



Microsoft Windows Server System



Přehled

Země:

Česká republika

Odvětví:

Bankovníctví

Profil zákazníka

Jsme dynamická a moderní banka, člen finanční skupiny České pojišťovny, která nabízí široké spektrum bankovních služeb pro fyzické osoby a firmy. Jako první banka v České republice jsme nabídli našim klientům možnost využívání služeb přímého bankovníctví. Neustálé zdokonalování současných služeb a rychlý vývoj nových produktů, spolu s vytvářením osobních vztahů s klienty, umožňuje vám i bance být vždy o několik kroků před ostatními.

Uživatelský autentikační systém od společnosti truconneXion komplexně řeší otázku bezpečnosti interních počítačových systémů eBanky, a.s.

Projekt Uživatelské Autentikační Služby (dále jen UAS) vychází z potřeby na zvýšení bezpečnosti přístupu uživatelů k interním počítačovým systémům banky. Po zjištění skutečnosti, že na trhu neexistuje požadované řešení, rozhodla se společnost truconneXion takový produkt implementovat.

Výchozí stav:

Společnost eBanka, a.s., která disponuje rozsáhlou počítačovou sítí a desítkami poboček po celé republice, používala standardní nástroje pro administraci uživatelských přístupů a vykonávání procesů pro podporu uživatelů. V rozsáhlé počítačové síti měl tento způsob administrace a vedení uživatelských účtů za následek existenci následujících problémů:

- **nečisté síťové prostředí** – bez vazby na personální systém a bez jakékoliv automatizace procesů pro podporu uživatelů docházelo k existenci nepoužívaných či neoprávněnými osobami zneužívaných tzv. „mrtvých“ účtů
- **sdílení uživatelských účtů** – nebylo možné uživatelům zabránit ve sdílení svých uživatelských účtů, tento problém obecně souvisel se znalostí hesla uživatele k vlastnímu uživatelskému účtu
- **neexistence kontroly** – nebyly dostupné mechanismy pro zaznamenávání informací o přístupech do počítačové sítě, které navíc nelze provádět bez jednoznačné identifikace přistupujícího
- **nekonzistentní způsoby autentizace** – bankovní i jiné používané aplikace používaly vlastní nekonzistentní způsoby autentizace uživatele

Profil partnera

Od vzniku společnosti v roce 1993 jsme se stali spolehlivým partnerem již mnoha společností.

Přispíváme ke vzniku a naplnění jejich informačních strategií, k definici podoby jejich e-sluzeb, vyhledávání a využití příležitostí, které poskytují dnešní informační technologie. Pomocí funkční e-strategie jim umožňujeme podpořit celkovou strategii jejich společnosti.

Kontakty:

eBanka a.s.

Na Příkopě 19
117 19 Praha 1
telefon: +420 222 115 222
Email: info@ebanka.cz
[Http://www.ebanka.cz](http://www.ebanka.cz)

truconneXion a.s.

S.K.Neumanna 449
293 01 Mladá Boleslav
Tel. +420 326 711 711
Email: info@txn.cz
[Http://www.txn.cz](http://www.txn.cz)

Cíl řešení

Projekt UAS si kladl především tyto cíle:

- UAS bude vystavěna na bázi PKI
- autentizace uživatele a privátní operace budou prováděny pomocí HW prvku (čipové karty Gemplus řady GPK, konkrétně GPK8000 a GPK16000)
- zabezpečené přihlášení k systému Windows 2000
- poskytnutí programového interface pro implementaci autentizačních mechanismů aplikacemi třetích stran
- možnost centralizovaného managementu systému a HW prvků
- provázání s personálním systémem
- automatizace procesů pro podporu uživatelů
- modulárnost a škálovatelnost
- možnost bezpečného terminálového použití

Řešení

Určení systému UAS

UAS je systém radikálním způsobem zvyšující zabezpečení počítačové sítě proti rizikům vnitřního ohrožení. Prostřednictvím HW prvků a vydávaných certifikátů zajišťuje nezneužitelnost uživatelských účtů a jednoznačnou identifikaci uživatele v počítačové síti. Automatizací procesů pro podporu uživatelů anuluje možná procesní rizika.

Management systému, HW prvků a uživatelských přístupů je implementován s vědomím možné potřeby bezpečné centralizace, která však není nutností.

Princip řešení

UAS je rozsáhlý systém kombinující množství funkcí. Dle již uvedeného je lze rozdělit na funkce týkající se omezení rizik plynoucích ze zneužití uživatelských účtů a práv a na funkce automatizující procesy pro podporu uživatelů.

Základem autentizace uživatele k síti je autentizace vůči předmětu, v tomto konkrétním případě k čipové kartě. Ta je vydána každému uživateli a bez ní se není možné k síti přihlásit. Každá z vydaných čipových karet je unikátní a obsahuje mimo jiné privátní klíč, certifikát a seznam uživatelských účtů, ke kterým má uživatel práva. V systému tedy existují dvě základní entity. Jednou z nich je osoba, která je ekvivalentní čipové kartě a druhou vlastní uživatelský účet. Vztah mezi oběma entitami je N:N, tedy jedna čipová karta může obsahovat více různých uživatelských účtů a naopak, jeden uživatelský účet může být obsažen na více čipových kartách.

Autentizace uživatele spočívá v první řadě ověřením znalosti PIN, následně certifikátu uloženého na čipové kartě a kontrolou jeho práv pro přihlášení na zvolený účet. Uživatel nezná hesla přidělených uživatelských účtů.

Autentizace terminálového přístupu je řešena podobně s rozdílem, že pro ověření je používána lokální čipová karta. Komunikace mezi vzdáleným počítačem a lokální čipovou kartou probíhá šifrovaně na bázi protokolu SSL.

Veškeré požadavky na autentizaci jsou systémem zaznamenávány.

System může být administrován z jednoho místa, ze kterého lze vytvářet nové uživatelské účty, personalizovat čipové karty, přiřazovat uživatelské účty osobám apod. Jelikož administraci musí být možné provádět vzdáleně, existuje systém tzv. servisních požadavků. Administrátor vygeneruje servisní požadavek daného typu a ten se uloží v datovém úložišti, konkrétně do databáze. Uživatel čipové karty má možnost daný servisní požadavek ručně zpracovat nebo nechat na automatickém vyřízení před příštím přihlášením. Tímto způsobem lze velmi jednoduše kontrolovat možnost přístupu osob k jednotlivým uživatelským účtům. Stejně tak lze tímto způsobem umožnit uživatelům např. odblokování/zablokování čipových karet. Veškerá komunikace mezi administrátorem, SQL serverem i uživatelem probíhá šifrovaně.

Automatizace administráčních procesů probíhá na základě provázání s personálním systémem a spočívá v provedení předem definovaných specifických kroků, které mají vztah ke změně vycházející z personálního systému.

System poskytuje programový interface pro využití autentizace vůči čipové kartě.

Harmonogram prací

Květen 2002	definice potřeb a funkcionality systému UAS
Červenec 2002	první testování a počátek vývoje
Listopad 2002	Zahájení vývoje
Leden 2003	pilotní nasazení produktu u zákazníka


Hlavní přínosy

- Bezpečný přístup uživatelů k síťovým zdrojům, souvisí např. s neznalostí hesel k uživatelským účtům
- Jednodušší přístup uživatelů k síťovým zdrojům
- Management uživatelských účtů a obecně celého systému umožňuje bezpečně odebírat či přidávat uživatelské účty kdykoliv, odkudkoliv a komukoliv
- Vazba s personálním systémem a automatizace procesů pro podporu uživatelů omezuje lidské chyby a důsledkem je maximálně čisté síťové prostředí
- Zpětná kontrola – je možné zjišťovat kdo, kde, kdy používal síťové prostředky
- Otevřenost systému – systém lze jednoduše použít i pro autentizaci v dalších zákaznickem používaných systémech

Ukázky uživatelského rozhraní



Přihlášení uživatele - stanice PC00123456

 Čtečka čipových karet: Gemplus GemPC430 0

Uživatelské jméno: martin (TX2K)

PIN: [XXXXXXXXXX]

Terminálový přístup

IP Adresa: [] Připojit

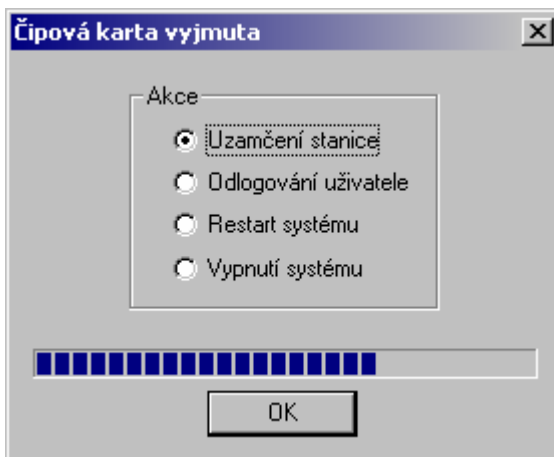
Vypnout stanici

Servisní požadavky

EN NUM Přihlásit Zpět Možnosti <<

Čipová karta je načtena.

Obr. 1: Přihlašovací dialog (nahrazuje standardní přihlašovací dialog Windows)



Čipová karta vyjmuta

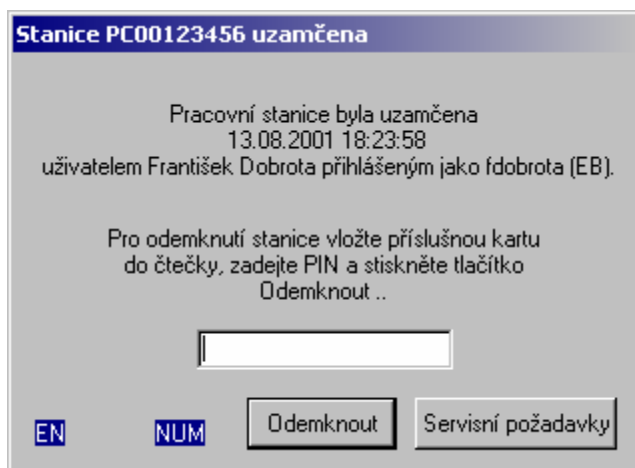
Akce

- Uzamčení stanice
- Odlogování uživatele
- Restart systému
- Vypnutí systému

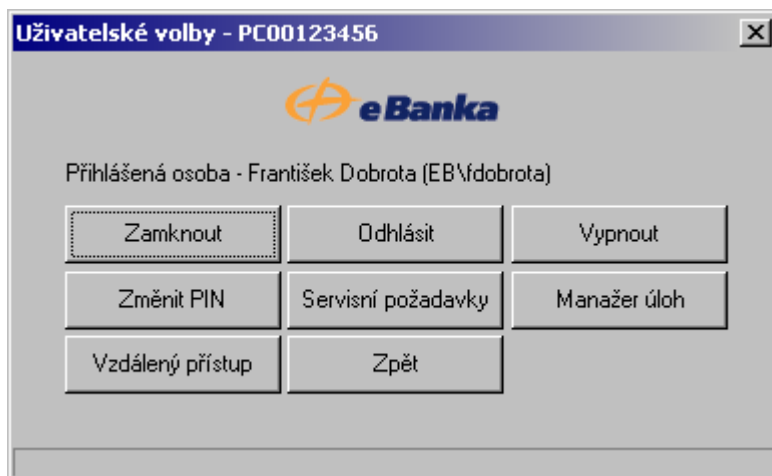
[Progress bar]

OK

Obr. 2: Dialog zobrazovaný po vyjmutí čipové karty ze čtečky



Obr. 3: Dialog uzamčené stanice (nahrazuje standardní dialog Windows)



Obr. 4: Dialog obsahující uživatelské volby (nahrazuje standardní dialog Windows)

Více informací

ČESKÁ REPUBLIKA:

Více informací o produktech a službách společnosti Microsoft s.r.o. naleznete na webových stránkách společnosti www.microsoft.com/cze nebo na telefonních číslech **Informační linky** +420 221 777 222, kde Vám jsou naši operátoři k dispozici denně od 8:00 do 20:00 a na **Hotline (Horké lince)** +420 221 503 222 v době od 8:00 do 18:00.

SLOVENSKÁ REPUBLIKA:

Více informací o produktech a službách společnosti Microsoft Slovakia naleznete na webových stránkách společnosti www.microsoft.com/slovakia nebo na telefonních číslech **Informační linky** +421 243 426 565, kde Vám jsou naši operátoři k dispozici denně od 9:00 do 17:00 a na **Hotline (Horké lince)** +421 267 296 296 v době od 9:00 do 17:00.

Logo Microsoft je registrovanou obchodní známkou společnosti Microsoft Corp. ve Spojených státech a/nebo v dalších zemích. Zmíněná jména ostatních společností a produktů mohou být rovněž ochrannými známkami.

Technologie Microsoft

- MS Windows 2000 Server
- MS Windows 2000 Professional
- MS SQL Server 2000
- MS Visual Studio 6.0

Technologie třetích stran

- Kryptografická knihovna (truconneXion)
- GZIP compression (Wei Dai)
- Lotus Notes SDK (IBM)

Partner

- **truconneXion a.s.**
S.K.Neumannova 449
293 01 Mladá Boleslav
- Kontakt: <http://www.txn.cz>