přiřazených šifrovacích klíčích. Z nastavené stanice lze vygenerovat konfigurační soubor systému AreaGuard®, který lze použít k nastavení systému AreaGuard® na koncové stanici.

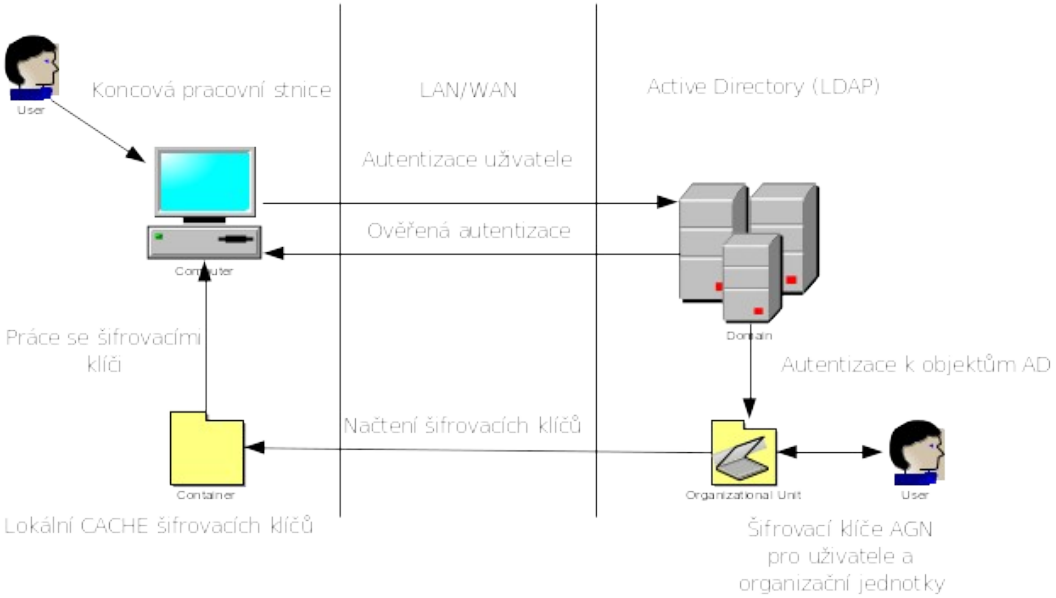


K administrátorské aplikaci AreaGuard® AdminKit je povolen přístup pouze definované skupině správců. Tuto skupinu může definovat pouze bezpečnostní správce celého systému. Veškerá data jsou uložena v šifrované podobě. O všech operacích s aplikací AreaGuard® AdminKit je veden LOG soubor, který má přístupný pouze bezpečnostní správce.

3.2. **Architektura AreaGuard® Notes s propojením na AD nebo LDAP**

Každý uživatel vlastní hardwarový předmět, ve kterém je uložen uživatelský certifikát a uživatelský podpisový klíč. Uživatel se autentizuje k serveru (AD nebo LDAP) pomocí tohoto předmětu. Při úspěšné autentizaci systém AreaGuard® zjistí, jestli se v záznamu uživatele nebo organizační jednotky AD, do které uživatel patří, nacházejí šifrovací klíče pro AreaGuard® a stáhne tyto klíče do lokálního klíčového skladu (Container). Šifrovací klíče uložené v AD nebo LDAP jsou šifrovány veřejným klíčem uživatele, který je součástí uživatelského certifikátu používajícího se k autentizaci. Takto zašifrované šifrovací klíče se přenáší prostřednictvím počítačové sítě LAN/WAN do lokálního klíčového skladu, ve kterém jsou uloženy ve stejné formě, jako v AD nebo LDAP. Systém AreaGuard® načítá tyto šifrovací klíče do vlastní vnitřní chráněné paměti, kde si tyto klíče dešifruje pomocí privátního šifrovacího klíče uživatele, který je uložen v hardwarovém předmětu.

Existence lokálního klíčového skladu je nutná v případě práce počítač v off-line připojení k podnikové síti (např. notebook mimo kancelář). U tohoto skladu je definován časový limit, po jehož dobu jsou šifrovací klíče platné a mohou být



použity. Po vypršení tohoto limitu nebo kdykoli v tomto limitu musí proběhnout přihlášení k AD nebo LDAP, aby došlo k aktualizaci těchto šifrovacích klíčů v lokálním skladu šifrovacích klíčů.

K důvěryhodnému serveru šifrovacích klíčů existuje podobné rozhraní, jak bylo popsáno v kapitole o AreaGuard® AdminKit. Toto rozhraní komunikuje přímo s AD nebo LDAP pomocí protokolu LDAP, který je zabezpečen protokolem SSL. Tímto nástrojem lze provádět administraci tohoto serveru z libovolného místa počítačové sítě.

3.3. **Administrování systému AreaGuard® a možnosti obnovy dat**

Pomocí administrátorského nástroje AreaGuard® AdminKit lze spravovat veškeré

informace o systému AreaGuard®. Pomocí tohoto nástroje probíhá vydávání a evidování šifrovacích klíčů jednotlivých uživatelů. Tyto šifrovací klíče lze automaticky a vzdáleně plnit do hardwarových předmětů nebo je možné je využít v případě obnovy dat.

V administrátorském nástroji je uchováno nastavení systému AreaGuard® lokálních stanic. Tohoto nastavení systém AreaGuard® využívá při automatické (bez zásahové) instalaci a konfiguraci systému AreaGuard® na pracovní stanici. Této konfigurace je možné využít také při změně konfigurace během provozu systému AreaGuard® na koncové stanici.

Nastavení vlastností systému AreaGuard® a přístup k uloženým šifrovacím klíčů v databázi má pouze organizací definovaná skupina administrátorů, kteří mohou tyto informace zpracovávat a mají k nim oprávněný přístup.

4. **Požadavky na zdroje zadavatele**
   - projekt vyžaduje jednoznačnou definici technického koordinátora na straně zadavatele, který bude zodpovědný za komunikaci se zhotovitelem a vytvoří si svůj pomocný tým, sestavený zejména z administrátorů serverů, pracovních stanic atd.
   - pracovní stanice musí obsahovat funkční operační systém MS-WINDOWS 9x a vyšší a připojením k doméně MS-WINDOWS 2000 server s Active Directory
   - pro školení administrátorů bude zapotřebí zajistit školící místnost s projekcí a funkčními vzorky vybraných stanic viz předchozí požadavek

5. **Nabídka možných bezpečnostních předmětů**
   Firma SODAT software spol. s r.o. standardně podporuje tokeny iKey od výrobce Ranbow Technologies jimž je certifikovaným partnerem s maximální podporou. Bližší informace: http://www.rainbow.com/company/PartnersSolution_detail.asp?CompanyName=SODAT%20Software

   Jako HW předměty lze standardně použít:
   - iKey 1000
   - iKey 1032
   - iKey 2000
   - iKey 2032
   - iKey 3000 (nutné testy)
   - SuperToken (nutná úprava)
   - eToken od výrobce Aladin
   - Čipové karty Datakey řady 330.

   Řešení AreaGuard® Solution je otevřené pro použití jiných tokenů nebo čipových karet, které splňují standard PKCS#11 a interface CAPI operačního systému MS-WINDOWS a výrobce k nim dodává SDK informace.

6. **Časové omezení licencí systémů řady AreaGuard®**
   AreaGuard® Notes je momentálně ve verzi 2.0, AreaGuard® AdminKit a AreaGuard®Gina verzi 1.0. Licence se nikterak neomezují časem a zadavatel tedy může výše uvedené systémy používat neomezeně.

7. **Support systémů řady AreaGuard®**
   Standardní telefonický a mailový support v pracovní dny od 8.00 do 16.30 je již zahrnut v ceně licencí AreaGuard®.
   Kontakt na support:
   - support@sodatsw.cz
   - 543 236 177-8

Nadstandardní support je předmětem dalšího jednání.

Porovnání řešení AreaGuard® Solution a EFS (Encrypting File System) ve WINDOWS 2000/XP

1. EFS lze použít pouze na NTFS souborovém systému. Zašifrované adresáře a soubory z NTFS nelze uložit v zašifrované podobě na výměnné a vzdálené (síťové) disky. To znemožňuje provádět zálohování souborů a případné sdílení mezi uživateli.
2. K šifrování pomocí EFS se používá asymetrické kryptografie k ukládání symetrických šifrovacích klíčů. Každý soubor má vygenerován vlastní symetrický klíč, který je k zašifrovanému souboru připojen. Asymetrická kryptografie je velmi náročná na čas. Příprava symetrického klíče musí probíhat při každém přístupu k souboru, což značně zpomaluje práci se zašifrovanými soubory.
3. Certifikát s privátním klíčem, který se používá k asymetrické kryptografii při přípravě symetrického šifrovacího klíče, se generuje v operačním systému pracovní stanice. Tento certifikát nelze přenést na jiný počítač a uživatel jej může kdykoli z operačního systému odstranit nebo si vygenerovat certifikát nový a začít soubory šifrovat takto nově vygenerovaným certifikátem.
4. Tajné části šifrovacích klíčů EFS se nachází v registrační databázi operačního systému, odkud mohou být neoprávněně získány.
5. EFS má velmi náročnou administraci a je naprosto nevyhovující k hromadnému použití v organizaci. EFS je použitelné pro domácí jednotlivce, kteří se spokojí s nižší úrovní zabezpečení.
6. Při reinstalaci operačního systému se ztrácí certifikáty s příslušným privátním klíčem a data se tím znepřístupní.

Obecné informace

Informace o výrobci

Systémy řady AreaGuard® jsou originálním dílem české společnosti SODAT software, která patří mezi přední dodavatele bezpečnostních řešení na českém i zahraničním trhu. Pracovníci a spolupracovníci firmy se aktivně účastní odborných seminářů, konferencí a výzkumných projektů v oblasti bezpečnosti informačních technologií a zasahují do dění kolem informační bezpečnosti finančních institucí, komerčních firem a státní správy. Na základě těchto zkušeností jsou schopni provést profesionální analýzu informační bezpečnosti organizace a navrhnout řešení celkové bezpečnosti organizace. Skupina vývojářů společnosti SODAT software je na základě provedených analýz schopna v krátkém čase upravit bezpečnostní řešení dle požadavků zákazníka. Veškeré kryptografické funkce splňují požadavky moderní kryptografie a jsou podrobovány důkladným testům pod dohledem předního českého kryptologa Dr. Ing. Petra Hanáčka z VUT Brno, Fakulty informačních technologií.

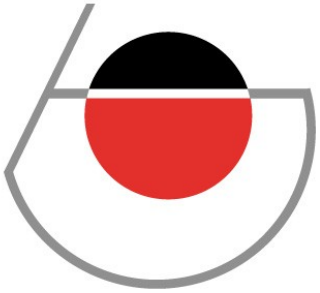
Informace o produktu

Systémy řady AreaGuard® splňují všechny současné požadavky na zabezpečení koncové počítačové stanice. Systémy se integrují do operačních systému MS-WINDOWS NT/2000/XP, kde rozšiřují vlastnosti operačního systému a plně podporují standardní ovládací prvky operačního systému. Nedílnou součástí softwarového bezpečnostního systému AreaGuard® je hardwarový předmět, který slouží k uchování podpisového klíče uživatele a šifrovacích klíčů k šifrování souborů pracovní stanice a podnikové počítačové sítě.

Systém 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 i na počítači, kde není AreaGuard® Notes instalován (např. WINDOWS 95/98/Me). Při mazání šifrovaného souboru se automaticky provádí nevratné mazání. Šifrovací klíče jsou standardně načítány z hardwarových předmětů iKey nebo čipových karet Datakey. Existuje také možnost manuálního vložení hesel šifrovacích klíčů z klávesnice, čehož se může využít v nouzových situacích. AreaGuard® Notes používá k šifrování standardizovaných algoritmů 3-DES, IDEA, RC4 a nového standardu AES reprezentovaného algoritmem Rijndael s délkou klíče 128 bitů, u algoritmu Rijndael až 256 bitů. Jejich implementace splňuje všechny požadavky moderní kryptografie. Na návrhu implementace se podílel přední český kryptolog Dr. Ing. Petr Hanáček z VUT Brno.

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

Dalším oceněním bylo udělení Křišťálového disku na Invexu 2002, udělené akademií informačních a komunikačních technologií ACIT, které předal ministr informatiky pan Vladimír Mlynář.



KŘIŠŤÁLOVÝ DISK

Vybraní referenční zákazníci

eBanka, a.s. kontaktní osoba: Josef Jeřábek
ČSOB pojišťovna, a.s. kontaktní osoba: Miloš Hatla
VSS Komerční banky -Modrá pyramida kontaktní osoba: Radoslav Šafránek

Seznam podporovaných aplikací, standardy a protokoly

Požadavky na hardware:

- USB token je připojen přímo na USB port, volitelně prostřednictvím prodlužovacího kabelu UCB, na kterém může být potisk s logem zákazníka



- Čipová karta Datakey 330 připojitelná pomocí čtečky na USB, nebo pro notebooky PCMCIA čtečka, případně čtečka integrovaná do klávesnice
- Čipové karty s bezkontaktním čipem Smart ISO Prox II výrobce HID, případně s magnetickým proužkem

Podporované operační systémy
- MS Windows NT/2000/XP

Podporované aplikace
- MS Internet Explorer 5.x/6.x
- MS Office 2000/XP
- MS Outlook 2000/XP
- MS Outlook Express od verze 5
- Lotus Notes od verze 6
- Další aplikace používající standard X509 v3

Standardy
- X509 v3
- PKCS#7, PKCS#11, PKCS#12

Šifrovací algoritmy
- AES Rijndael (128 bitů),
- 3-DES (112 bitů),
- IDEA (128 bitů)
- RC4 (40 až 128 bitů) v CBC režimu

Hashovací algoritmy
- SHA-1
- SHA-256

Protokoly
- SSL/TLS, PPTP, IPSec
- Autentizace MS Windows NT/2000/XP, PPTP
- Kerberos

Cenová rozvaha:

1.	AreaGuard® Notes	1 licence	1.999,-
	AreaGuard® Notes	50 licencí	71.500,-
	AreaGuard® Notes	100 licencí	100.000,-
	AreaGuard® Notes	200 licencí	200.000,-
2.	AreaGuard® AdminKit	základ obsahující 20 uživatelů	30.000,-
	každý další uživatel		500,-
3.	AreaGuard® Gina	1 licence	500,-
4.	AreaGuard® FirmWall	1 licence	19.990,-
5.	Čipové karty, čtečky, tokeny software		viz ceník SODAT
6.	Maintenance s platností 1 rok:		
	- AreaGuard®		25%
7.	Servis a služby:		
	- servis v místě uživatele		1.200,-/hod
	- programové úpravy pro uživatele		2.000,-/hod
	- přítomnost bezpečnostního specialisty u uživatele		2.400,-/hod
	- doprava k uživateli		7,-/km

Projekt nasazení:
- Zhotovitel vypracuje projekt nasazení bezpečnostního systému v prostředí objednatele. Tento projekt bude vytvořen na základě osobní konzultace s objednatelem a následné telefonické a e-mailové komunikace zhotovitele a objednatele. Tento projekt bude odevzdán v písemné i elektronické podobě.

- Instalace a nastavení bezpečnostního systému na vybraném vzorku stanic, které budou zástupci jednotlivých skupin počítačů objednatele. Osobní dohled a řešení přímo u objednatele.

Smluvní servis v místě uživatele, programové úpravy ochranného systému dle požadavků uživatele a doprava k uživateli.

Cena: viz ceník SODAT software

Veškeré ceny jsou v Kč bez DPH dle platných předpisů.

Ceny jsou uvedeny k datu 1.6.2003 a jejich aktuální stav je vždy uveden na www.areaguard.cz/cenik.htm

V Brně dne 25.6.2003

Tomáš Stranyánek