1. ÚVOD

Město Ústí nad Orlicí (dále také zadavatel či objednatel) již provozuje čipové karty ProID+Q a nyní požaduje další rozšíření v podobě implementace nadstavbových modulů. Za tímto účelem dne 23.5.2019 proběhl úvodní technicky zaměřený telefonát se zástupcem města Ústí nad Orlicí, na jehož základě předkládáme tuto specifikaci v předpokládaném základním rozsahu pro pokrytí primární potřeby zadavatele.

- **Základní komponenty ProID+**
  - čipové karty ProID+Q, hybridní s EM4102 (120 ks)
  - čtečky čipových karet Gemalto IDBridge CT30 (120 ks)

zadavatel **již nakoupil** v minulosti od předkladatele a další dokup se v rámci této dodávky nepředpokládá, nejsou tudíž předmětem.

Dodávka předpokládá integraci nadstavbových komponent ProID+ a služeb:

- **Nadstavbové komponenty ProID+**
  - Manažer ProID+ (softwarové nástroje):
    - Kartové centrum (KC)
    - Card management systém (CMS)
    - Authentication Certificate Exchange (ACEx)
    - aktualizovaný uživatelský SW balíček ProID+Q (s podporou synchronizace dat do CMS)
- **Služby**
  - Dokumentace (návrh životního cyklu karet v organizaci, návrh architektury PKI a základních parametrů, návrh šablon certifikátů, návrh doménových politik asistence s rozběnutím systému)
  - Aktivace doménové certifikační autority
  - Implementace aplikací pro správu karet
  - Školení
  - Servisní podpora

Požadavky k nasazení jednotlivých nadstavbových komponent ProID+ jsou následující:

- **KC**
  - je požadováno zřídit 2 pracoviště správce karet (tj. 2x instalace KC)
  - bude provozováno na odd. IT
  - Aplikace bude obsahovat následující scénáře:

  - Vydání nové karty – Scénáře budou nabízet funkcionalitu pro podporu procesu vydání nové čipové karty uživateli.
    - Vydání uživatelské karty a certifikátu
      - Uživatel se bude účastnit procesu vydání karty
      - Uživatel si bude nastavovat bezpečnostní kódy čipové karty na pracovišti správce karet pomocí klávesnice – PIN, QPIN i PUK, nebude se tisknout PIN formulář
      - Bude vytištěn protokol o předání karty a certifikátu

    - Vydání karty a certifikátu správce
        - Uživatel se bude účastnit procesu vydání karty
        - Uživatel si bude nastavovat bezpečnostní kódy čipové karty na pracovišti správce karet pomocí klávesnice – PIN, QPIN i PUK, nebude se tisknout PIN formulář
        - Bude vytištěn protokol o předání karty a certifikátu
    - Vydání dočasné karty – scénář pro vydání karty s certifikáte s omezenou dobou platnosti na 7 dní.
        - Na dočasné karty nebudou vydávány certifikáty z CA PostSignum
        - Uživatel se bude účastnit procesu vydání karty
        - Uživatel si bude nastavovat bezpečnostní kódy čipové karty na pracovišti správce karet pomocí klávesnice – PIN, QPIN i PUK, nebude se tisknout PIN formulář
        - Jako další možnost, bude v dokumentaci zmíněna možnost povolení dočasného přihlášení pomocí jména a hesla. Objednatel se bude moci později sám rozhodnout, kterou možnost zvolí.
- Spárování karty s uživatelem – Scénář, poskytující možnost, na již používané karty dovydat certifikáty z doménové CA a karty zanést do budované evidence.
    - Spárování používané karty s držitelem
        - Uživatel se bude účastnit procesu vydání karty, bude zadávat bezpečnostní kód PIN
        - Bude vytištěn protokol o předání certifikátu
    - Spárování používané karty se správcem
        - Uživatel se bude účastnit procesu vydání karty, bude zadávat bezpečnostní kód PIN
        - Bude vytištěn protokol o předání certifikátu
- Obnova certifikátů – Scénář bude sloužit k obnově neplatných certifikátů vydaných z doménové CA, např. po vypršení jejich platnosti
    - Obnova certifikátu uživatele
    - Obnova certifikátu správce
- Recyklace karty – formou průvodce smaže z karty všechny certifikáty a nastaví výchozí hodnoty bezpečnostních kódů. Použitou kartu připraví k vydání novému držiteli. Původní držitel bude muset zadat PUK čipové karty.
- Problémové stavy karty – Scénáře určené k řešení problémových stavů karty:
    - Ztráta
    - Odebrání
    - Skartace.
- Import nových karet

CMS

- Aplikace CMS_WP a webové služby CCM, CMS a IIM budou instalovány na nově zřízený virtuální server OS Windows server 2012 pracovníky Monet+ pomocí vzdáleného přístupu. Zřízení serveru a zřízení vzdálených přístupů zajistí objednatel.
- DB pro tuto aplikaci a služby bude instalována na stejném virtuálním serveru, MS SQL 2018 edice express. Instalaci DB zajistí objednatel.

ACEx

- Bude zajišťovat obnovu certifikátů na čipových kartách z CA PostSignum i z doménové CA
    - Certifikát uživatele vydávaný na čipovou kartu z doménové CA
    - Certifikát Správce karet vydávaný na čipovou kartu z doménové CA
    - Kvalifikovaný certifikát vydávaný z CA Post Signum na čipovou kartu
    - Komerční certifikát vydávaný z CA Post Signum na čipovou kartu

Balíček ProID+Q

- zadavatel používá nyní standardní verzi balíčku, staženou z webu ProID+ (tzn. bez funkce Card Content Monitor – CCM,)
- dojde k nahrazení balíčku za verzi s CCM, budou synchronizovány karty vůči nově budované evidenci CMS

- **CA**
  - zadavatel aktuálně neprovozuje doménovou CA
  - zadavatel zřídí nový samostatný virtuální stroj Windows Server 2012 kde zhotovitel vybuduje novou CA na platformě MS Windows server v módu Enterprise
  - zadavatel nyní používá kvalifikované i komerční certifikáty od CA PostSignum. Postup správy a vydávání těchto certifikátů nebude tímto projektem zasažen, procesy zůstanou zachovány
  - Plánované použití PKI a certifikátů vydávaných z doménové v prostředí zadavatele:
    - autentizace uživatelů do PC pomocí certifikátu a čipové karty (nahradí aktuálně používané přihlášení doménovým jménem a heslem)
    - podepisování interních e-mailů
    - podepisování v interních systémech
    - bez podpory šifrovaní
    - platnost certifikátů pouze v rámci domény (klíč CA a CRL nebude vystaveno do internetu)
    - pro servery vystavené do internetu zadavatel používá HTTPS certifikáty externích dodavatelů (nebude tímto projektem zasaženo, procesy zůstanou zachovány)
    - zadavatel používá Open VPN (nebude tímto projektem zasaženo, procesy zůstanou zachovány)
    - zadavatel obdrží od předkladatele před zahájením realizace projektu požadavky na zřízení vzdáleného přístupu a zřízení serverů

  - Dokumentace bude zahrnovat
    - popis životního cyklu karet a certifikátů v organizaci
    - návrh architektury PKI a základních parametrů
    - návrh šablon certifikátů
    - návrh doménových politik

Jednotlivé naní dodávané komponenty jsou podrobněji specifikovány v následujícím textu.

2. NADSTAVBOVÉ KOMPONENTY PROID+

Manažer ProID+ je balíček SW nástrojů, který integruje do organizace nejdůležitější procesy potřebné pro práci s čipovými kartami a certifikáty.

Manažer ProID+ zajišťuje snadné ovládání procesů spojených s kartami a certifikáty v organizaci. Jeho funkce jsou do organizace implementovány prostřednictvím samostatných aplikací. Následující podkapitoly popisují funkci jednotlivých aplikací.

2.1 KARTOVÉ CENTRUM PROID+

Kartové centrum ProID+ spolu s Card Management Systémem ProID+ (CMS ProID+) je hlavním manažerem karet a certifikátů v organizaci, může se také starat o potisk karet či tisk dalších dokumentů. Kartové centrum **ProID+** s CMS **ProID+** velmi zjednodušuje agendu potřebnou pro správu karet a certifikátů. Díky zjednodušení správy mohou být tyto nové kompetence uděleny mimo IT oddělení.

Kartové centrum ProID+ je aplikací pro centrální personalizaci a správu čipových karet. Je implementováno jako tlustý klient a bude instalováno na počítači či počítačích správců karet.

Kartové centrum ProID+ formou intuitivního grafického rozhraní podporuje řadu scénářů, každý scénář je určen pro jinou situaci v rámci životního cyklu karty (konkrétní scénáře, zvolené zadavatelem, jsou zmíněny v úvodu výše):

- **Vydání uživatelské karty a certifikátu.** Obsluha zvolí uživatele a pomocí kartového centra pro něj kompletně připravuje funkční kartu: vydává na kartu certifikát, formou průvodce provede budoucího držitele procesem změny bezpečnostních kódů PIN, QPIN a PUK, kdy si budoucí držitel tyto hodnoty změní na klávesnici počítače a vytiskne protokol o předání karty. Výsledkem procesu je kompletně připravená karta, kterou si pracovník přebere a ihned ji může začít používat. Součástí procesu nebude vydání certifikátů z CA PostSignum. Součástí procesu vydání karty jsou kontroly, např. zda daná karta náleží danému uživateli anebo zda jde o správný typ karty.
- **Vydání karty a certifikátu správce.** Obsluha zvolí uživatele a pomocí kartového centra pro něj kompletně připravuje funkční kartu s certifikátem Enrollment Agenta: vydává na kartu certifikát, formou průvodce provede budoucího držitele procesem změny bezpečnostních kódů PIN, QPIN a PUK, kdy si budoucí držitel tyto hodnoty změní na klávesnici počítače a vytiskne protokol o předání karty. Výsledkem procesu je kompletně připravená karta, kterou si nový správce karet přebere a ihned ji může začít používat. Součástí procesu nebude vydání certifikátů z CA PostSignum. Součástí procesu vydání karty jsou kontroly, např. zda daná karta náleží danému uživateli anebo zda jde o správný typ karty.
- **Vydání dočasné karty.** Obsluha zvolí uživatele a poté mu na dočasnou kartu vydá certifikát se zkrácenou dobou platnosti. Průvodce provede budoucího držitele procesem změny bezpečnostních kódů PIN, QPIN a PUK, kdy si budoucí držitel tyto hodnoty změní na klávesnici počítače. Scénář slouží pro řešení situace, kdy je třeba pracovníkovi operativně vydat kartu s certifikáty; např. při zapomenutí karty, ztráty karty či u nových zaměstnanců. Předpokládá se, že dočasná karta překlene období, než se pracovníkovi vydá trvalá karta.
- **Spárování používané karty s držitelem.** Scénář poskytující podobnou funkcionalitu, jako scénář Vydání uživatelské karty a certifikátu. Pro vydání je použita čipová karta, kterou má již uživatel v držení. V prostředí zákazníka se typicky bude jednat o karty, na kterých již jsou vydány certifikáty PostSignum.
- **Spárování používané karty se správcem**. Scénář poskytující podobnou funkcionalitu, jako scénář Vydání karty a certifikátu správce. Pro vydání je použita čipová karta, kterou má již uživatel v držení. V prostředí zákazníka se typicky bude jednat o karty, na kterých již jsou vydány certifikáty PostSignum.
- **Obnova doménových certifikátů na kartě.** Obsluha obnoví sadu certifikátů, uloženou na kartě jiného pracovníka. Držitel karty autorizuje operaci zadáním PIN (musí být přítomen operaci). Po obnově jsou z karty odstraněny nepotřebné certifikáty a klíče.
- **Recyklace karty.** Obsluha může recyklovat již nepotřebnou čipovou kartu. Formou průvodce z karty smaže všechny certifikáty a nastaví výchozí hodnoty bezpečnostních kódů PIN, QPIN a PUK. Operace se bude muset účastnit původní držitel karty. Bude nutné zadat PUK čipové karty. Takto připravenou čipovou kartu bude možné vydat novému držiteli.
- **Problémové stavy karty.** Scénáře určené k řešení jednotlivých problémových stavů spojených s čipovými kartami. Scénář zaeviduje změnu v držení čipové karty a odvolá všechny doménové certifikáty vydané na čipové kartě.

- Ztráta karty
- Odebrání karty
- Skartace karty

- **Import informací o nových kartách.** Informace o nově dodaných kartách se importují do centrální evidence. Jsou spárovány s evidovanými držiteli. Importované informace o bezkontaktním čipu mohou být propagovány do návazných (bezkontaktních) systémů.

Kartové centrum ProID+ provádí bezpečnostně citlivé operace. Informace o prováděných operacích jsou (pro zpětnou kontrolu) auditovány do žurnálu operačního systému.

Kartové centrum ProID+ komunikuje s

- CMS ProID+ (čtení a zápis informací o kartách, prostřednictvím webových služeb)
- Doménovou certifikační autoritou – vydávání a odvolávání certifikátů (prostřednictvím standardního DCOM rozhraní CA)
- Active Directory (informace o uživatelích a šablonách certifikátů)

Pro přístup k uvedeným subsystémům se využívá integrovaná doménová autentizace (SSO).

Při vydávání certifikátů je Kartové centrum ProID+ plně kompatibilní s doménovou MS CA Enterprise; přebírá její bezpečnostní koncept a technologii.

Kartové centrum ProID+ plně podporuje standardní archivaci šifrovacích klíčů, implementovanou v MS CA Enterprise (technologie Key Recovery Agent).

Kartové centrum ProID+ podporuje tzv. profily uživatelů. Součástí profilu je mj. seznam typů certifikátů, které mají být (naráz) vydány novému držiteli na kartu. Typy certifikátů jsou reprezentovány šablonami certifikátů, definovaných v AD a publikovaných v CA. Obsluha kartového centra volí z definovaných profilů – podle zvoleného profilu je na kartu vydána příslušná sada certifikátů.

Obrázek 1 *Ukázka Kartové centrum ProID+*

Oprávnění k použití Kartového centra

Pro použití aplikace Kartové centrum ProID+ se předpokládá využití integrované doménové autentizace, kdy Kartové centrum ProID+ akceptuje doménová pověření obsluhy.

Obsluha musí mít tato oprávnění

- Pro vydávání certifikátů musí být držitelem certifikátu typu enrollment agent
- Pro schvalování žádostí a odvolávání certifikátů musí mít vůči CA oprávnění Issue and Manage Certificates
- Pro čtení / zápis dat do CMS musí mít oprávnění správce karet CMS

Požadovaná oprávnění budou operátorům přidělena prostřednictvím členství v definované doménové skupině.

2.2 CARD MANAGEMENT SYSTEM PROID+

Pro evidenci a správu karet implementujeme Card Management System ProID+ (CMS ProID+). CMS ProID+ je základním modulem pro evidenci a podporu karet v organizaci. Mezi hlavní funkce CMS ProID+ patří

- evidence karet, používaných v rámci organizace;
- evidence držitelů karet a
- evidence dat na kartách (certifikáty, uživatelská data).

Evidence CMS **ProID+** dává komplexní a aktuální obraz o kartách, používaných v rámci organizace. Umožňuje provádět efektivní správu, včetně podpory a sledování životního cyklu karet.

Obrázek 2 *Ukázka aplikace CMS ProID+*

Data karty

CMS **ProID+** eviduje kompletní informace o kartách

- identifikátor karty (kontaktního čipu i bezkontaktního čipu),
- typ karty (hybridní,…),
- druh karty (uživatelská…),
- stav karty (nová, používaná, skartovaná,…),
- historii karty (datum zavedení do evidence, vydání uživateli, recyklace, …),
- držitele karty (aktuálního držitele i všechny předchozí držitele) a
- data na kartě (certifikáty a další data, včetně historie dat na kartě).

Integrace CMS ProID+ do domény MS Windows

Card Management System ProID+ je velmi těsně integrován do domény MS Windows

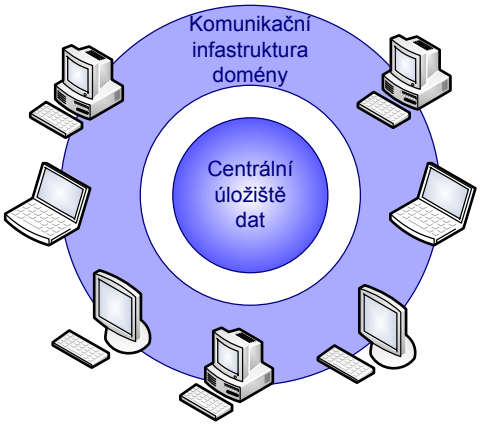
- CMS využívá doménová Active Directory jako zdroj informací o uživatelích / držitelích karet,
- CMS akceptuje nastavení doménových bezpečnostních politik,
- uživatelské role CMS jsou mapovány na doménové skupiny (domain groups),
- CMS definuje oprávnění na úrovni doménových skupin,
- CMS podporuje využití integrované autentizace domény MS Windows (Single Sign On).

Centrální úložiště dat CMS ProID+

Evidence CMS je striktně centralizovaná, veškerá data CMS jsou uložena v jedné MS SQL databázi.

Pro přístup do centrální evidence se využívá doménové infrastruktury

- K centrální evidenci lze přistupovat po síti. Využívá se sítových propojení, nad kterými běží i komunikační mechanismy domény.
- Při přístupu k datům se využívá integrovaná autentizace MS Windows. Doménoví uživatelé nemusí při přístupu k datům zadávat žádné autentizační údaje; je akceptováno doménové pověření uživatele.
- Přístupová oprávnění k jednotlivým typům dat jsou řízena na úrovni doménových skupin. Správa přístupových oprávnění je pak integrována do Active Directory, oprávnění jsou přidělována běžnými nástroji MS Windows, resp. automaticky Identity Management Systemem.



Obrázek 3 *Pozice úložiště dat CMS ProID+ v doméně*

Přístup k datům přes webové rozhraní

Běžní uživatelé ani operátoři nepřistupují přímo do centrální databáze CMS. S databází CMS komunikují prostřednictvím webového serveru CMS.

K prohlížení dat CMS nepotřebují mít na svém počítači instalován žádný specifický program, používají webový prohlížeč.

Díky tomu jsou data CMS dostupná z libovolného počítače v rámci domény: uživatel se může přihlásit k libovolnému počítači v doméně, spustit prohlížeč a vyhledat data.

Uživatel se při přístupu k webu CMS nemusí speciálně autentizovat. Web CMS akceptuje uživatelský účet (resp. pověření), jímž se uživatel přihlásil do domény (integrovaná autentizace, Single Sign On).

Uživatel může prohlížet a manipulovat pouze s daty, k nimž má přístupová oprávnění. Přístupová oprávnění jsou definována na úrovni doménových skupin. (Uživatel musí být členem příslušné doménové skupiny.)

CMS spolupracuje s dalšími podpůrnými programovými moduly technologie ProID+ (např. Kartové centrum, atd.). Tyto moduly čtou a zapisují data do centrální evidence CMS.

Podobně jako uživatelé, ani moduly ProID+ nepřistupují do centrální databáze přímo, nýbrž prostřednictvím webového serveru, resp. webových služeb (web services).

Podpora životního cyklu karet

CMS eviduje stavy jednotlivých karet např. nová, používaná, ztracená, skartovaná, atd.

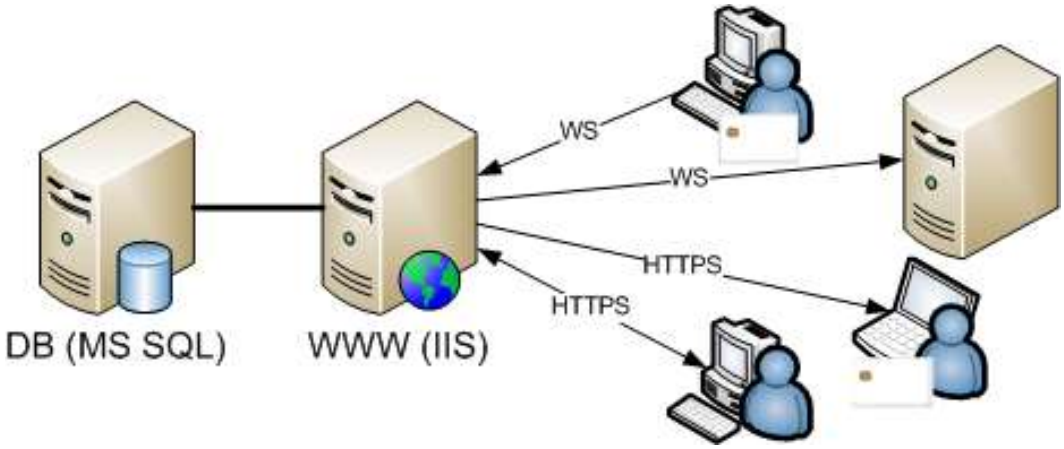
CMS také spolupracuje s dalšími moduly technologie ProID+, které pracují s čipovými kartami. Tyto moduly zasílají informace o provedených operacích do CMS. Změny stavů i informace o držitelích jsou tak automaticky promítány do centrální evidence. Díky tomu jsou údaje vždy aktuální. Centrální evidence poskytuje komplexní obraz nad daty a událostmi jednotlivých karet.

Úpravy životního cyklu karet se řeší v průběhu přípravy implementace CMS do interních systémů organizace.

Architektura CMS ProID+

Systém CMS tvoří dva základní stavební kameny

- MS SQL databáze, která obsahuje data o kartách.
- Webový server, jehož prostřednictvím mohou klienti číst a zapisovat data z/do centrální evidence.



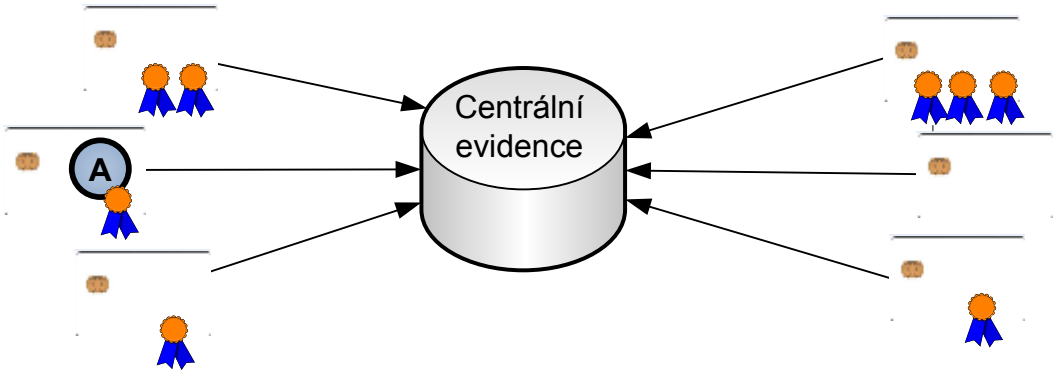
Obrázek 4 *Architektura CMS ProID+*

WWW server zprostředkovává přístup k centrální databázi karet

- uživatelům umožňuje nahlížet do centrální evidence prostřednictvím webových formulářů,
- správcům umožňuje pomocí webového prohlížeče modifikovat evidovaná data,
- modulům technologie ProID+ dává možnost zapisovat údaje přes webové služby (web services),
- externím systémům umožňuje čerpat informace o kartách prostřednictvím webových služeb.

Sledování dat na kartě

Data čipových karet jsou modifikována lokálně na počítači uživatele, příp. na počítačích správců (např. Kartové centrum). Pro organizaci (a pro správce) je výhodné sledovat datové změny na provozovaných čipových kartách a mít tak evidovaný kompletní datový obraz karet.



Obrázek 5 *Komunikace karet s centrální evidencí*

Centrální evidence dat na kartách přináší tyto výhody

- Správce systému má přehled nad kartami a elektronickými identitami uživatelů domény.
- Správce může snadno zjistit, zda uživatel má na své kartě elektronické identity, které tam má mít (zda mu nějaká nechybí a zda na kartě nemá identity, které by mít neměl).
- Správce může snadno zjistit, v jakém stavu jsou elektronické identity na kartě uživatele: zda jsou platné, jak dlouho ještě budou platné, atd.
- Informace lze využít např. při ztrátě karty: certifikáty uložené na kartě je třeba odvolat.
- Informace lze z evidence exportovat do návazných systémů.

Centrální evidenci dat na kartách realizuje modul Card Content Monitor (CCM):

- Klientský modul CCM je instalován na všechny klientské počítače. (Je integrován do obslužného software čipové karty, který je instalován na klientské počítače.) Klientský modul CCM monitoruje veškeré operace prováděné s čipovou kartou. Pokud jsou na kartě provedeny datové změny, klientský modul CCM je automaticky zapíše do centrální evidence.
- Centrální evidence dat obsahuje datové struktury pro evidenci dat na kartách.
- Webová služba CCM je instalována na webovém serveru CMS. Prostřednictvím webové služby odesílá klientský modul CCM do centrální evidence informace o datových změnách.

Je třeba zdůraznit, že systém CCM eviduje pouze veřejná data, jako jsou

- čísla karet,
- názvy kontejnerů na kartách,
- certifikáty (s veřejnými klíči),
- veřejné datové objekty.

Privátní klíče nelze z čipových karet přečíst, nejsou uvedeny v centrální evidenci. Předpokládá se však, že každý evidovaný kontejner obsahuje privátní klíč.

CCM také do evidence nezapisuje hodnoty PIN / PUK, případně QPIN.

Webové stránky CSM ProID+

Součástí implementace CMS je webový server. Hostuje webové stránky a prostřednictvím jich lze

- prohlížet data evidovaná v CMS,
- modifikovat (některá) data CMS a
- generovat reporty s informacemi o kartách.

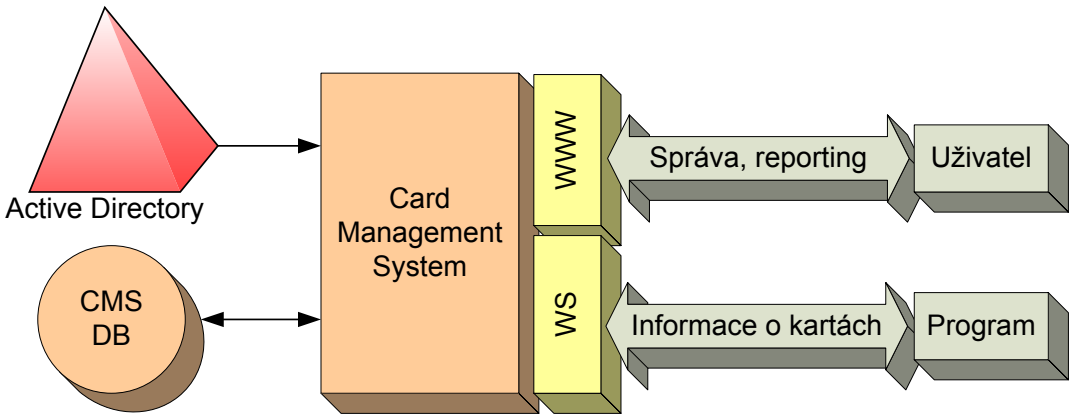
Navigace v datech CMS využívá běžných webových odkazů, menu a grafických symbolů. Ovládání webových stránek je intuitivní. Po krátkém zaškolení zvládne obsluhu stránek i méně zkušený uživatel.

Informace o uživatelích

CMS nevede vlastní evidenci uživatelů, čerpá data o uživatelích z Active Directory (AD). V databázi CMS je evidován pouze identifikátor (SID) uživatele AD. Veškeré další informace o uživatelích jsou v případě potřeby vyhledána v AD.

Správa uživatelů v systému je tak jednotná, není třeba řešit problematiku dvojí evidence a synchronizace dat. Změní-li se v AD informace o uživateli (např. jméno, příjmení, …) jsou tyto změny automaticky propagovány i do formulářů CMS.

Pro vyhledání informací o uživatelích musí mít webový server CMS přístup (pro čtení) do AD.



Obrázek 6 *Zdroj dat o uživatelích*

Předpokládá se, že všichni uživatelé CMS (správcové karet i držitelé karet) jsou doménovými uživateli.

2.3 ACEX

Aplikace pro automatizovanou obnovu certifikátů (ACEx) spolu s čipovou kartou nabízí maximální pohodlí při práci s kartou a úsporu nákladů. Pomocí aplikace ACEx si mohou uživatelé obnovit jakékoli certifikáty vydané na čipové kartě ProID+ či ProID+Q přímo z pohodlí svého počítače bez nutnosti návštěvy administrátora. Aplikace ACEx dokáže obnovit jak certifikáty vydané z doménové certifikační autority, tak certifikáty z akreditovaných certifikačních autorit PostSignum či eIdentity.

ACEx je aplikace pro automatizovanou obnovu certifikátů. Pomáhá uživatelům s procesem vydání nového certifikátu bez nutnosti navštívení výdejního místa. Celá obnova je provedena z jeho pracovního počítače. ACEx podporuje obnovu doménových i akreditovaných certifikátů.

Obnova certifikátu na čipovou kartu může být pro méně zkušeného uživatele komplikovaný proces. Proto je na počítače uživatelů instalována aplikace ACEx (Authentication Certificate Exchange), která

- pravidelně kontroluje certifikáty na kartě a v případě potřeby automaticky vyzve uživatele k obnově certifikátů.
- provádí uživatele celým procesem vydání nového certifikátu.

Obrázek 7 *Ukázka aplikace ACEx*

Úkolem ACEx je především

- Kontrolovat obsah karty a rozhodnout, kdy je třeba obnovit na kartě certifikát.
- Postarat se o úspěšnou obnovu certifikátu na kartě.

ACEx je tedy jednoduchý grafický průvodce procesem obnovy certifikátu. Po úspěšném dokončení práce aplikace ACEx by uživatel měl mít na kartě obnovené certifikáty, použitelné v dalším období v rámci budovaného prostředí.

Jedním z úkolů aplikace ACEx je: pravidelně kontrolovat obsah karty, resp. blížící se konec platnosti certifikátu. Pro zajištění pravidelné kontroly je ACEx spouštěn vždy po přihlášení uživatele. Uživatel spuštění aplikace ACEx nezaznamená: aplikace funguje na pozadí, bez grafického rozhraní. Pouze v případě potřeby provést obnovu certifikátu zobrazí okno s výzvou k započetí procesu.

Aplikace ACEx žurnáluje svoji činnost pro usnadnění detekce a řešení případných chybových stavů. Žurnál je vytvářen během analýzy karet i během vydávání certifikátu.

2.4 SLUŽBY

2.4.1 Dokumentace - návrh životního cyklu karet v organizaci

Před implementací karet a aplikací bude vypracován dokument s návrhem životního cyklu karet v organizaci. V rámci dokumentu jsou řešena obvykle tato témata:

- Role uživatelů pro správu a použití karet
- Způsob distribuce karet uživatelům
- Vydání a obnova certifikátů na kartách
- Způsob aplikačního využití karet (operace, využívaná aplikační rozhraní)
- Podporované stavy karet a jejich vlastnosti
- Řešení nestandardních stavů karet (zapomenutí, ztráta, zničení, …)
- Aplikační scénáře (podklady pro konfiguraci dodávaných aplikací)
- Návrh tiskových protokolů

Postup Zpracování návrhu životního cyklu se předpokládá následujícím způsobem

- Úvodní schůzka se zákazníkem
  - » Prezentace nabízeného řešení a diskuze nad možnostmi konfigurace dle potřeb organizace
  - » Na schůzce dojde k dohodě nad obsahem a nasazením požadovaného řešení do organizace
- Zpracování draftu dokumentu životního cyklu
  - » Organizace prostudují a okomentují dodaný návrh řešení
- Finalizace dokumentu s návrhem životního cyklu
  - » V průběhu finalizace budou pracovníci organizace vznášet připomínky k návrhu
  - » Výstup (akceptovaný dokument) bude sloužit pro následnou implementaci a konfiguraci karet a aplikací

2.4.2 Aktivace doménové certifikační autority

Nejsnazší cestou k certifikátům v doméně je aktivace doménové certifikační služby a vydávání certifikátů z takto vytvořené doménové certifikační autority (dále jen „CA“). Takto získané certifikáty jsou pro organizaci zdarma. Tyto certifikáty ale nelze použít pro kvalifikovaný elektronický podpis.

MONET+ tímto způsobem vytvořil doménový PKI systém v řadě projektů. CA na platformě MS Windows Server nabízí značnou variabilitu budovaného řešení. Malé organizace většinou (z ekonomických důvodů) preferují elementarizované řešení:

- Certifikační autorita v módu enterprise (=vydávající CA)
- Klíč CA chráněn v operačním systému
- CRL publikován do intranetu přes Active Directory a přes WWW server, hostovaný na CA
- Základní sada šablon certifikátů (Domain Controller, WWW server, Enrollment Agent, Smartcard User)
- Zálohování CA pravidelně spouštěným skriptem
- Nejsou dodávány certifikační politiky ani certifikační prováděcí směrnice

Toto řešení bude využito také u zadavatele.

Větší organizace – anebo organizace, které důsledně dbají na bezpečnosti a kontinuitě systémů – mohou požadovat komplexní implementaci doménového PKI, se specifickými požadavky, např.:

- Specifická dokumentace pro správu a provoz CA, spolu s havarijními plány CA.
- Návrh bezpečnostního konceptu, integrace do bezpečnostních politik organizace.
- Hierarchii CA.
- Ochrana klíčů CA v HSM.
- Dodávka certifikačních politik a/nebo certifikačních prováděcích směrnic.
- Přihlášení do wifi.

Tyto specifické požadavky řeší MONET+ projektově, na vyžádání, nejsou tedy předmětem této dodávky. Nejčastěji je požadováno zpracovat specifickou dokumentaci (1.odrážka výše) a to i u středních či menších organizací, kdy základní rozsah této dokumentace představuje náklad 67 tis. Kč bez DPH, čas na její zpracování je okolo 4 týdnů, dle aktuálních kapacit předkladatele, plus nutný čas na připomínky a akceptaci zadavatelem.

2.4.3 Implementace

V závislosti na rozsahu zvolené dodávky je MONET+ připraven provést všechny služby spojené s úspěšnou implementací dodávky a provedení zaškolení kompetentních pracovníků.

Podkladem pro implementaci a konfiguraci aplikací bude:

- Dokument s návrhem životního cyklu
- Dokument s návrhem PKI

Po dokončení implementace budou funkční všechny aplikace a procesy, spojené se správou karet a životním cyklem certifikátů. Součástí implementace je ověření fungování karet, certifikátů a nainstalovaných aplikací:

- Autentizace do domény
- Podepsání dat

2.4.4 Školení

Součástí dodávky je také školení správců karet obsluhujících dodané aplikace. Obvyklý rozsah je v průběhu do jednoho pracovního dne, v prostředí zadavatele, v předem dohodnutém termínu.

V rámci školení bude prezentována kompletní funkčnost systému a všech instalovaných aplikací.

2.4.5 Akceptační podmínky

Dodané řešení bude akceptováno na základě ověření fungování v produkčním prostředí, vč. akceptace dokumentace. Akceptace jako taková bude osvědčena podpisem předávacího protokolu.