

NMAS

Novell Modular Authentication Services

Szerző: Linda Kennard (Niche Associates).

Megjelent a Netware Connection 2000. Februári számában.

Látta 1997 sikerfilmjét, a „Mission Impossible-t”? Ebben az esetben emlékeznie kell arra a jelenetre, mikor Ethan Hunt (Tom Cruise alakításában) egy nyílason leeresztve magát szupertitkos információkat tölt le egy nyomás-érzékeny padló felett lebegve. (Kevésbé izgulós nézők Leslie Nielsent csodálhatták meg a „Szikiszőkevények”-ben, hasonló helyzetben). Míg nézzük a Hollywoodi Gyártelep életről való elképzelését, valószínűleg mindannyian Hunt-ért szurkolunk. Pedig a való életben sokkal valószínűbb hogy azért az IT csapatért kellene szorítanunk, amely felelős azoknak az információknak a biztonságáért, amelyet éppen ezek a Hunt félek akarnak ellopni. Nagy valószínűséggel a kedves olvasó is adminisztrátor, és munkájának része az információ, az adatok védelme.

Nyilván nem feladatunk olyan titkosságú adatok védelme, amiért a kémfilmek pozitív hősei életüket kockáztatják. Mindazonáltal saját vállalatunknak is vannak bizalmas adatai – lehetnek ezek akár kormányzati vagy katonai titkok, hallgatók vagy betegek adatai, bankszámlák, kutatási eredmények, vagy afféle egyéb hétköznapi dolgok, mint például egy bérjegyzék. Hogyan védhetjük meg információinkat? Először megköveteljük a felhasználótól, hogy hitelesítse (authenticálja) magát, ezután megbizonyosodhatunk arról, csak a felfogósított felhasználók érhetnek el hálózati információkat. Aztán, használhatjuk az igen biztonságos NDS password authentication technológiát, mondja Buck Gashler, igen neves Novell termékfelelős, bár - teszi hozzá - van bizonyos biztonsági probléma a jelszavakkal. Mi mindannyian tudjuk, mire gondolt neves barátunk. Akárhányszor is mondhatjuk el felhasználóinknak a biztonságos jelszóképzés alapjait, ezeknek az alapoknak megvalósíttatása végül meghaladja erőnket. Hogy lehetne garantálni, hogy senki se használja születési dátumát vagy kutyájának nevét? Hogy győződhetünk meg arról, hogy a kiragasztott kis sárga Post-it cetlikre nincs kiírva jelszó, vagy egyéb bizalmas adat. A válasz (nemcsak Buck Gushler mondja!): sehogy. Egy kémnek nem kell nagyon igyekeznie a jelszó feltörésével, elég egy figyelmetlen vagy közömbös felhasználó!

Mit tudsz? Mid van? Ki vagy?

Természetesen a jelszó nem az egyetlen titkos dolog, amit a felhasználó használhat a hálózat eléréséhez. A jelszó csupán egyike a három login fiktornak. Mely három kategóriáról van szó? Ime:

- Mit tudsz? - valami, amit a felhasználó tud, például a jelszó.
- Mid van? - valami, ami a felhasználó birtokában van, például token, nyilvános kulcsú azonosítás, smart card.
- Ki vagy? - személyes tulajdonság, csak a felhasználóra jellemző: arc, szem, ujjlenyomat, hang, homlok, stb...

A login eljárások egy vagy több faktort használhatnak a három említett kategóriából. Mindegyik módszernek megvan a saját erőssége és gyengesége. Rossz a kérdés, hogy melyik közülük a legbiztonságosabb. Felismerve a jelszavas bejelentkezés problémáit sokan fontolgatják alternatív login módok használatát. Bár sokan gondolkodnak e lehetőségek használatáról, mindeközéig mégiscsak a jó öreg jelszavas azonosítást használják. Az ok: a jelszavas azonosítás volt az egyetlen, amit az NDS natívan támogatott, ráadásul az alternatív azonosítási módok sokkal több időt (és pénzt) rabolnak el, mint amennyit meg lehet spórolni.

A múlt században még mindenestre a kétkedőknek volt igazuk. A XXI. Század első negyedében a Novell Modular Authentication Service (NMAS) rácáfolt eddigi kalkulációinkra. Az NMAS kliens-szerver szoftvere és ConsoleOne snap-in modul segítségével bármelyik login faktort bármilyen kombinációban használhatjuk felhasználóink NDS-beli azonosításához.

Erősebb védelem

Az NMAS ezeket a login metódusokat a számos saját, és más gyártó hitelesítő moduljainak használatával támogatja. Ebben az első változatban (release) a Novell fejlesztésű modulok az NDS password, illetve az X.509 v3 alapú belépéseket támogatják.

A Novell Certificate Server 2.01 egy nyilvános kulcsú hálózat (PKI) szoftver, melynek segítségével létrehozhatunk, menedzselhetünk, tárolhatunk nyilvános kulcsú hitelesítéseket (szabványos X.509 v3 formában) a hozzátartozó privát kulcsokkal. Az NDS fán belül alkothatunk egy vállalat-specifikus Certificate Authority (CA) szolgáltatást. Ezzel létrehozhatunk egy belső CA aláírást szerver és felhasználó azonosítására. Külső CA, mint például a VeriSign felé küldhetünk aláírások hitelesítő kéréseket. A Novell Certificate Server 2.01 megtalálható az NMAS Enterprise Edition CD-n, valamint a <http://www.novell.com/download#NDS> oldalról. A Novell Certificate Server a felhasználói bizonyítványokat az NDS User objektum userCertificate nevű attribútumában tárolja. Mielőtt egy NMAS engedélyezett hálózathoz akarnánk használni az azonosító kulcsot, az NDS-ből le kell azt tölteni floppyra, a helyi merevlemezre vagy akár egy smart card-ra.

A Novell által fejlesztett autentikációs modulon kívül az NMAS a következő modulokat tartalmazza:

- ActivCard Module for NMAS az ActiCard Inc. termékeként,
- Identicator Biologon for NMAS az Identicator Technology-tól,
- RSA/ACE/Agent for NMAS az RSA Security Inc. terméke
- Secure Authentication Facility (SAF) Module for NMAS a SAFLINK Corp. terméke,
- VASCO Digipass Module for NMAS a VASCO Data Security Inc áldásaként.

Ezeknek a moduloknak a révén a login faktorok széles választékát használhatjuk. Hitelesíthetünk smart card, token, ujjlenyomat, hang vagy arc alapján. Használatukhoz szükség van további hardver, illetve szoftver elemekre. Amint több gyártó készít NMAS hitelesítő modulokat saját login eljárásuk használatához, lehetőségünk lesz a megfelelő szoftver installálására. Természetesen az új NMAS modul attól a gyártótól szerezhető be, aki ezt kifejlesztette. Emellett a Novell lehetővé teszi ezeknek az új moduloknak letöltését a saját web oldaláról.

A hitelesítő modulok arzenáljával lehetőség nyílik egy vagy több vállalati hitelesítési irányelv (policy) kialakítására, melyek mindegyike olyan login szekvenciát jelez, mely az NDS hitelesítéshez szükséges. Ez a szekvencia egy vagy több NMAS által támogatott login módszert használhat, attól függően, hogy az NMAS Starter Pack vagy Enterprise Edition verzióját használjuk.

Az NMAS Starter Pack letölthető a Novell Web site-ről. Használatával egy vagy több login szekvenciát, sorrendet hozhatunk létre mindegyikük egy, de csak egy login módszeren alapulhat. Például használhatjuk az Identicator BioLogon modulját, ami egy ujjlenyomat ellenőrző login módszer. Ilyenkor egy ujjlenyomat-olvasó berendezés használatával történik az azonosítás. Használhatunk kétfaktoros login módszert, ilyen az RSA Security RSA/ACE Agent, amelyik PIN kód bevitelét és token, vagy smart card használatát követeli meg. De az ActiveCard vagy a VASCO modulokat szintén alkalmazhatjuk kétfaktoros bejelentkezéshez. A biztonság első szintjén túl szabályozhatjuk a felhasználóink hozzáférését a hálózathoz az Acces Control List (ACL) használatával.

Más szavakkal, az NMAS Starter Pack-al nem vagyunk többé jelszó alapú login metódusokhoz kötve. Viszont ebben az esetben nem kombinálhatjuk a login módszereket, és nem vezérelhetjük a login szekvencia alapú felhasználói hozzáféréseket. Ezekhez a lehetőségekhez az NMAS Enterprise Edition verzióját kell választani.

Ellentétben a Starter Pack-kal, itt korlátlanul kombinálhatjuk a login szekvenciákhoz alkalmazott módszereket, például az ActiveCard smart card megoldását az Identicator ujjlenyomat-azonosító Biologon moduljával. Ebben az esetben a hitelesítéshez az NDS jelszó, egy PIN kód, egy smart card és ujjlenyomat olvasó szükséges. Habár a login metódusok keverése önmagában is érdekfeszítő, mégsem ez a legizgalmasabb vonása az NMAS Enterprise Edition-nek. Ennél is értékesebb a Netware5 hitelesítési osztályainak, fokozatainak (Graded authentication) kihasználása. Ez a képesség tovább finomítja a biztonságot a három különböző eszköz kombinációjával:

- Grades (fokok, fokozatok),
- Security labels (biztonsági címkék),
- Clearence levels (engedély szintek).

Mikor az NMAS modulokat fejlesztették, mindegyik modulhoz egy fokot rendeltek. Az NMAS 1.0-nál ez a fok a login faktor vagy faktorokon alapul. A következő fokok (grades) léteznek:

- Biometric & Password & Token
- Biometric & Password
- Biometric & Token
- Password & Token
- Biometric
- Password
- Token.

Az NMAS lehetővé teszi, hogy biztonsági címkéket rendeljünk az NDS partíciókhoz és NetWare kötetekhez. Ezek a címkék, egy kivételtől eltekintve ugyanazok, mint a fentebb felsorolt fokok. A kivétel a „Logged In” biztonsági címke, amellyel lehetővé válik a hozzáférés mindenféle különleges login metód nélkül. Mindegyik felhasználó, aki a hálózatra kapcsolódik, de nincs hitelesítve, read only joggal bír bármelyik Logged In címkéjű kötethez, partícióhoz. (Természetesen a NetWare kötetekhez a hozzáférést továbbra is az ACL határozza meg). Mivel a NetWare kötetek és partíciók alapértéke Logged In, csupán címkét kell cserélni a hozzáférés korlátozásához.

A hozzárendelt biztonsági címkék megfelelnek a login metódus fok(ozat)ainak. Például, ha Biometric & Token címkét rendelünk kötetünkhöz, majd olyan login szekvenciát hozunk létre, mely egy login metódusban egyesíti a Biometric és Token fokokat. Létrehozhatunk login módszereket külön-külön Biometric és Token fokokkal, ezek kombinált foka megegyezik a Biometric & Token biztonsági címkével.

A biztonsági címkék partíciókhoz és kötetekhez való rendelésének fő előnye az, hogy megnöveli az érzékeny információt tartalmazó hálózati részek biztonságát. A címkék használata önmagában nem elegendő, érvényre juttatásukhoz az NDS User objektumhoz kell rendelni egy vagy több engedély szintet (clearance level). A hozzárendelt engedélyszint nevek azonosak a biztonsági címkék neveivel éppúgy, mint ahogy a fokok nevei a hitelesítő modulokéval. Tehát a User object engedélyszintjeinek neve Biometric & Password & Token, Biometric & Password, Biometric & Token, s így tovább. Hozzárendelhetünk továbbá „Multilevel Administration” engedélyt, mellyel a teljes hálózatra írás-olvasás jogot biztosít. Nyilván ez utóbbi szintet csak korlátozott számban javasolt biztosítani.

Midőn a felhasználóhoz egy meghatározott engedélyszintet rendelünk, írás-olvasás jogot kap azokhoz a NetWare kötetekhez, partíciókhoz ahol ez a szint megegyezik az adott biztonsági szinttel. Természetesen ennek az a feltétele, hogy a felhasználótól elvárt legyen az adott engedélyszint és a használt login módszer ezzel egyezzen meg. Például tételezzük fel, hogy felhasználónk Biometric & Token engedélyszinttel rendelkezik, a login folyamán ez „kérve van”, és Biometric & Token metódust használ. Ebben az esetben R/W jogai vannak minden olyan kötethez, mely ezzel a Biometric & Token címkével bír. Sőt, Read Only joggal hozzáférhet azokhoz a kötetekhez/partíciókhoz, ahol kevesebb, de legalább egy faktort megneveztünk az engedélyezési szintben.

Ha egy felhasználó Biometric & Token engedélyhez kötött, a login folyamán ez elvárt, akkor a Biometric címkés és a Token címkés kötetekhez csak olvasás (RO) hozzáférése lesz. Ha most a kedves olvasó azon csodálkozik, hogy miért is nincs ezekhez a kötetekhez rögtön írás/olvasás jog, fontolja meg: minél több faktor típust használunk a login folyamán, annál biztonságosabb a hitelesítő rendszer. Épp ezért, a kötet/partíció címkék két vagy három különböző típusú login faktor kombinációjával legbizalmasabb információinkat védhetik meg – biztosnak kell lennünk abban, hogy a RW joggal rendelkező user azért mégse tudja felülírni a fontos adatokat tartalmazó köteteket. Ezeknek az információknak a védelmére az NMAS csupán Read Only jogot ad oda, ahol a címkékben ugyanaz előfordul ugyan, de a felhasználói engedély szintben (user clearance level) meghatározottnál kevesebb faktor azonos.

Dan Fritch, neves Novell fejlesztő menedzser szerint a fokozatos hitelesítő tudása révén az NMAS „dinamikus mount és dismount képességével lehetővé teszi, hogy a login folyamattól függjön kötetek írás, vagy olvasás elérése, ahelyett hogy globálisan kelljen ezekhez a kötetekhez Ro vagy Rw jogokat adni. Más szavakkal, az NMAS-sal és a fokozatos hitelesítéssel lényegében session alapon mount-dismountolhatunk köteteket és adhatunk írás-olvasás vagy csak olvasás jogot.

Fokok készítése

Az NMAS Starter Pack vagy Enterprise Edition futtatásához Netware 5 operációs rendszer és legalább Support Pack 3, NDS 8 és a Novell International Cryptographic Infrastructure (NICI) 1.5 szükséges, ez utóbbi része az NMAS-nak. A konfiguráláshoz a ConsoleOne 1.2 verzióját használhatjuk, amely szintén megtalálható az NMAS csomagban. A Starter Pack üzembe helyezéséhez az alábbiakban felsorolt pontok közül az első négyet, az Enterprise Edition-höz mind a hatot végre kell hajtani :

1. Létre kell hozni egy Login Method konténert.
2. Létre kell hozni egy Login Policy konténert.
3. Létre kell hozni egy Login Method konténert.
4. Létre kell hozni egy login szekvenciát.
5. A kötetekhez és partíciókhoz hitelesítési fok címkéket (authentication label) kell hozzárendelni.
6. A létrehozott címkéket User Objektumokhoz rendeljük.

Az NMAS installálásakor az NDS fá Security konténerében létrejön a Login Method konténer. Ezen a konténeren belül létrehozott Login Method objektumok megfelelnek a Novell vagy más gyártók által használt metódusoknak. Ugyancsak installálásakor jön létre a Login Policy konténer, melyen belül létrehozhatók a login szekvenciák. Általában azt mondhatjuk, hogy mindenegyes engedélyszinthez (clearance level) tartozik legalább egy login szekvencia. Például amennyiben Biometric & Password & Token, Biometric & Token és engedélyszintet hozunk létre, legalább három login szekvenciát is kell alkotnunk, egyik a Biometric, Token és Password, a másik Biometric és Token, és a harmadik Token metódust tartalmaz. Amennyiben létrehozunk egy Password engedélyt, ehhez nem kell létrehozni login szekvenciát, mivel az NMAS alapértelmezésben biztosít egy olyan szekvenciát, mely tartalmazza a Novell Password metódust.

Egy login szekvencia kialakításához a Login Policy konténer tulajdonság fülben a New Login Sequence sort választhatjuk. Ekkor az előugró Login Policy képernyőn két mező tűnik fel: baloldalon az elérhető metódusok (NDS password, SmartCard azonosítás, stb.), míg jobboldalon a Login Sequence (SafeLink Voice, RSA Token). Az Available Method mező tartalmazza az összes olyan metódust, amit a Login Method objektum részére hoztunk létre. Egy új login szekvencia létrehozásához egyszerűen csak egy új nevet kell adni és a baloldali Available Method mezőből a kívánt metódusokat kijelölni. Mielőtt kilépnénk a menüpontból, győződjünk meg a választott metódusok kívánt, helyes sorrendjéről. Végezetül, engedélyeznünk kell a hitelesítési fokozat -minősítéseket (graded authentication): biztonsági címkéket rendelünk mindazokhoz az NDS kötetekhez és partíciókhoz, amelyeket meg akarunk védeni és engedélyezési szinteket minden olyan felhasználó User objektumához, akinek el kell érnie ezeket az erőforrásokat. Pl.: Ssy kötet Properties/Security fülben Biometric&Token Securitz Label beállítással.

Megnövelt biztonság: az NMAS használata

Tegyük fel, hogy feladatunk a fizetési adatok megvédése, és ehhez a nemes feladathoz az NMAS programunkat, valamint minősített hitelesítést használunk. Azt akarjuk, hogy ezekhez az adatokhoz csak a személyzeti osztály dolgozói férjenek hozzá, Biometrikus és Token hitelesítési metódusok igénybevételével. Példánkban feltételezzük, hogy az NMAS-t már telepítettük, a szükséges adatok egy külön Netware kötetben találhatóak. Egy-egy Biometrikus illetve Token login metódus létrehozása után a Login Policy konténerben egy login szekvenciát állítunk össze, legyen ennek a neve Fizetés. A Login Sequence mező neve tehát Fizetés, a képernyő baloldalán található Available Methods mezőből adjuk hozzá a Biometric és Token metódusokat. Hozzárendeljük a Biometric&Token címkét ahhoz a kötethez és partícióhoz, amelyik azokat a bizalmas fizetési adatokat tartalmazza. Végezetül Biometric&Token engedélyeket rendelünk a személyzeti osztály dolgozóinak User Object-jeihez. Mikor Anna nevű felhasználónk először lép be a hálózatba, kezdeti Login screen mezőjébe nevét beütve az Advanced fülre fog kattintani. Két újabb mező fog feltűnni, mindkettőben legördülő mező ad választékot. A Login mezőben kiválaszthatjuk annak a szekvenciának a nevét, amit használni fogunk, azaz a Fizetés nevűt. A Clearance (engedély) mezőben a Biometric&Token szintet választjuk. Az OK gombra kattantva Anna az NDS által hitelesítődve írás/olvasás jogot nyer ahhoz a kötethez, ahol a fizetési adatok vannak, és read only jogot kap az összes olyan kötethez, amelyikhez Logged In, Token vagy Biometric címkék vannak rendelve (feltételezve, hogy Anna ACL-jei szintén lehetővé teszik ezt). Az Advanced beállításokat csak az első belépéskor, illetve változáskor kell állítani.

Színfalak mögött

Bár már tudjuk mi történik mikor Anna az OK gombra kattint, igen érdekes az is, ami a háttérben zajlik. Mikor Anna első belépésekor beírta nevét, kiválasztotta a belépési szekvenciákat és szinteket, ezek a beállítások a Windows registry-be íródnak. Az OK gombra kattintva a Novell kliens meghívja az NMAS klienset. Ez utóbbi keresi a hálózaton azt a szerveret, amelyik az Anna User object adatait tartalmazza. Ezeknek a szervereknek a megtalálása után az NMAS szerveret kell megtalálni. Azzal létesítünk kapcsolatot, amelyik tartalmazza Anna adatait. (Amennyiben több NMAS szerveren megtalálhatóak Anna Felhasználói Objektumának példányai, a kliens véletlenszerűen választ egyet). Ezután az NMAS szerver és kliens egy, a NICI által generált session key-t cserél. Ez a kulcs lehetővé teszi egy biztonságos csatoma létrehozását, amelyiken át a titkosított hitelesítő információk áramlanak. A következő lépésben az NMAS kliens küld egy üzenetet a szervernek, amely tartalmazza az összes login metódust, ami installáltunk. A Novell minden login metódushoz egy számot rendel hozzá. Tételezzük fel, hogy bár Anna NMAS kliense 5, 6, 7, és 8 metódusokat támogatja, most ő csak az 5. és 8.-t fogja használni. Tehát az üzenet felsorolja mind a négy lehetséges metódust,

jelzi, hogy először az 5-ös számú, majd a 7. hajtódik végre. Az NMAS szerver válaszul meghívja a Login Server Method (LSM) eljárást az 5. metódushoz kapcsolva, üzenetet küld a kliensnek (*DO 5*, azaz biometrikus eljárás következik), a kliens pedig meghívja a megfelelő Login Client Method –t(LCM) és DLL-t.

Az LSM és LCM egy Multiprotocol-Authentication Framework (MAF) protokoll segítségével cserél információt. Ez a Novell által fejlesztett protokoll „Multi-Authentication Framework Method for SOCKSv5” néven az IETF egyik Internet tervezete. Az NMAS-nak nincs tudomása arról, hogy a kliensek milyen információt küldözgetnek egymásnak. Ebben az eljárásban LCM által meghívott user interféce megkéri Annát, hogy nyomja hüvelykujját az ujjlenyomat-olvasóba. Az LSM-be küldött adatok összehasonlítodnak az NDS-ben tároltakkal. Amennyiben Annát a biometrikus faktor azonosítja, az LSM üzenetet küld sikeres műveletről. Amennyiben az azonosítás nem sikerült, sikertelen login szekvencia jelzés érkezik a klienshez, a képernyőn újra megjelenik a login screen, Anna próbálkozhat újra. A sikeres login metódus után az NMAS szerver ellenőrzi, hogy vajon megkapta-e az összes szükséges információt. Ebben az esetben hiányzik a token bevitele, tehát *DO 7* üzenet érkezik az NMAS klienshez, tehát a token adatit is be kell vinni. Az eljárás addig folytatódik, míg a szerver az összes olyan adatot meg nem kapja, ami Anna biztonságos hitelesítéséhez szükséges. Amikor az összes hitelesítéshez szükséges információ megérkezett, az NMAS szerver nyugtát küld a kliensnek. Erre válaszul a kliens kéri, és kapja Anna NDS jogosítványait, amelyek ennek a session-nek az engedélyszintjeit jelzik. A kapott jogosítványokat a kliens egy titkos helyen tárolja, s mikor a felhasználó a szerveren információkat akar elérni, Anna jogosítványait titkosítva elküldi. Ebben a pillanatban létrejön a hitelesített kapcsolat. Ez a folyamat, bármilyen bonyolult is, a másodperc törtrésze alatt zajlik le.

Az NMAS hatása a hollywoodi profitra

Amennyiben a háttérben dolgozó lelkes IT csapat az NMAS-t és valamelyik login kombinációt alkalmazta volna információi megvédésére Ethan Hunt ellen, a „Mission Impossible” kevésbé lett volna sikeres a nézőknek éppúgy, mint a producereknek. Nem kellett volna aggódni a leesni készülő édesség miatt, vagy a riasztót is megszólaltató – végül valóban leeső – kés miatt. A nézők unatkozva majszolhatnák pattogatott kukoricájukat, ásítózva figyelve Hunt szánalmas kísérleteit. A „betörés” nyilvánvalóan sikertelen, Tom Cruisznak nem olyan a hangja, más az ujjja, nincs Smart kártyája: esélye se lenne bármilyen bizalmas adat birtokába jutni – még a jelszó birtokában sem. Bár az efféle filmek nyilvánvalóan megbuknának, a biztonságos azonosításra épülő új világtrend által nyújtott lehetőségek biztosan kárpótolnak majd a veszteségért.

Login metódusok

ActiveCard modul (ActivCard Inc.) biztosítja a szerver szoftvert a Smart kártya alapú digitális azonosításhoz, és PIN kódot. Amikor az ActiveCard metódust használjuk egy login folyamatban, az ActiveCard Gold kártyát bedugva a leolvasóba és a PIN kód (vagy akár nyilvános kulcsú azonosítás) bevitelével lehet a rendszerbe belépni. Az ActiveCard Module for NMAS kompatibilis a Novell Certificate Server 2.0.1 –el, amelyik a felhasználók nyilvános, és a hozzá tartozó privát kulcsukat tárolja az NDS-ben. Ezt az információt át lehet másolni az ActivCard Goldra. A kártya nem csak azonosításra szolgálhat: a felhasználó konfigurálhatja levelező programját, titkosíthatja és digitális aláírással láthatja el leveleit. (A Novell Certificata Server letölthető a <http://www.novell.com/download>NDS> oldalról. Azonkívül amit az ActiveCard Module for NMAS szerver szoftver biztosít, a következő hardver és szoftver elemeket kell beszerezni :

- ActiveCard Gold (felhasználónként egyet), amelyik tartalmazza a kliens szoftvert, a többcélú smart kártyát, opcionálisan a kártyaolvasót,

- ActivePack for NDS, egység és jogosítvány menedzselő szoftvert, segítségével az adminisztrátorok közvetlenül a ConsoleOne által felügyelhetik a smart kártyákat és azok tartalmát.

Az ActivCard weboldala : <http://www.activcard.com> , európai képviselőéhez a <mailto:info@activcard.fr> címen lehet írni.

Identicator biologon module for NMAS

Gyártója az Identicator Technology (Identix). A szerver és kliens szoftver lehetővé teszi ujjlenyomat alapján történő azonosítást. Támogatja a legtöbb hardvergyártó ujjlenyomat-olvasóját, a standalone egységeket és a billentyűzetbe vagy egérbe épített egyaránt. Információt a <http://www.identicator.com> oldalon találhatunk.

RSA Ace/Agent for NMAS

Az RSA Security Inc. termékeként kétfaktoros login metódust tesz lehetővé. A felhasználótól nem csak egy PIN kód bevitelét követeli meg, hanem egy RSA SecureId azonosítót is. Ez az azonosító lehet akár egy smart kártyán, de lehet egy hardver vagy szoftver alapú token, attól függően, hogy melyik opciót választottuk. Az RSA SecureId minden 60 másodpercben generál egy egyszer használatos jelszót. A kétfaktoros login után az RSA ACE/Agent átirányítja a kérést a az RSA ACE/Serverhez, amely hitelesítő szoftvert az RSA Security -től kell megvenni. További leírás a <http://www.rsasecurity.com> oldalon található.

Secure Authentication Facility (SAF) Module for NMAS

Ez a termék a SAFLINK Corp. fejlesztése, szerver és menedzsmint szoftvert tartalmaz biometrikus login faktorokhoz. A SAFLINK login metódus alkalmazásához szükség van a client software for the SAF module for NMAS termékre, amely három plug in modul tartalmaz: egy a hang alapján történő azonosításhoz, egy az arc , végül az utolsó egy ujjlenyomat alapján történő azonosításhoz használható. A hang azonosításhoz csupán egy kommersz hangkártyára és mikrofonra van szükség, az arcfelismeréshez mindössze egy digitális kamera kell. A SAFLINK megadja azoknak a kameráknak, ujjlenyomat-olvasóknak a listáját, amelyek biztosan használhatók szoftveréhez, illetve közvetlenül tőle is rendelhető ujjlenyomat azonosító.

Az alap modulokon kívül vásárolható íriszazonosításon alapuló metódus NMAS környezetbe.

A SAF Module for NMAS plug-in kliens modulok próba verziója letölthető a SAFLINK web oldaláról : <http://www.saflink.com> .

VASCO Digipass Module for NMAS

A VASCO Data Security Inc. termékeként token alapú technológiát biztosít. Az NMAS-ban található szoftver mellett meg kell venni a Digipass authentication device -t minden felhasználó számára, aki ezt a login metódust használja. Használható bármilyen jelenleg létező és jövőben előállításra kerülő termék, így a Digipass Series 100, 300, 500, 600, 700, Access Key II, Authenticard egységek. Mindegyik ismeri és támogatja a Response Only és Challenge-Response üzemmódokat, használatul PIN kóddal védett. A beépített menedzsmint szoftverrel könnyen felügyelhetjük ezeket a PIN kódokat. Európában az info_europe@vasco.com címre írhat bővebb információért, illetve keresse a <http://www.vasco.com> oldalakat.

Fordította : Várkonyi György (Computer 2000 Hungary)