

SODAT software spol. s r.o.

Sedláková 33, 602 00 Brno

Tel.: +420 - 543 236 177, fax: +420 - 543 236 177

Kontaktní osoba: Ing. Tomáš Stranyánek

e-mail: tomas@sodatsw.cz

<http://www.sodatsw.cz>**Vztah k řešení: producent****Šifrovací systém AreaGuard®**České/slovenské uživatelské prostředí: **ano/ano**Podporovaná legislativa: **česká, slovenská**Počet instalací ve světě/ČR/SR: **0/200/100**Typický počet uživatelů aplikace: **více než 20**

Orientační cena typické instalace

včetně nasazení systému (v Kč): **neuvedeno**Reference v ČR/SR: **eBanka, a.s., IPB pojišťovna, a.s., Všeobecná stavební spořitelna Komerční banky, a.s.,**

státní správa a samospráva
finančnictví, bankovníctví, pojišťovnictví, leasing
energetika (vodovody, plyn, elektřina, teplo, ...)
doprava nebo spoje (telekomunikace, pošta, ...)
prům. výroba, zemědělství, stavebnictví, zpracov. prům.
velkoobchod, maloobchod, služby
zdravotnictví
jiná úzká specializace

Microsoft Windows Server	Microsoft Exchange Server	Microsoft SQL Server	Microsoft Biztalk Server	Microsoft Content Management Server	Microsoft Commerce Server	Microsoft SharePoint Portal Server	Integrace s Microsoft Office	Microsoft Visio	Microsoft Project	Podpora clusterových řešení Microsoft	Podpora mobilních zařízení	Komunikace v XML
VYUŽÍVÁ	VYUŽÍVÁ	VYUŽÍVÁ		VYUŽÍVÁ			VYUŽÍVÁ			VYUŽÍVÁ	VYUŽÍVÁ	

Systém AreaGuard® slouží k ochraně dat jednotlivých uživatelů i firem. Standardně data v elektronické podobě jsou snadno dostupná a kopírovatelná na koncových stanicích, serverech, výměnných médiích či záložních kopiích uživatelem.

AreaGuard® Notes

při práci se soubory v šifrovaných adresářích zajišťuje jejich on-line šifrování a dešifrování nastaveným šifrovacím algoritmem a klíčem v paměti pracovní stanice. Na disku jsou příslušné soubory vždy v zašifrovaném tvaru. Šifrovací klíče jsou uloženy v hardwarovém předmětu uživatele (tokenu nebo čipové kartě splňující standard PKCS#11) a jejich použití je podmíněno znalostí PIN stejně jako při autentizaci uživatele.

AreaGuard® Firewall

je ochrana postavena na základě definice privilegiovaných aplikací, které mají oprávnění pracovat s šifrovanými daty umístěnými v chráněných datových oblastech (lokálních, síťových nebo výměnných disků).

K dešifrovaným datům může získat přístup pouze privilegovaná aplikace. Ta nemůže data uložit, exportovat nebo přenést do jiné než chráněné oblasti. Data pak nelze z privilegiovaných aplikací získat v elektronické podobě žádným způsobem. Jsou-li data uložena v chráněné oblasti mimo lokální disk, po síti se přenáší v zašifrované podobě a k dešifrování dochází až v paměti lokální stanice.

Nasazení je určeno pro případy, kdy data v elektronické podobě mají velkou cenu a význam pro jejich majitele nebo jsou chráněna zákonem. Zpravidla se jedná o SQL databáze obsahující například rodná čísla, digitální výkresy a mapy s jejich dokumentací, výkresy projekčních kanceláří, zdrojové kódy rozsáhlých softwarových projektů atd.

**AreaGuard® Gina**

představuje hardwarovou ochranu přihlašovací informací (jméno, heslo, doména a podobně) pro operační systém i uživatelské aplikace. Uživatel se přihlašuje vložením hardwarového předmětu a zadáním PIN. Při využití hardwarových předmětů je možné nastavit reakci systému a aplikace na jeho odstranění. Dostupné funkčnosti jsou uzamčení pracovní stanice, okamžité odhlášení uživatele či neprovedení žádné akce.

řešení ERP, ekonomické agendy, personalistika
intranetové portály, správa dokumentů, workflow, helpdesk, správa zákazníků
nástroje pro analýzu finančních, obchodních a marketingových dat (Business Intelligence)
nástroje a řešení pro řízení projektů
Six Sigma
integrace podnikových aplikací (Enterprise Application Integration – EAI)
komunikace s dodavateli a odběrateli (B2B scénáře)
podnikové portály (Internet Business)
průmyslová automatizace, vizualizace, CAD, SCADA, GIS
řešení pro architekturu systémů
bezpečnost a PKI (ochrana dat, firewally, smartcards, apod.)
nástroje pro řízení a správu systémů
mobilitní řešení

AreaGuard® AdminKit

slouží k vydávání, sledování a evidování hardwarových předmětů, šifrovacích klíčů a certifikátů jednotlivých uživatelů. Klíče a certifikáty jsou bezpečně uloženy v databázi, k níž má přístup pouze **bezpečnostní** administrátor. Data lze automaticky a vzdáleně plnit do hardwarových předmětů u nichž je sledováno sériové číslo. Aplikaci je možné využít v případě obnovy uživatelských šifrovaných dat. AreaGuard® AdminKit může být nasazen jako lokální aplikace nebo nadstavba LDAP Serveru (Active Directory). AreaGuard® AdminKit umožňuje vzdáleně sledovat a upravovat nastavení jednotlivých koncových stanic. Konfigurační soubory lze upravovat a využívat rovněž při automatické (bez zásahové) instalaci, správě a plnění dat do hardwarových předmětů.

Při srovnání se šifrovaným souborovým systémem EFS má AreaGuard® tyto výhody:

- nevyžaduje souborový systém NTFS, šifrovaná data lze bez omezení sdílet a zálohovat;
- je méně časově náročný;
- uživatelské šifrovací klíče nejsou omezeny pouze na konkrétní stanici;
- uživatelské šifrovací klíče jsou uloženy v hardwarových předmětech;
- snadná administrace a hromadné nasazení v organizaci;
- při reinstalaci operačního systému nedojde ke ztrátě certifikátů a dat.