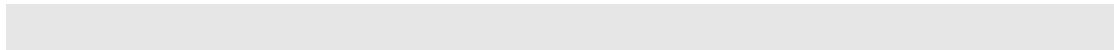




Kliens oldali erős autentikáció RSA Authentication Manager-el

.....A következő dokumentum az RSA Authentication Manager termékét mutatja be. Ennek a dokumentumnak a segítségével a kívánt termékről alapszintű információ kapható, azonban a pontos specifikációhoz, kérjük keresse fel az Ön által preferált RSA viszonteladót.....





1. TARTALOMJEGYZÉK

1. TARTALOMJEGYZÉK	2
2. KLIENS OLDALI ERŐS AUTENTIKÁCIÓ RSA AUTHENTICATION MANAGER-EL.....	3
3. A MEGOLDÁS ÁTTEKINTÉSE	3
4. RSA AUTHENTICATION MANAGER.....	4
5. RSA AUTHENTICATION AGENT	6
6. RSA SECURID TOKEN	7

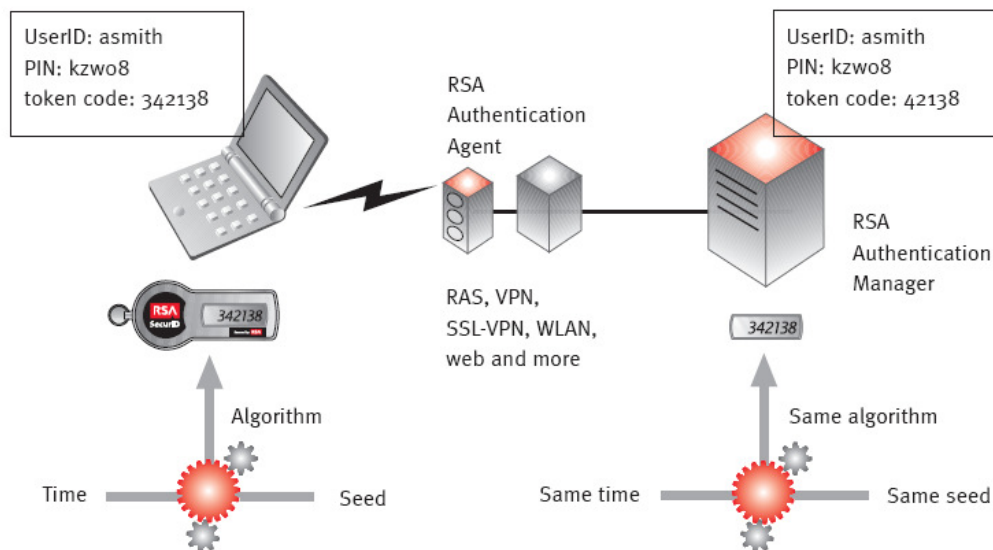
2. KLIENS OLDALI ERŐS AUTENTIKÁCIÓ RSA AUTHENTICATION MANAGER-EL

A megoldás segítségével a felhasználók nem csak felhasználónév / jelszó párossal azonosítják magukat, hanem az ennél biztonságosabb kétfaktoros azonosítást használják. Ennek előnye az adminisztrátorok, IT Security szakemberek számára, hogy jóval biztonságosabb a informatikai hálózat, hiszen a felhasználónév / jelszó páros mellett egy speciális hardver eszköz (a későbbiekben kerül ismertetésre) is szükséges a hálózatba történő belépéshez. A felhasználók számára pedig a megoldás könnyen megszokható, nem kíván előképzettséget a használata, sőt a testreszabható rendszerűzenetek segítségével az üzemeltetésre sem hárul nagy feladat a bevezetés, üzemeltetéseknél.

3. A MEGOLDÁS ÁTTEKINTÉSE

A megoldás három fő részből áll:

- RSA Authentication Manager
- RSA Authentication Agent
- RSA SecurID token



1. ábra: Az RSA kétfaktoros azonosítás áttekintése.

A megoldás során az általunk telepített és konfigurált RSA Authentication Manager a központi komponens. Tárolja a használatban lévő token-ek azonosítóit, tárolja a használatban lévő felhasználóneveket (természetesen LDAP szinkronizáció lehetséges), tárolja a token-ekre és



felhasználókra vonatkozó házirendeket is (azaz melyik felhasználó melyik token-el, milyen alkalmazást tud használni).

Az RSA Authentication Agent, mely egyfajta "biztonsági őrnök" tekinthető azonosítja a felhasználót. Ezt a komponenst minden egyes szerverre, tűzfalra, kliensre telepíteni kell, ahol a későbbiekben kétfaktoros azonosítást szeretnénk. Ez a komponens továbbítja a felhasználó által megadott felhasználói nevet, jelszót, PIN kódot, és 6 számból álló sorozatot az RSA Authentication Manager-nek. Amennyiben az Agent oldali algoritmus és az RSA Authentication Manager-től megkapott úgynevezett "seed" megegyezik, akkor a felhasználó jogosult az adott rendszer használatára (a seed egy olyan speciális számsorozat, mely a PIN kód, token kód, felhasználónév, jelszó és az aktuális idő adataiból egy speciális algoritmus által előállított karaktorsor).

4. RSA AUTHENTICATION MANAGER

Az RSA Authentication Manager az RSA SecurID megoldás felügyeleti komponense, segítségével ellenőrizhetőek az azonosítási kérések, valamint központilag adminisztrálhatóak a hálózati hozzáférések. A feladatát a másik két komponens segítségével végzi.

A megoldás olyan kétfaktoros azonosítást jelent, mellyel megoldható a VPN megoldások, vezeték nélküli hozzáférések, web alkalmazások, üzleti alkalmazások, operációs rendszerek fokozott biztonsága (az összes támogatott alkalmazás megtalálható az alábbi weboldalon: <http://www.rsa.com/rsasecured>).

RSA Authentication Manager szoftvert úgy tervezték, hogy bármilyen méretű szervezet igényeinek megfeleljen. Vállalati szintű multiprocesszoros architektúrára alapozva az RSA Authentication Manager szoftver minimális számú, alig huszonöt felhasználótól kezdve, akár több millió felhasználót, valamint akár több száz egyidejű felhasználói azonosítást is képes kezelni szerverenként. Az RSA Authentication Manager szoftvert világszerte több ezer rendszerben telepítették (bankokban, kormányzatban, iparban, laboratóriumokban, egészségügyben, nem csak nagyvállalati, de kis- és középméretű vállalkozásoknál is). Az RSA Authentication Manager két változatban áll rendelkezésre, Base Edition és a Enterprise Edition változatban.

Az RSA Authentication Manager replikáció funkciója rugalmas hálózati konfigurációt és terheléelosztást tesz lehetővé miáltal a felügyeleti költségek csökkennek.

Az RSA Authentication Manager Base Edition verzió egy master és egy replika szerver lehetőségét kínálja.

A felhasználó adminisztrációja és azonosítása a master szerveren történik és minden információ átmásolódik a replika szerverre is. Mindkét szerver alkalmas az azonosítási kérések kezelésére.

Az RSA Authentication Agents a válaszidők figyelembevételével osztja ki a kéréseket a szervereknek az optimális teljesítmény biztosítása céljából.

Az Enterprise Editiont nagy telepítések kezelésére tervezett megoldás, egy master és akár tíz replika szerver telepítését teszi lehetővé egy tartományon belül és akár 6 különböző tartományt képes kezelni. Ez biztosítja az adminisztrátoroknak, hogy valós időben követni tudják a hálózatukhoz érkező azonosítási kéréseket bárhol a világról, egyidőben frissüljenek a biztonsági házirendek az egész világon, és felépítsenek teljes hálózati topológiát, amely növeli a hálózati teljesítményt. Az Enterprise Edition – amely működik a VERITAS Cluster Szerver magas



rendelkezésre állású platformján Sun Solaris™ környezetben – további katasztrófa helyreállítást és fail-over opciókat is kínál.

Az RSA Authentication Manager szoftver magas felügyeleti rugalmasságot és irányítást nyújt. Vezérelhető a szerver konzoljáról közvetlenül, vagy távolról Windows felületen, vagy web böngészőn keresztül. A kezelői felületről valamennyi RSA SecurID autentikátor felügyelhető, akár egyedi felhasználóról, akár tömeges kiutalásról vagy cseréről is legyen szó. Az LDAP támogatás és a Quick Admin, a web-alapú ügyfélszolgálati kiegészítés a biztonsági adminisztrátor munkáját teszi könnyebbé. Az LDAP támogatás lehetővé teszi a felhasználók és csoportok központosított adminisztrációját a címtárban, mely információk automatikusan szinkronizálódnak az RSA Authentication Manager-ben tárolt információkkal. A Quick Admin lehetővé teszi az adminisztrátor számára, hogy módosítsa a felhasználói és token-információkat anélkül, hogy minden munkaállomásra külön felügyeleti klienset telepítene.

Az RSA Authentication Manager Enterprise Edition-je tartalmazza az RSA Authentication Deployment Manager-t, amely egy web-alapú szoftver eszköz, és jelentős mértékben csökkenti képes a tokenek kiosztásának idejét és költségét.

Mivel az RSA Authentication Manager szoftver valamennyi tranzakciót és felhasználói tevékenységet naplózza, az adminisztrátorok felhasználhatják, mint auditálási, accounting és megfelelési eszközt. Tartalmaz riport mintákat, amelyeket könnyen az adminisztrátor igényeire lehet szabni, beleértve a tevékenység-, a kivétel-, az esemény-, és a felhasználási összesítőket.

RSA Authentication Manager szoftver több, a piacon található nagyobb hálózati infrastruktúrával és operációs rendszerrel képes együttműködni - beleértve 200 gyártó több, mint 285 termékét -, amelyek a maximális rugalmasságot és befektetés-védelemet jelenti a szervezeteknek.

Az RSA Secured stratégiai partner programon keresztül a távoli hozzáférésű termékek, a VPN-ek, a tűzfalak, a vezeték nélküli hálózati eszközök, a web-szerverek és az üzleti alkalmazások vezető gyártói beépítették az RSA Authentication Manager kompatibilitását termékeikbe. Különleges esetekben a multi-threaded API segítségével az adminisztrátorok saját RSA Authentication Agents-t készíthetnek.

Az RSA Authentication Manager ideális megoldás azon szervezetek számára, akik erős felhasználó azonosítást keresnek Microsoft operációs rendszerekbe történő belépéshez.. Az innovatív új technológia révén a Microsoft Windows környezetre fejlesztett RSA SecurID for Microsoft Windows megoldás lehetővé teszi a RSA SecurID azonosítás alkalmazását Microsoft Windows környezetben, mind online, akár offline bejelentkezésre. A megoldás megerősíti a Windows környezetek biztonságát, egyszerűsített, átláthatóbb felhasználó azonosítást módszert nyújt.

A megoldás hardver igénye (RSA Authentication Manager 6.1 esetén):

Támogatott operációs rendszer	Minimum követelmény
Windows 2000 Server SP4	Intel® Pentium® 800 MHz processor
Windows Standard Server 2003 SP1	256 MB of RAM és további 1 MB 1000
Windows 2000 Advanced Server SP4	felhasználónként
Windows Enterprise Server 2003 SP1	1 GB swap file
Windows Enterprise Server 2003 R2	200 MB HDD és további 1 MB 1000
Windows Standard Server 2003 R2	felhasználónként

Windows Enterprise Server 2003 SP2 Windows Standard Server 2003 SP2 Windows Enterprise Server 2003 R2 SP2 Windows Standard Server 2003 R2 SP2	
Linux Red Hat ES 3.0 SUSE Linux Enterprise Server 9	Intel® Pentium® 800 MHz processor 256 MB of RAM és további 1 MB 1000 felhasználónként 1 GB swap file 200 MB HDD és további 1 MB 1000 felhasználónként
Unix	Sun Solaris™ Ultra™ SPARCTM processor, vagy HP-UX: PA-RISC 2.x, vagy IBM AIX RISC System/6000, vagy IBM AIX PowerPC processor 256 MB of RAM és további 1 MB 1000 felhasználónként 1 GB swap file 400 MB HDD és további 1 MB 1000 felhasználónként, valamint 1 GB a log file-oknak

5. RSA AUTHENTICATION AGENT

A megoldás ezen része megállítja és megvizsgálja a hozzáférési kezdeményezéseket és kétfaktoros azonosítást kér a felhasználóktól, legyenek azok akár lokális felhasználók, akár távoliak.

A megoldás képes a tűzfalak, VPN kapcsolatok, web szerverek, Unix operációs rendszerek, Windows rendszerek védelmére is. Leggyakrabban használt része az RSA authentication Agents for Microsoft Windows, melynek segítségével a felhasználói azonosítás lesz biztonságosabb a munkaállomásra történő belépéskor.

RSA Authentication Agents lehetővé teszi ugyanazoknak az RSA SecurID autentikátoroknak és ugyanannak az RSA Authentication Manager-nek az alkalmazását korlátlan számú erőforrásnak a megóvására, és így módon a befektetés kiemelt megtérülését biztosítja. Az egyszerűen konfigurálható RSA Authentication Agent, amely beépül és együttműködik az alkalmazással (RAS, VPN alkalmazások vagy web szerverek) és azonnali védelmet kínál az erőforrásnak a két-faktoros RSA SecurID azonosítással. Továbbá a központi felhasználó adminisztráció következtében minimális ráfordítással új felhasználókat adhatunk a rendszerhez, és új erőforrásokat óvhatunk meg.

Az extranetek alapvető e-business összetevővé nőttek ki magukat lehetővé téve a vevőkkel, az üzletfelekkel és a szállítókkal történő kommunikációt. Ha a Microsoft IIS, az Outlook Web Access, az Apache vagy a Sun ONE web szerverek bármelyikének a védelmére van szükség, az RSA Authentication Agents megóvjá a web-alkalmazásokat a jogosulatlan hozzáféréstől. Továbbá a rendszeradminisztrátornak lehetősége van arra, hogy felügyelje a felhasználói jogosultságokat



abból a célból, hogy meghatározzák, melyik felhasználók tekinthetnek be és melyek nem, miután már megszerezték a belépési jogosultságot. Mivel a megoldást úgy tervezték, hogy együttműködjön a Secure Socket Layer (SSL) titkosítással, az információ védett a hálózaton keresztül történő kommunikáció során.

Védelmet nyújt az IIS, az Apache és a Sun ONE web szervereknek. A web oldalak, fájlok és könyvtárak biztonságát a két-faktoros azonosítással biztosítja. Helyfüggetlen megoldást nyújt, mert nincs szükség külön szoftver telepítésére a felhasználók számítógépeire. Teljes felhasználói felelősséget kínál az Internet, intranet és extranet alkalmazásokhoz

Támogatja a natív Microsoft Windows NT, Windows 2000 és Windows XP biztonságot. Védelmet nyújt az IIS, a dial-up, a RAS/RRAS és interaktív desktop hozzáférésnél. Megóvja a Microsoft e-business platformokat, beleértve az Exchange Server-t az Outlook Web Access-el, a Proxy Server-t és a Site Server-t. Megóvja a Citrix NFuse-t, a MetaFrame-t, a Windows TerminalSzerver-t és a Symantec pcAnywhere-t.

Védelmet nyújt a Solaris, HP-UX, AIX és Red Hat Linux platformoknak. Támogatja a helyi, a telnet és az FTP hozzáférést. Beilleszthető a meglévő infrastruktúrába. Megóvja a NetWare -t és az NDS-t. Támogatja az NMAST (Novell Modular Authentication Service). Felügyeli a felhasználói hozzáférési jogokat az NDS-en belül, és egyidejűleg továbbhasonosítja az RSA Authentication Manager beruházását. Ha a távoli hozzáférésre és a VPN-re vonatkozó biztonsági követelmények növekednek a rendszeradminisztrátorok biztosak lehetnek abban, hogy az Agent szoftver megfelel majd a megnövekedett követelményeknek. Részletes műszaki leírás az alábbi oldalon érhető el: <http://www.rsasecurity.com/node.asp?id=1174>

Az RSA Authentication Agents beágyazásra került sok nagyobb hálózati kommunikációs termékbe, beleértve a legtöbb távoli hozzáférésű szerver, VPN-eket, tűzfalakat és egyebeket. Ma több mint 190 vezető gyártónak mintegy 290 terméke kapta meg az RSA SecurID Ready minősítést. Ez azt jelent, hogy megszerezték az RSA Secured státuszt, mivel biztonsági megoldásukat az RSA Security megoldására alapozták. Ily módon függetlenül attól, hogy a beszerzés során mit választanak hálózati infrastruktúrájukhoz, az RSA SecurID funkciói minden valószínűség szerint beépítésre kerültek a termékbe.

A megoldás hardver igénye (RSA Authentication Manager 6.1 esetén):

Támogatott operációs rendszer	Minimum követelmény
Microsoft Windows XP	733 MHz Pentium processor
Microsoft Windows XP (SP1)	512 MB of RAM
Microsoft Windows XP (SP2)	50 MB of free disk space
	TCP/IP networking

6. RSA SECURID TOKEN

Az RSA SecurID token egy speciális eszköz, mely 60 másodpercenként egy 6 számból álló sorozatot állít elő, ezt kell a felhasználónak azonosítás céljából megadni. Ezzel a módszerrel elérhető, hogy a felhasználónak biztosan rendelkeznie kell a token-el, hiszen 60 másodperc elteltével az – esetlegesen – megjegyzett számsorozat már nem érvényes. További biztonságot jelent, hogy a mobiltelefonokhoz hasonlóan maga a token is védhető egy PIN kód segítségével.



Az RSA SecurID autentikátorok egy jelszó megadásával egyszerűen használhatók, azonban ennél sokkal biztonságosabbak. Minden végfelhasználó számára kijelölésre került egy RSA SecurID autentikátor, amely egy egyszer használatos kódot generál. Bejelentkezéskor a felhasználó egyszerűen megadja ezt a számot és titkos PIN-jét, hogy sikeresen azonosítsa magát. Az RSA SecurID megoldást egyformán könnyű bevezetni és felügyelni. További előny, hogy az RSA SecurID hardver tokenek előzetes ismereteket nem igénylő megoldások, melyeknek nincs egyéb szoftverre szükségük a felhasználó számítógépén, így az eszközök átvételkor azonnal működőképesek. Az adminisztrátorok gyoRSAn felfedezik, hogy az RSA SecurID megoldást sokkal kevésbé költséges kezelni, mint a jelszavakat.

Minden RSA SecurID autentikátor rendelkezik egy nagyteljesítményű algoritmussal kombinált egyedi szimmetrikus kulccsal, amely 60 másodpercenként új kódot generál. Mivel a szám megjósolhatatlan és dinamikus, a hacker számára kivételesen nehéz feladatot jelent a helyes számot kitalálni bármely adott időben. A szabadalmaztatott műszaki megoldás minden autentikátort szinkronizál a biztonsági szerverrel, így garantálva a biztonság magas szintjét. Ez a védelem szinte megfizethetetlen, ha a figyelembe vesszük az illetéktelen hozzáférésnek kitett kritikus erőforrásokkal járó kockázatot.

Az RSA SecurID Ready Programon keresztül több mint 190 vezető tűzfal, távoli hozzáférésű szerver és VPN gyártó terméke támogatja az RSA SecurID azonosítási megoldását. Továbbá az RSA Authentication Agent szoftver segítségével lehetséges a két-faktoros azonosítás kiterjesztése a hálózati operációs rendszerre és alkalmazásokra, ideértve a Windows környezeteket és a web alapú alkalmazásokat. Az együttműködő-képességnek ez a magas szintje az adminisztrátorok számára lehetővé teszi a kezdeti azonosítási beruházások megóvását és egyedülálló az iparban.

Az RSA SecurID rendszer egyike a világ vezető két-faktoros felhasználó azonosító megoldásainak. A többféle megjelenésű második faktor révén minden szervezet megtalálhatja az igényeinek megfelelő RSA SecurID autentikátort.

A népszerű RSA SecurID idő-szinkronizált hardver token is egyike azoknak az eszközöknek, amelyek új kódot generálnak és mutatnak a képernyőn 60 másodpercenként. A népszerű kulcstartó forma (key-fob) szélsőségesen nagy tartósságot biztosít megbízható és helyfüggetlen formában. Az eredeti RSA SecurID hardver token hitelkártya méretű eszköz, amely ugyanazt a kiváló teljesítményt és minőséget nyújtja, mint amit minden RSA SecurID autentik garantál. Ezen túlmenően az RSA SecurID PINpad kártya hasonlít a általánosan használt kártyára azzal a kiegészítő tulajdonsággal, amely lehetővé teszi a felhasználók számára, hogy titkosítsák bejelentkezési kódjukat és ezzel még magasabb szintű biztonságra tegyenek szert.

Az RSA SecurID szoftver tokenek ugyanazokat az algoritmusokat használják, mint az RSA SecurID hardver tokenek. A szoftver alkalmazás úgy működik, mint az RSA SecurID PINPad kártya azzal a plusz előnnyel, hogy automatizált hozzáférést biztosít a védett web-oldalakhoz egy általános böngésző interfészen keresztül. Az RSA SecurID szoftver tokenek kiküszöbölik annak a feladatát, hogy a felhasználók csak dedikált hardver eszközökkel azonosíthassák magukat jól ismert interfészekon használatakor. Az RSA SecurID szoftver tokenek rendelkezésre állnak a Microsoft Windows munkaállomásokhoz, a PDA-khoz (beleértve a Palm Pocket PC-t és a Blackberry eszközöket), a Windows Mobile 2003 eszközökhöz és a Nokia, Ericsson és DoCoMo mobiltelefonjaihoz.

Az RSA SecurID autentikátorokat úgy terveztük, hogy az AES (Advanced Encryption Standard) algoritmus ipari szabványainak előnyeivel rendelkezzenek. A vevők élvezhetik az AES algoritmus használatából adódó integritást és minőségbiztosítást.

Az RSA SecurID szoftver token támogatja a minőségellenőrzött smart kártyákat vagy az USB autentikátorokat. A PIN védett RSA 5100 SmartCard és az RSA 6100 USB Autentikátor képes tárolni az RSA SecurID szimmetrikus kulcsot. Ezen eszközök digitális dokumentumokat és Java appleteket is tárolnak sokoldalú alkalmazási környezetek számára.

Az RSA jelenleg kétfajta token típust árul:

- Szoftveres token
- Hardveres token

Az alábbi ábrán láthatóak a jelenleg forgalomban lévő eszközök. A megoldások kaphatóak 2, 3, 4, 5 éves időtartammal is, a vásárlás után a token-el kapcsolatosan nincs további költség.



RSA SecurID SD600



RSA SecurID SID700



RSA SecurID SD200



RSA SecurID SID800



RSA SecurID SD520



BlackBerry with
RSA SecurID software token

2. ábra: Az RSA token-ek áttekintése.

A szoftveres token-ek kaphatóak nem csak Blackberry, de Microsoft Pocket PC-re, Microsoft Mobile-ra, Balckberry eszközre, Palm-ra is.