

AreaGuard Notes ver. 1.0

Program AreaGuard Notes slouží k uživatelskému šifrování souborů. Program poskytuje uživateli možnost chránit si svá diskrétní data. Chráněná data jsou na počítači uložena v zašifrované podobě, přičemž pouze jejich majitel zná tajemství, za pomoci kterého lze k datům přistoupit. Taková data lze zašifrování uložit nejen na disk počítače nebo serveru, ale je možné je uložit na přenosné médium (disketa, CD-ROM, ZIP ...), poslat elektronickou poštou nebo jiným způsobem na síti zveřejnit (FTP).

Program AreaGuard Notes dokáže soubory ON-LINE šifrovat a dešifrovat. Program AreaGuard Notes je určen pro operační systém WINDOWS NT ver. 4.0, Service Pack 4 a vyšší. Program se postupně vyvíjí i do dalších operačních systémů. Aktuální informace získáte u výrobce programu.

Program AreaGuard Notes používá k ochraně dat standardních šifrovacích algoritmů, které uživatel může použít k zašifrování svých diskrétních dat. Uživatel má k dispozici algoritmy 3-DES, IDEA a RC4.

Vlastnosti šifrovaných souborů

Šifrování je dnes považováno za jedinou možnou metodu, jak dokonale ochránit svá diskrétní data. Ovšem není pravdou, že to co je zašifrované je taky bezpečné. Při šifrování je zapotřebí dodržet mnoho zásad a pravidel. Mnohá pravidla za Vás řeší software poskytující možnost šifrovat data, ale úroveň zabezpečení dat záleží také na samotném uživateli.

Systém AreaGuard® Notes se chová podle všech pravidel, které dnes vyžaduje moderní kryptografie. Soubory zašifrované systémem AreaGuard® Notes mají následující vlastnosti:

1. Soubory jsou na disku (médii) uloženy vždy v zašifrované podobě a při použití dochází k ON-LINE šifrování a dešifrování.
1. Hodnota šifrovacího klíče není nikde v souboru ani systému samotném uložena, ale je vyžadována po majiteli zašifrovaného souboru, který ji musí zadat před vlastním šifrováním/dešifrováním.
1. Dva zašifrované soubory se stejným obsahem za použití stejného algoritmu a šifrovacího klíče jsou zcela různé.
1. Pokud se načítá zašifrovaný soubor ze vzdáleného disku (server, FTP ...), pak po síti je přenášen jako zašifrovaný a k dešifrování nastává na cílové stanici, z které se soubor načítá.
1. Soubory lze šifrovat a dešifrovat pouze produkty z rodiny AreaGuard®.
1. **Zašifrované soubory nelze bez znalosti šifrovacího klíče žádným způsobem dešifrovat.**

Šifrování souborů se provádí z kontextového menu k souborům a adresářům, ve kterém zvolíte volbu šifruj. K dešifrování souborů lze použít volbu dešifruj.

Pokud pracujete se zašifrovaným souborem, pak jste vyzváni k vložení hodnoty šifrovacího klíče. Pokud je již hodnota daného klíče vložena, pak se dešifrování provádí automaticky.

Při práci se šifrovanými soubory se oříte pravidly pro práci se šifrovacími klíči a volte vhodný šifrovací algoritmus.

Volba šifrovacího algoritmu

Šifrovací algoritmus je jedním z hlavních předpokladů, aby byla diskrétní data dobře chráněna. V dnešní době se k šifrování využívá standardizovaných algoritmů, ke kterým je veřejný popis a zdrojové kódy. Tyto algoritmy jsou neustále vystavovány útokům ze strany kryptografických specialistů a všechny možné pochybnosti o jejich bezpečnosti jsou ihned masově zveřejněny. Všechny algoritmy (3DES, IDEA a RC4), které jsou v systému AreaGuard® použity, jsou v dnešní době považovány za **bezpečné a nerozlušitelné**.

Šifrovací algoritmus používá k šifrování dat šifrovací klíč, který je jedinou neznámou v šifrovacím a dešifrovacím procesu. Pokud není tento šifrovací klíč vyjádřen, pak neexistuje metoda, která by v reálném světě mohla text zašifrovaný systémem AreaGuard® dešifrovat. Při práci se šifrovacím klíčem se musíte chovat podle určitých pravidel.

Popis jednotlivých algoritmů:

3-DES

Je nástupce známého algoritmu DES, který se již dnes považuje díky krátké délce šifrovacího klíče (pouze 56 bitů) za rozlušitelný v reálném světě. V algoritmu 3-DES se používá 112 bitový klíč. Tento algoritmus nebyl nikdy zpochybněn a nebyla v něm nalezena bezpečnostní díra. Z použitých algoritmů je 3-DES algoritmem nejpomalejším, ale poskytuje bezpečnost, které v komerčním světě důvěruje celý svět. 3-DES je nejrozšířenějším algoritmem pro ochranu informací v USA.

IDEA

Svémi vlastnostmi velmi podobný algoritmus algoritmu 3-DES. Délka šifrovacího klíče je 128 bitů. Není známa metoda, kterou by šlo data dešifrovat v reálném světě. Je podstatně rychlejší než 3-DES a v Evropě je jeden z nejpoužívanějších algoritmů.

RC4

Velmi jednoduchý a rychlý algoritmus. Z použitých algoritmů v systému AreaGuard® je nejrychlejší (řádově 10 krát rychlejší než 3-DES). Algoritmus RC4 používá délku klíče 128 bitů. V dnešní době není znám úspěšný útok na rozluštění zašifrovaných dat pomocí tohoto algoritmu.

Uživatel si při šifrování souboru volí jeden z uvedených algoritmů. Pokud uživatel chce mít data zašifrovány nejdůvěryhodnějším algoritmem, přičemž pochopí zpomalení načítání a ukládání takto zašifrovaných souborů, použije algoritmus **3-DES**. Pokud dá přednost rychlosti načítání a ukládání šifrovaných souborů, pak zcela určitě použije algoritmus **RC4**.

Všechny používané algoritmy systému AreaGuard® jsou vysoce bezpečné a záleží jen na samotném uživateli, kterému z algoritmů projeví největší důvěru.

Práce se šifrovacími klíči

Šifrovacím klíčem se rozumí tajemství, které zná pouze majitel zašifrovaných dat, bez kterého nelze žádným způsobem zašifrovaná data dešifrovat. Šifrovací klíče se v systému AreaGuard® nikde neukládají, takže bez znalosti šifrovacího klíče jsou zašifrovaná data nerozluštitelná. Šifrovací klíč je tajemstvím majitele dat, který jej při šifrování a dešifrování vkládá z klávesnice.

Po vložení tajemství majite (øetízce šifrovacího klíče) se generuje hodnota (hodnota šifrovacího klíče), která se použije k šifrování a dešifrování dat. Generování této hodnoty zabere v průměru 2 sekundy. Tato hodnota se generuje pouze po vložení øetízce šifrovacího klíče z klávesnice.

Při práci se šifrovacími klíči se øiíte obecnými doporučeními.

Pøedpoklad pro dobøe chránìný soubor

Jeden z pøedpokladù, aby byla data opravdu dobøe chránìná, je chování uživatele (majitele) dat při šifrování a dešifrování. Øiíte se následujícími pokyny:

1. Nikdy nevkládejte øetizec šifrovacího klíèe za pøítomnosti cizí osoby.
1. Jako øetizec šifrovacího klíèe nepoužívejte obecní známá slova nebo slova, která jsou blízka Vaší osobì. Je velmi pravdìpodobné, že potenciální útoèník nejprve vyzkouší všechna takováto slova.
1. Délku øetizec volte minimální 8 znakù, pøièemž kombinujte èíslo, malá a velká písmena, rozné znaky, které lze zadat z klávesnice.
1. Øetizec si vždy zapamatujte a nikde jinde jej neukládejte. Jen ve Vaší hlavì je v bezpečí.
1. Pokud je øetizec prozrazen, zašifrujte všechna data jiným šifrovacím klíèem, protože se nedají považovat za dobøe chránìná.
1. Při odchodu od počítaèe odstraòte všechny šifrovací klíèe z pamìti.
1. Nikdy nesdílejte øetizec šifrovacího klíèe prostøednictvím pošty, telefonu, faxu ani e-mailu. Jediným možným pøedáním je osobní sdílení nebo použití prostøedkù pro bezpečnou výminu šifrovacích klíèù.

Pokud zapomenete šifrovací klíè, neexistuje žádná metoda, jak data dešifrovat.

Výrobce systému AreaGuard Notes ver. 1.0

BETA 4.5.2000

SODAT software spol. s r.o.

Sedláková 33, 602 00 BRNO

Tel./FAX: +420-5-43236177 (8)

e-mail: technická podpora: support@areaguard.cz

informace: info@areaguard.cz

<http://www.areaguard.cz>

© 2000 SODAT software

Přidání systému do počítače

Spusťte z instalační diskety program SETUP.EXE, který Vás provede celou instalací systému AreaGuard Notes do počítače. Všechny soubory se kopírují přímo do operačního systému, protože systém AreaGuard Notes rozšiřuje vlastnosti operačního systému. Po dokončení instalace je zapotřebí provést restart počítače. Po novém startu počítače můžete začít pracovat s šifrovacím systémem AreaGuard Notes.

Odstranění systému z počítače

Spusťte ovládací panel Poidat nebo Ubrat programy a vyberte položku se systémem AreaGuard Notes. Pak zvolte odinstalování a všechny části systému AreaGuard se odstraní z Vašeho počítače. Po odstranění všech částí je zapotřebí provést restart počítače.

Pokud by nešlo spustit odinstalování z ovládacího panelu, pak je možné spustit přímo program `\System32\Aguninst.exe`.

Základní informace o ovládání systému AreaGuard® Notes

System AreaGuard® Notes rozšiřuje možnosti operačního systému. Standardní nabídky rozšíří o přidání nabídek umožňujících práci se šifrovanými soubory.

Operační systém je rozšířen o následující funkce:

1. Kliknutím pravého tlačítka myši na souboru, adresáři nebo seznamu souborů a adresářů se kontextové menu rozšíří o nabídku AreaGuard šifruj a AreaGuard dešifruj.
1. V oblasti SysTray se přidá ovládací ikona systému AreaGuard® Notes, která umožňuje mít stav šifrování.
1. Při práci se zašifrovaným souborem se automaticky zobrazí dialog pro zadání hodnoty šifrovacího klíče, pokud se šifrovací klíč nenachází v paměti.

Zašifování vybraných souborů uživatelem

Dříve než začnete používat šifrované soubory, musíte si je zašifrovat. Šifrování vyvoláte z Průzkumníku kliknutím pravého tlačítka myši na souboru, seznamu souborů, adresáři nebo seznamu adresářů a zvolíte volbu AreaGuard šifruj.

Trvalé dešifrování zašifrovaných souborů

Trvalé dešifrování souborů provedete z Průzkumníku kliknutím pravého tlačítka myši na souboru, seznamu souborů, adresáři nebo seznamu adresářů a zvolením volby AreaGuard dešifruj.

AreaGuard šifrování souborů

Před zašifrováním souboru, seznamu souborů nebo adresářů, musíte zadat údaje, podle kterých se provede požadované zašifrování. Všechny údaje potřebné k provedení šifrování se zadávají v tomto okně.

Doporučené chování a volení šifrovacích klíčů a šifrovacích algoritmů.

Jméno klíče

Jméno klíče slouží k označení šifrovacího klíče, kterým se soubor (soubory) zašifrují. Můžete zadat zcela nové jméno nebo vybrat jméno ze seznamu jmen, která již byla použita a jejíž šifrovací klíče jsou již vloženy do paměti. Seznam vložených jmen můžete zobrazit kliknutím na šipku u combo boxu, ve kterém se zadává jméno klíče. Pokud vyberete ze seznamu nebo zadáte z klávesnice jméno, které je již vloženo v paměti, pak hodnota šifrovacího klíče nelze zadat. Hodnota šifrovacího klíče již byla vložena dříve.

Pokud budete chtít použít jméno klíče, který je již vloženy v paměti, ale chcete vložit jinou hodnotu šifrovacího klíče, pak je nutné odstranit vložené klíče z paměti.

Šifrovací klíč

Zde vložte řetězec znaků, podle kterého se bude zvolený soubor (seznam souborů) šifrovat. Tato hodnota je Vaším tajemstvím a bez její znalosti nelze soubor dešifrovat. Doporučujeme volit tento řetězec podle doporučených pravidel o heslech.

Ověření šifrovacího klíče

Slouží k ověření správnosti vloženého řetězce se šifrovacím klíčem. Musí být shodný s šifrovacím klíčem.

Šifrovací algoritmus

Zvolte jeden z algoritmů, kterým se příslušný soubor zašifruje. K dispozici jsou standardizované algoritmy 3-DES, IDEA a RC4.

System Tray – je oblast v pravém dolním rohu monitoru.

Jméno klíče je jednoznačné označení klíče, které se ukládá k zašifrovaným souborům a napomáhá uživateli k zadání hodnoty šifrovacího klíče. **Jméno klíče** volte srozumitelné a výstižné pro danou hodnotu šifrovacího klíče. Doporučujeme používat stejnou hodnotu šifrovacího klíče pro dané **jméno klíče**.

Vložení hodnoty klíče pro dešifrování

Pokud pracujete se zašifrovaným souborem, pak se tento soubor musí ON-LINE šifrovat při zápisu a dešifrovat při čtení souboru. Každý soubor je zašifrován šifrovacím klíčem, který má svoje jméno a svou hodnotu.

Pokud při práci se souborem se šifrovací klíče, kterým je tento soubor šifrován, nenachází v paměti, pak je nutné jej zadat.

Jméno klíče

Veřejné jméno klíče, který napomáhá uživateli identifikovat hodnotu klíče, kterou musí zadat, aby soubor byl správně dešifrován.

Šifrovací klíče

Tajemství uživatele, které slouží ke generování šifrovacího klíče, kterým je daný soubor šifrován.

ON-LINE šifrování a dešifrování souborů

Máte-li zašifrované soubory, pak jsou tyto soubory automaticky při práci dešifrovány a šifrovány. Při prvním přístupu k zašifrovaným souborům je zapotřebí zadat hodnotu šifrovacího klíče.

Ovládací aplikace v SysTray

V ovládací aplikaci máte možnost:

1. Deaktivovat šifrování – pak šifrované soubory jsou načítány v zašifrovaném tvaru a můžete je kopírovat a posílat mailem v zašifrovaném tvaru.
1. Odstranit klíče z paměti – odstraní se všechny vložené šifrovací klíče. Při nutnosti šifrovacího klíče budete vyzváni k novému vložení hodnoty šifrovacího klíče.

Kopírování šifrovaných souborů

Zašifrované soubory můžete kopírovat v zašifrovaném tvaru pokud deaktivujete ON-LINE šifrování v Control aplikaci.

Zasílání šifrovaných souborů e-mailem

Šifrované soubory můžete zašifrovaně poslat mailem, pokud deaktivujete ON-LINE šifrování v Control aplikaci.

Odstranění šifrovacích klíčů z paměti

V control aplikaci volnou Odstraň klíče z paměti, je zapotřebí provést při opuštění počítače, aby nežádoucí uživatel nemohl použít Vaše šifrovací klíče a přistoupit tak k zašifrovaným souborům.

Jméno klíče je jednoznačné označení klíče, které se ukládá k zašifrovaným souborům a napomáhá uživateli k zadání hodnoty šifrovacího klíče. **Jméno klíče** volte srozumitelné a výstižné pro danou hodnotu šifrovacího klíče. Doporučujeme používat stejnou hodnotu šifrovacího klíče pro dané **jméno klíče**.

Šifrovací klíč je tajemství, které zná pouze uživatel. Bez znalosti tohoto tajemství nelze zašifrovaný soubor dešifrovat. Z tohoto tajemství (øetizce znakù) se generuje hodnota, která vstupuje do šifrovacího algoritmu jako šifrovací klíč.

Šifrovací klíč je tajemství, které zná pouze uživatel. Bez znalosti tohoto tajemství nelze zašifrovaný soubor dešifrovat. Z tohoto tajemství (øetizce znakù) se generuje hodnota, která vstupuje do šifrovacího algoritmu jako šifrovací klíč.

Ověření šifrovacího klíče slouží k porovnání hodnot šifrovacího klíče, aby nemohla nastat situace, že se soubor zašifroval jiným klíčem, než uživatel zadal.

3-DES (triple DES) je algoritmem, který do dnešního dne nebyl rozluštěn a považuje se za kryptografický standard v USA. Délka klíče je 112 bitů a není znám žádný útok, kterým by zašifrovaný soubor šel rozšifrovat v reálném čase.

IDEA – je šifrovacím algoritmem, který se nejvíce používá v Evropě. Nikdy nebyl standardizován, ale není znám žádný reálný útok, kterým by šlo zašifrovaná data dešifrovat v reálném čase. Délka klíče je 128 bitů.

RC4 – je velmi rychlý algoritmus, který se dnes používá například k zabezpečené komunikaci MS Internet Exploreru. Délka šifrovacího klíče je 128 bitů. Není znám reálný útok na zašifrovaná data.

ON-LINE šifrování – při načítání dat ze souboru se automaticky převádí z šifrované podoby do nezašifrované podoby, ve které se předkládají uživateli. Při ukládání dat do souboru se data automaticky šifrují a uloží se zašifrovaná. To znamená, že diskrétní data jsou v souboru uložena vždy v zašifrované (pro jiné uživatele nepoužitelné) podobě.

Øetizec šifrovacího klíèe je øetizec, který uživatel zadává v dialogu při šifrování nebo dešifrování souboru. Z tohoto øetizce je pak generována hodnota šifrovacího klíèe, která se použije ve vybraném šifrovacím algoritmu jako šifrovací klíè. **Øetizec šifrovacího klíèe** je tajemstvím majitele dat.

Hodnota šifrovacího klíče je generována z šetizce šifrovacího klíče a používá se jako šifrovací klíče šifrovacího algoritmu. Generování této hodnoty zabere v průměru 2 sekundy.

Combo Box je pole k editaci (vstupu) øetizce z klávesnice. Kromi klávesnice lze øetizec vybrat za seznamu, který se zobrazí po kliknutí levého tlačítka myši na šipku, která je v pravé části tohoto pole.

