

KUPNÍ SMLOUVA

č. 1802235118

uzavřená níže uvedeného dne, měsíce a roku mezi smluvními stranami:

Smluvní strany

1. Kupující: Město Třebíč
Se sídlem: Karlovo nám. 104/55
Zastoupen: Ing. Pavlem Janatou - starostou
IČO: 00290629
DIČ: CZ00290629
Bankovní spojení: KB Třebíč
Číslo účtu: 329711/0100
Osoba oprávněná jednat ve věcech technických:
Ing. Pavel Kaláb, tel.: 725 976 867, e-mail: pavel.kalab@trebic.cz
Bc. Petr Blaise, DiS., tel.: 724 701 976, e-mail: petr.blaise@trebic.cz

(dále jen „kupující“)

2. Prodávající: MONET+, a.s.
Se sídlem: Za Dvorem 505, 763 14 Zlín - Štípa
Zastoupen: Ing. Břetislavem Endrysem – předsedou představenstva
Mgr. Jiřím Benešem - prokuristou
IČO: 26217783
DIČ: CZ26217783
Zapsána v obchodním rejstříku vedeném Krajským soudem v Brně sp. zn. B 3351
Bankovní spojení: KB Zlín
Číslo účtu: 1547260257/0100
Osoba oprávněná jednat ve věcech technických:
Bc. David Říhošek, tel.: 731 191 721, drihosek@monetplus.cz

(dále jen „prodávající“)

(společně také jen „smluvní strany“)

Článek I. Předmět plnění

1. Prodávající se zavazuje že, za podmínek této smlouvy ve lhůtě a v místě plnění, dle pokynů kupujícího dodá 280 ks multifunkčních čipových karet ProID+Q MAV4/EM4102 v požadovaném designu a 280 ks adekvátních čteček čipových karet Gemalto IDBridge CT30 (dále jen „zboží“), tiskárnu karet se spotřebním materiálem, SW centrální evidence + 1 licence kartového centra, návrh životního cyklu karet a certifikátů a doménové certifikační autority + havarijní a provozní dokumentace certifikační autority dle přílohy č. 1 této smlouvy a dále:
 - a) zaškolí určené zaměstnance,
 - b) převede na kupujícího vlastnické právo ke zboží,
 - c) provede implementaci a konfiguraci SW,
 - d) zajistí základní servis nabízeného řešení, který zahrnuje podporu od podpisu předávacího protokolu po dobu jednoho roku.
2. Kupující se zavazuje řádně a včas dodaný předmět plnění převzít a zaplatit za něj sjednanou kupní cenu.

Článek II. Zboží

1. Prodávající je povinen dodat kupujícímu zboží v množství, druhu, kvalitě a technické specifikaci, jak bylo sjednáno v této smlouvě.
2. Zboží musí splňovat veškeré požadavky stanovené příslušnými právními předpisy, musí být vybaveno veškerými atesty, prohlášeními o shodě a certifikáty nutnými k jeho nerušenému a bezpečnému užívání.
3. Prodávající je povinen společně se zbožím kupujícímu předat veškerou dokumentaci, zejména návod k použití zboží (uživatelský manuál obsahující i zjednodušený postup při poškození nebo poruše zboží), zápis o provedeném zaškolení obsluhy, výkresovou dokumentaci a další doklady související se zbožím, vše v českém jazyce a potvrzení o záruce.
4. Prodávající musí umožnit kupujícímu prohlídku dodaného zboží a ověření funkčnosti zboží.
5. Po ověření funkčnosti zboží, provedení implementace a konfigurace bez vad a nedodělků a kontrole dokladů souvisejících se zbožím obě smluvní strany podepíší předávací protokol, přičemž okamžikem podpisu předávacího protokolu se předmět plnění považuje za řádně předaný prodávajícím a převzatý kupujícím.
6. Kupující není povinen převzít předmět plnění, který trpí jakýmkoliv vadami, zejména nesplňuje-li některý z požadavků na zboží dle této smlouvy nebo nebyla-li dodána úplná dokumentace ke zboží dle odst. 2 a 3 tohoto článku nebo v případě výskytu vad souvisejících s implementací a konfigurací zboží.
7. V případě, že kupující odmítne převzít předmět plnění z kteréhokoliv důvodu uvedeného v odst. 6 tohoto článku smlouvy, je prodávající povinen dodat kupujícímu bezvadné a plně funkční zboží, splňující veškeré vlastnosti specifikované v této smlouvě, a to v dodatečné lhůtě 15 dnů ode dne, kdy kupující odmítl zboží převzít. Za dodání bezvadného a plně funkčního zboží se považuje i provedení implementace a konfigurace zboží bez vad a nedodělků.
8. Prodávající odpovídá za škodu, kterou způsobí sám nebo prostřednictvím svých poddodavatelů kupujícímu nebo třetím osobám při plnění předmětu této smlouvy nebo v souvislosti s ním.

Článek III.

Termín a místo plnění

1. Prodávající je povinen kupujícímu zboží dodat, provést implementaci a konfiguraci dodaného zboží v sídle kupujícího, za podmínek této smlouvy ve 2 fázích.
 - 1. fáze do 15. 12. 2018 - 280ks karet, 280 ks čteček, tiskárna karet se spotřebním materiálem), SW centrální evidence + 1 licence kartového centra, započít práce na návrhu životního cyklu karet a certifikátů a na doménové certifikační autoritě,
 - 2. fáze do 30. 05. 2019 - Návrh životního cyklu karet a certifikátů, Implementace, školení, vybudování doménové certifikační autority + havarijní a provozní dokumentace certifikační autority

Článek IV.

Přechod práv ke zboží

1. Vlastnické právo ke zboží přechází na kupujícího okamžikem připsání kupní ceny, sjednané v čl. V této smlouvy, na účet prodávajícího. Nebezpečí škody na zboží přechází na kupujícího okamžikem podpisu předávacího protokolu v souladu s čl. II odst. 5 této smlouvy.

Článek V.

Kupní cena způsob její úhrady

1. Smluvní strany sjednávají kupní cenu a cenu za servisní podporu za předmět plnění takto:

a) Kupní cena

Zboží	718 300 Kč
DPH 21 %	150 843 Kč
Cena za předmět plnění celkem:	869 143 Kč

Ceny jsou bez servisní podpory 1. a 2. fáze.

Celková částka bude rozložena do dvou fakturačních období. První fáze bude fakturována k datu 15. 12. 2018 na základě dodaného zboží a provedených prací, dle nabídky, jenž je přílohou této smlouvy. Druhá fáze bude fakturována po dokončení implementace. Před každou vystavenou fakturou bude vystaven předávací protokol, v němž obě strany odsouhlasí dodaný materiál a provedené práce. Součet těchto dílčích faktur nesmí přesáhnout celkovou cenu za dílo.

- b) Cena za servisní podporu, specifikovanou v Článku I. bod d), je 3 980 Kč bez DPH za měsíc. Servisní podpora se začíná platit ode dne podepsání předávacího protokolu o úspěšné implementaci po dobu jednoho roku s 2měsíční výpovědní lhůtou. Servisní podpora bude fakturována měsíčně, vždy za uplynulý kalendářní měsíc zpětně.

Dnem zdanitelného plnění je vždy poslední kalendářní den měsíce, ve kterém byly služby poskytnuty

2. Sjednanou kupní cenou se rozumí cena zboží včetně veškerých nákladů prodávajícího spojených s dodávkou zboží, jeho implementací a konfigurací a provedením veškerých zkoušek funkčnosti v místě plnění.
3. Cena za předmět plnění bez DPH uvedená v odst. 1 tohoto článku je cenou nejvýše přípustnou a nelze ji překročit. Nebezpečí změny okolností přebírá prodávající.

Článek VI.

Platební podmínky

1. Zálohy na platby nejsou sjednány.
2. Podkladem pro úhradu kupní ceny a ceny za servisní podporu bude faktura, která bude mít náležitosti daňového dokladu dle zákona o DPH a náležitosti stanovené dalšími obecně závaznými právními předpisy (dále jen „faktura“). Kromě náležitostí stanovených platnými právními předpisy pro daňový doklad bude prodávající povinen ve faktuře uvést i tyto údaje:
 - a) předmět koupě včetně uvedení místa plnění (pouze při plnění podle článku 5.1.a),
 - b) označení banky a číslo účtu, na který musí být zaplacen (pokud je číslo účtu odlišné od čísla uvedeného v této smlouvě, je prodávající povinen o této skutečnosti bez zbytečného odkladu informovat kupujícího),
 - c) lhůtu splatnosti faktury,
 - d) označení osoby, která fakturu vyhotovila, vč. jejího podpisu a kontaktního telefonu,
 - e) přílohou vystavené faktury bude předávací protokol (čl.II. odst.5 této smlouvy), (pouze při plnění podle článku 5.1.a).
3. Kupující, příjemce plnění, prohlašuje, že plnění, které je předmětem smlouvy, nepoužije pro svou ekonomickou činnost, ale výlučně pro účely související s jeho činností při výkonu veřejné správy, při níž se nepovažuje za osobu povinnou k dani (viz § 5 odst. 3 zákona o DPH). Z uvedeného důvodu se na toto plnění nevztahuje režim přenesení daňové povinnosti dle § 92e uvedeného zákona a prodávajícím bude vystavena faktura za předmětné plnění včetně daně z přidané hodnoty.
4. Kupující uplatní institut zvláštního způsobu zajištění daně dle § 109 a zákona o DPH a hodnotu plnění odpovídající dani z přidané hodnoty uvedené na faktuře uhradí v termínu splatnosti této faktury stanoveném dle smlouvy přímo na osobní depozitní účet prodávajícího vedený u místně příslušného správce daně v případě, že:
 - prodávající bude ke dni uskutečnění zdanitelného plnění zveřejněn v aplikaci „Registr plátců DPH“ jako nespolehlivý plátcce, nebo
 - prodávající bude ke dni uskutečnění zdanitelného plnění v insolvenčním řízení, nebo
 - bankovní účet prodávajícího určený k úhradě plnění uvedený na faktuře nebude správcem daně zveřejněn v aplikaci „Registr plátců DPH“.
5. Lhůta splatnosti faktury je dohodou stanovena na 20 kalendářních dnů ode dne jejího doručení kupujícímu.
6. Doručení faktury se provede osobně na podatelnu kupujícího, doručenkou prostřednictvím provozovatele poštovních služeb nebo elektronicky na e-mailovou adresu, kterou zadavatel poskytne na zasílání elektronických faktur.
7. Kupující je oprávněn vadnou fakturu před uplynutím lhůty splatnosti vrátit druhé smluvní straně bez zaplacení k provedení opravy v těchto případech:
 - nebude-li faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude-li chybně vyúčtována kupní cena,
 - bude-li DPH vyúčtována v nesprávné výši,
 - bude-li fakturováno plnění, které fakticky nebylo provedeno nebo dodáno.

Ve vrácené faktuře kupující vyznačí důvod vrácení. Proávající provede opravu vystavením nové faktury. Vráť-li kupující vadnou fakturu prodávajícímu, přestává běžet původní lhůta splatnosti.

Celá lhůta splatnosti běží opět ode dne doručení nově vyhotovené faktury kupujícímu. Prodávající je povinen doručit kupujícímu opravenou fakturu do 3 pracovních dnů po obdržení kupujícím vrácené vadné faktury.

8. Povinnost zaplatit kupní cenu je splněna dnem odepsání příslušné částky z účtu kupujícího.

Článek VII.

Záruční doba, reklamace a servis

1. Prodávající podpisem předávacího protokolu poskytuje kupujícímu záruku za to, že předmět plnění nebude trpět žádnými vadami, ať už se jedná o vady materiálu, výrobní vady nebo vady zjevné či skryté nebo o vady právní či faktické, a že předmět plnění bude plně odpovídat jeho specifikaci a vlastnostem dle této smlouvy a dle platných právních předpisů.

2. Záruka se nevztahuje na vady zboží vzniklé:

- a) poškozením zboží třetí osobou,
- b) užíváním zboží kupujícím v rozporu s návodem k použití.

Záruka se dále nevztahuje na software implementovaný ve zboží a software se zbožím související.

3. Prodávající poskytuje kupujícímu záruku na předmět plnění v rozsahu tohoto článku smlouvy v délce 24 měsíců na čtečky a v délce 12 měsíců na karty

Záruční doba počíná běžet dnem následujícím po dni předání a převzetí zboží v souladu s čl. II. odst. 5 této smlouvy. V případě oznámení vady zboží kupujícím se běh záruční doby staví a počíná znovu běžet ode dne převzetí opraveného reklamovaného zboží kupujícím.

4. Kupující je povinen oznámit prodávajícímu vadu předmětu plnění, která se vyskytla v průběhu záruční doby, bez zbytečného odkladu poté, kdy kupující vadu zjistil. Kupující vytkne vadu předmětu plnění prodávajícímu nejprve telefonicky. Jestliže prodávající nebude na určeném telefonním čísle kontaktní nebo nebude na telefonické vytknutí vady nijak reagovat, kupující zašle oznámení o vadě předmětu plnění prodávajícímu prostřednictvím e-mailu nebo písemně prostřednictvím držitele poštovní licence na dodejku na adresu sídla prodávajícího.

5. Prodávající je povinen odstranit podstatnou vadu předmětu plnění, která brání jeho užívání do 24 hodin od vytknutí vady kupujícím. V případě výskytu jiných vad předmětu plnění je prodávající povinen tyto vady odstranit nejpozději do 10 pracovních dnů ode dne jejich vytknutí kupujícím. Jestliže bude vytknutá vada předmětu plnění neopravitelná, kupující je oprávněn požadovat výměnu vadného předmětu plnění za bezvadný nebo slevu z kupní ceny nebo odstoupit od této smlouvy, a to podle svého výběru.

6. Jestliže prodávající neodstraní vytknutou vadu předmětu plnění ve lhůtě uvedené v odst. 5 tohoto článku, má kupující právo pověřit odstraněním vady třetí osobu nebo odstoupit od smlouvy, ledaže by se smluvní strany dohodly na jiném způsobu řešení reklamace. Tím není dotčeno právo kupujícího na smluvní pokutu.

7. V případě, že prodávající písemně oznámí kupujícímu, že jím vytknutou vadu nepovažuje za záruční vadu, je kupující oprávněn zajistit posouzení vady znalcem na základě znaleckého posudku.

Jestliže bude znaleckým posudkem zjištěno, že se jedná o záruční vadu, ponese náklady na jeho vyhotovení prodávající, který současně nejpozději do tří dnů zahájí odstraňování vady.

Nebude-li se, podle znaleckého posudku, jednat o záruční vadu, ponese náklady na jeho vyhotovení kupující.

8. Prodávající se zavazuje po dobu jednoho roku od podpisu předávacího protokolu poskytovat kupujícímu servisní podporu:
- operačních systémů na klientských stanicích Windows 7 až Windows 10
 - serverových operačních systémů Windows Server 2008 R2 a vyšších
 - čipových karet do konce životnosti
 - čteček pro práci s kartou, které splňují standard PC/SC
 - instalovaných aplikací pro správu životního cyklu karet a certifikátů
 - formou Service Desku v režimu 5 x 8, jehož provozní doba musí být min. od 8:00 do 16:00 v pracovní dny.

Reakční doby:

- Přijetí požadavku do 2 hodin od nahlášení.
- Dočasné řešení do 1 pracovního dne od přijetí požadavku.
- Vyřešení požadavku do 3 pracovních dnů od dodání dočasného řešení.
- Reakční doby musí být garantovány pro serverové komponenty řešení.

Článek VIII. Povinnosti prodávajícího

1. Prodávající je povinen:
- a) informovat kupujícího o skutečnostech majících vliv na plnění smlouvy, a to bez zbytečného odkladu, nejpozději následující pracovní den poté, kdy příslušná skutečnost nastala nebo prodávající zjistí, že by nastat mohla;
 - b) zachovávat mlčenlivost o všech skutečnostech, které se v souvislosti s plněním předmětu této smlouvy dozvěděl nebo které byly smluvními stranami označeny za důvěrné.

Článek IX. Sankční ujednání

1. Kupující má právo na zaplacení smluvní pokuty ve výši 0,05 % z ceny za předmět plnění bez DPH za každý i započatý den prodlení v případě, že prodávající nedodá předmět plnění včas, nebo od této smlouvy odstoupit.
2. Pro případ prodlení se zaplacením ceny za předmět plnění sjednávají smluvní strany smluvní úrok z prodlení ve výši 0,05 % z dlužné částky bez DPH za každý den prodlení.
3. V případě nedodržení stanoveného termínu k odstranění vady reklamované v záruční době je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 2.000 Kč za každou reklamovanou vadu, a za každý den prodlení.
4. V případě, že závazek dodat předmět plnění zanikne před jeho řádným dodáním, nezaniká nárok na smluvní pokutu, pokud vznikl dřívějším porušením povinnosti. Zánik závazku pozdním splněním neznamena zánik nároku na smluvní pokutu za prodlení s plněním.
5. Sjednané smluvní pokuty zaplatí povinná strana nezávisle na zavinění a na tom, zda a v jaké výši vznikne druhé straně škoda.
6. Smluvní strany se dohodly, že zaplacením smluvní pokuty a úroků z prodlení není dotčeno právo na náhradu škody, ustanovení § 2050 občanského zákoníku se nepoužije. Rovněž není dotčena povinnost řádně splnit závazky vyplývající z této smlouvy.

7. Smluvní strany se dohodly, že vyúčtovaná smluvní pokuta může být jednostranně započtena vůči ceně předmětu plnění, kterou je kupující povinen uhradit.

Článek X. Odstoupení od smlouvy

1. Smluvní strany jsou oprávněny odstoupit od této smlouvy zejména v případě, že:
 - a) podstatným způsobem poruší smluvní povinnost specifikovanou níže nebo
 - b) prodávající bude v úpadku nebo s ním bude zahájeno insolvenční řízení nebo bude v likvidaci.
2. Smluvní strany se dohodly, že za podstatné porušení smluvních podmínek považují:
 - a) Prodlení kupujícího s úhradou ceny předmětu plnění, která nebude uhrazena ani do dvou měsíců ode dne písemného vytčení prodlení prodávajícím kupujícímu.
 - b) Prodlení prodávajícího s plněním předmětu této smlouvy v termínu sjednaném v této smlouvě, pokud se smluvní strany nedohodnou jinak.
 - c) Prodlení prodávajícího s odstraněním reklamované vady dle čl. VII. této smlouvy.
 - d) Opakovaný výskyt vad předmětu plnění (nejméně trojí vyskytnutí vady, přičemž se nemusí jednat o jednu a tutéž vadu).
3. Odstoupení od smlouvy je platné a účinné dnem jeho doručení druhé smluvní straně v souladu s touto smlouvou. Odstoupením od smlouvy nezaniká nárok na náhradu škody nebo bezdůvodné obohacení.
4. Pro případ odstoupení od smlouvy z důvodu uvedeného v odst. 2 písm. a) tohoto článku, je prodávající oprávněn odvézt zboží z místa plnění na náklady kupujícího.
5. Pro případ odstoupení od smlouvy z důvodu uvedeného v odst. 2 písm. b) tohoto článku, se tato smlouva ruší od počátku, pokud nemá částečné plnění samo o sobě pro kupujícího hospodářský význam.
6. Pro případ odstoupení od smlouvy z důvodu uvedeného v odst. 2 písm. c) a d) tohoto článku, se tato smlouva ruší s účinky do budoucna.
7. Pro případ odstoupení od smlouvy, smluvní strany výslovně ujednaly, že v tomto případě kupující uhradí prodávajícímu peněžitou částku ve výši odpovídající hodnotě plnění předmětu této smlouvy do odstoupení od smlouvy, tj. to, o co se kupující obohatil, a to pouze za podmínky, že předmět plnění nebo jeho část do odstoupení od smlouvy byl plněn řádně a za podmínek této smlouvy a má pro kupujícího hospodářský význam.

Článek XI. Součástí Smlouvy

1. Následující přílohy tvoří nedílnou součást smlouvy:

Příloha č. 1 – Obchodní nabídka

Příloha č. 2 – Harmonogram implementačních prací

Článek XII. Závěrečná ustanovení

1. Změnit nebo doplnit smlouvu mohou smluvní strany pouze formou písemných dodatků, které budou vzestupně číslovány, výslovně prohlášeny za dodatek této smlouvy a podepsány oprávněnými zástupci smluvních stran.
2. Smlouva nabývá platnosti dnem podpisu druhé smluvní strany a účinnosti dnem jejího zveřejnění v registru smluv v souladu se zákonem č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů. Smluvní strany se dohodly, že tuto smlouvu zveřejní v registru smluv kupující po podpisu smlouvy oběma smluvními stranami.
3. Smlouva je vyhotovena ve dvou stejnopisech s platností originálu podepsaných oprávněnými zástupci smluvních stran, přičemž kupující a prodávající obdrží jedno vyhotovení.
4. Smluvní strany se dohodly, že veškerá komunikace související s plněním předmětu této smlouvy bude probíhat prostřednictvím e-mailu oprávněných osob, přičemž se e-mailová zpráva považuje za doručenou tehdy, potvrdí-li oprávněná osoba druhé smluvní strany její doručení; telefonicky na čísla osob oprávněných jednat ve věcech technických; osobním předáním, prostřednictvím držitele poštovní licence na adresu sídla smluvní strany. Pro případ doručování prostřednictvím pošty si smluvní strany sjednávají, že zásilka je druhé smluvní straně doručena pátým dnem ode dne jejího odeslání první smluvní stranou, pokud se smluvní strany nedohodnou jinak.
5. Práva a povinnosti smluvních stran neupravené v této smlouvě se řídí příslušnými ustanoveními občanského zákoníku.
6. Smluvní strany prohlašují, že skutečnosti uvedené v této smlouvě nepovažují za obchodní tajemství ve smyslu § 504 občanského zákoníku, a udělují svolení k jejich užití a zveřejnění bez stanovení jakýchkoliv dalších podmínek.
7. Smluvní strany shodně prohlašují, že si smlouvu před jejím podpisem přečetly a že byla uzavřena po vzájemném projednání podle jejich pravé a svobodné vůle určitě, vážně a srozumitelně, nikoliv v tísní nebo za nápadně nevýhodných podmínek, a že se dohodly o celém jejím obsahu, což stvrzují svými podpisy.
8. Uzavření Smlouvy rozhodla za Objednatele rada města Třebíče svým usnesením č. 69/19/RM/2018 ze dne 9. 8. 2018

V Třebíči dne

Ve Zlíně dne

Za kupujícího:

Ing. Pavel Janata
Starosta města Třebíče

Za prodávajícího:

Ing. Břetislav Endrys
Předseda představenstva

Za prodávajícího:

Mgr. Jiří Beneš
Prokurista

PŘÍLOHA Č. 1 KE SMLouvě Č. 1802235118

OBCHODNÍ NABÍDKA JEDNA KARTA NA VŠECHNO

PRO SPOLEČNOST	Městský úřad Třebíč (dále jen „Třebíč“)
PŘEDKLÁDÁ	MONET+, a.s. (dále jen „Monet+“)

Tento dokument zůstává vlastnictvím MONET+, a.s. Duplikace a/nebo předání kterékoli části tohoto dokumentu třetí straně není povoleno bez předchozího písemného souhlasu autorů. Autoři dokumentu souhlasí s použitím informací uvedených v tomto dokumentu pro účely uvedené v titulu dokumentu.

1 OBSAH

1	Obsah	2
2	Manažerské shrnutí.....	3
3	Řešení ProID+	4
4	Služby a Komponenty ProID+	6
4.1	Návrh životního cyklu karet	6
4.1.1	Postup zpracování návrhu životního cyklu	6
4.2	Doménová certifikační autorita	6
4.3	Čipové karty ProID+ Q	7
4.3.1	Formát ID-1	7
4.4	Čtečky čipových karet.....	8
4.5	Manažer ProID+	9
4.5.1	Kartové centrum ProID+	9
4.5.2	Card Management System (CMS) ProID+	11
4.6	ACEx.....	15
4.7	Potisk čipových karet	16
4.8	Implementace aplikací pro správu karet a školení.....	16
4.9	Servisní podpora.....	16
5	Cenová nabídka.....	18

2 MANAŽERSKÉ SHRUTÍ

Třebíč zvažuje zavedení multifunkčních čipových karet. Čipová karta přinese zaměstnancům města několik výhod:

- ▶ Získají prostředek pro uložení certifikátu pro kvalifikovaný elektronický podpis podle nařízení Evropské unie č. 910/2014 eIDAS. Nařízení eIDAS prostřednictvím české legislativy vyžaduje přechod na samosprávy právě na takový podpis.
- ▶ Začnou používat dvoufaktorovou autentizaci do pracovních počítačů. Silná autentizace splňuje kritéria zákona o kybernetické bezpečnosti v oblasti autentizace a zajišťuje ochranu osobních údajů související s nařízením Evropské unie GDPR.
- ▶ Do těla karty je integrován bezkontaktní čip pro použití v bezkontaktních systémech – docházkový systém, tiskové řešení, fyzické přístupy, atd. Zaměstnanec tak pro pohyb po budovách úřadu použije jeden prostředek.
- ▶ Po vytažení karty ze čtečky, dojde k automatickému uzamčení pracovní stanice. Uživatelská data jsou tak zabezpečena a jsou nepřístupná pro další osoby.

Čipové karty jsou součástí řešení ProID+. ProID+ je komplexní PKI řešení s podporou čipových karet.

Monet+ nabízí bezpečnostní předměty, které podporují práci s certifikáty z doménové i akreditované certifikační autority PostSignum. Zároveň dodává službu aktivace doménové certifikační autority a spolupracuje s akreditovanými poskytovateli certifikačních služeb, kteří se zaměřují na výdej certifikátů pro kvalifikovaný elektronický podpis.

Výhodou čipových karet od Monet+ je jejich bezpečnost splňující nejprísnější kritéria a **certifikace**, které jsou vyžadovány aktuální legislativou a to nejen evropským nařízením eIDAS. Karty podporují **automatizované obnovy certifikátů**. Automatizovanou obnovu certifikátů využije každý držitel karty a obnoví si svůj certifikát pohodlně ze svého počítače bez nutnosti návštěvy registračního místa opakovaně každý rok.

Každá operace s privátním klíčem uloženým na kartě je chráněna zadáním PINu. Funguje to podobně jako u bankomatu nebo při platbě kartou na platebním terminálu, kde je držitel z důvodu bezpečnosti vyzván k prokázání znalosti PINu ke kartě. Právě tomu se říká 2-faktorová bezpečnost.

Silná autentizace je bezpochyby trendem, který přichází a je to zejména z důvodu naplnění evropské směrnice GDPR, která klade důraz na práci s osobními údaji pacientů a zaměřuje se na přístup k nim a jejich ochranu.

Desítky karet a certifikátů z různých autorit je třeba v organizaci spolehlivě řídit. Na organizaci to klade nové nároky. Monet+ má všechny karetní procesy zvládnuté a dokáže nutné postupy značně trivializovat. Snadnost použití vede k tomu, že všechny základní úkony mohou být předány mimo IT oddělení. Veškeré funkce jsou reprezentovány Manažerem ProID+. Manažer ProID+ je soubor aplikací, které nabízejí komplexní správu karet a certifikátů.

Monet+ je specialistou na dodávku PKI řešení na bázi čipových karet. Za dobu své působnosti implementoval řadu úspěšných projektů. Naše systémy kladou důraz na jednoduché ovládání a správu. Maximalizace automatizace nových procesů s kartami a certifikáty zajistí hladký start používání čipových karet a certifikátů v organizaci.

Velmi dobře si uvědomujeme, že řešení se dotýká téměř každého zaměstnance, a proto je nutné zvolit citlivý přístup k implementaci. Úspěšné zvládnutí projektu zajistí především úzká spolupráce s oddělením informačních technologií a oboustranný proaktivní přístup.

3 ŘEŠENÍ PROID+

Řešení ProID+ se skládá z čipových karet ProID+ Q a Manažera ProID+, který zajišťuje řízení životního cyklu karet a certifikátů. Řešení ProID+ nabízí zavedení a nastavení nových procesů spojených s přítomností karet a certifikátů ve Vaší organizaci.

Služby a komponenty ProID+

► Karty ProID+ Q

Certifikované karty ProID+ Q **podléhají certifikaci SSOD / QSCD a je v souladu s evropskou směrnicí eIDAS**. Jsou určeny pro ochranu soukromých klíčů, spojených s elektronickými certifikáty.

Čipová karta **ProID+ Q je určena pro práci s kvalifikovaným elektronickým podpisem**. Tento podpis je založený na certifikátu vydaném od akreditovaných certifikačních autorit – eIdentity a PostSignum. Mimo tohoto typu certifikátu karta podporuje i jiné certifikáty od neakreditovaných autorit.

ProID+ Q je špičkový produkt ve své kategorii a výrazně se odlišuje od ostatních bezpečnostních předmětů na trhu. Karty **ProID+ Q je možné recyklovat** v souladu s požadavky a standardy kladenými na certifikované čipové karty. Služba recyklace přinese výrazné snížení nákladů na pořízení nových karet.

Aplikace pro automatizovanou obnovu certifikátů (ACEx) spolu s čipovou kartou nabízí maximální pohodlí při práci s kartou. Automatizovaná obnova certifikátů zároveň podporuje i obnovu certifikátů z doménové certifikační autority.

Vlastnosti karty ProID+ Q uvítají především zástupci samosprávy a veřejné správy (eGovernment), zdravotnictví (eHealth a ePreskripce), justice, soudního znalcství, ekonomického útvaru, a vůbec všichni, kteří potřebují svým elektronickým podpisem projevit nejvyšší stupeň důvěry.

ProID+ Q jsou karty s PKI funkcionalitou + podpůrný software, který zajišťuje integraci karet do operačního systému uživatele a umožňuje s nimi pracovat.

Nasazení čipových karet doporučují nebo přímo vynucují všechny aktuální normativní a legislativní dokumenty:

- » GDPR,
- » Zákon o kybernetické bezpečnosti,
- » eIDAS a
- » rodina standardů ISO 27000.

Čipové karty nabízí nejvyšší stupeň bezpečnosti. Formou jednoduchého použití, které všichni znají například při použití bankovní karty.

► Čtečky čipových karet

Pro práci s čipovou kartou jsou potřebné čtečky. Čtečka je připojena do počítače přes standardní usb port.

► Manažer ProID+

Manažer ProID+ integruje do organizace nejdůležitější procesy potřebné pro práci s kartou a certifikáty.

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 z doménových a akreditovaných certifikátů.

Kartové centrum s CMS je manažerem karet a doménových certifikátů v organizaci, stará se o potisk. Kartové centrum s CMS velmi zjednodušuje agendu potřebnou pro správu karet a certifikátů. Díky zjednodušení správy mohou být tyto nové kompetence uděleny mimo IT oddělení.

► **Služby**

- » Implementace
- » Aktivace doménové PKI infrastruktury
- » Dokumentace
- » Servisní podpory

Řešení ProID+ je určeno primárně pro použití v rámci organizací, mohou jej však využít i samostatné (fyzické či právnické) osoby. Nejsnáze lze ProID+ integrovat do organizací, které chtějí kvalifikovaný elektronický podpis nebo dvoufaktorovou autentizaci a provozují doménu MS Windows s Active Directory.

Poměrně často se uživatelé ProID+ stávají organizace, které dosud provozují karty (pouze) v bezkontaktních systémech. Tyto organizace jsou zvyklé na používání karet, chápou jejich výhody a chtějí rozšířit jejich použití i pro zabezpečení informačních systémů.

Mezi obvyklé důvody, proč si organizace pořizují ProID+, patří:

► **Kvalifikovaný elektronický podpis**

- » naplnění požadavků eIDAS v bodech určených pro kvalifikovaný elektronický podpis;
- » certifikáty vydané akreditovanou certifikační autoritou.

► **Dvoufaktorová autentizace do počítače**

- » základní doporučení pro zákon č. 181/2014 Sb Zákon o kybernetické bezpečnosti a normy ISO / IEC 27001 a 27002, GDPR;
- » náhrada přihlášení jménem / heslem, Smartcard Logon;
- » odstranění nepříjemně dlouhých hesel s nutností periodické obnovy;
- » základ pro Single Sign On.

► Bezpečná autentizace do VPN

► Elektronické podepisování a šifrování e-mailů

► Šifrování disků a souborů

► Autentizace certifikátem na webové servery (HTTPS)

► atd...

ProID+ jsou karty pro ochranu soukromých klíčů, spojených s elektronickými certifikáty. Vzhledem ke komplexnosti celého řešení je třeba životní cyklus čipových karet a certifikátů v organizaci řídit, proto jsou jako součást řešení dodávány aplikace, které celou správu automatizují a zjednodušují.

ProID+ je modulární řešení a jeho funkcionalitu můžete postupně doplňovat. Tento dokument si klade za cíl představit řešení ProID+.

4 SLUŽBY A KOMPONENTY PROID+

Pro provoz karet ProID+ Q je Monet+ schopen dodat řadu položek. Některé z těchto položek jsou povinné (např. samotné karty ProID+ Q). Další položky, dodávané s ProID+ jsou nepovinné – vytvářejí nadstavbu nad kartami, řeší specifické problémy životního cyklu karet, příp. zvyšují komfort uživatelů a správců karet. Položky jsou podrobněji specifikovány v následujících podkapitolách.

4.1 NÁVRH ŽIVOTNÍHO CYKLU KARET

Před implementací karet a aplikací bude vypracován dokument s návrhem životního cyklu karet v organizaci. V rámci dokumentu budou řešena 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
- ▶ Potisk dodávaných karet

4.1.1 Postup zpracování návrhu životního cyklu

Zpracování návrhu životního cyklu se předpokládá následujícím způsobem

- ▶ Zpracování draftu dokumentu životního cyklu
 - » Předpokládá se, že si pracovníci organizace prostudují návrh před prezentačním workshopem
- ▶ Workshop, na němž budou vzneseny připomínky k navrženému životnímu cyklu
 - » Bude bezprostředně navazovat na prezentaci životního cyklu
 - » V průběhu workshopu budou pracovníci organizace vznášet připomínky k návrhu
- ▶ Finalizace dokumentu s návrhem životního cyklu (zpracování připomínek z workshopu)
 - » Výstup bude sloužit pro následnou implementaci a konfiguraci karet a aplikací

4.2 DOMÉNOVÁ CERTIFIKAČNÍ AUTORITA

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 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:

- ▶ Kořenová 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
- ▶ Je dodána specifická dokumentace pro správu a provoz, spolu s havarijnými plány.
- ▶ Nejsou dodávány certifikační politiky ani certifikační prováděcí směrnice

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

- ▶ Návrh bezpečnostního konceptu, integrace do bezpečnostních politik organizace.
- ▶ Hierarchii CA.
- ▶ Ochrana klíčů CA v HSM.
- ▶ Dodávka certifikačních politik a/nebo certifikačních prováděcích směrnic.

Tyto specifické požadavky řeší MONET+ projektově.

4.3 ČIPOVÉ KARTY PROID+ Q

ProID+ Q jsou karty pro ochranu soukromých klíčů, spojených s elektronickými certifikáty. Pro jejich použití je proto nutno mít v čipu uložen alespoň jeden pár klíčů s certifikátem.

Certifikát musí vydat certifikační autorita; v doménovém prostředí je to nejčastěji doménová certifikační autorita na platformě MS Windows Server. Karty však mohou hostovat certifikáty, vydané z libovolných certifikačních autorit, např. akreditovaných poskytovatelů certifikačních služeb – eIdentity a PostSignum.

Karty ProID+ Q jsou procesorové čipové karty, s implementovanou asymetrickou kryptografií na kontaktním čipu, umožňují bezpečné uložení privátních klíčů a z toho vyplývající výhody

- ▶ Všechny operace s privátním klíčem probíhají uvnitř čipu – klíč neopustí prostředí karty.
- ▶ Privátní klíč uložený na kartě nelze z karty vyexportovat.
- ▶ Klíče mohou být generovány v čipu anebo mohou být na kartu importovány.
- ▶ K párům klíčů lze na kartu uložit i příslušné certifikáty.
- ▶ Po vytažení karty se čtečky se automaticky uzamkne pc nebo přeruší komunikace s aplikací.

Kontaktní část čipových karet reprezentuje čip od společnosti Gemalto. Tento typ čipu splňuje mezinárodní kryptografické standardy. Jedná se o nejnovější dodávaný typ čipu.

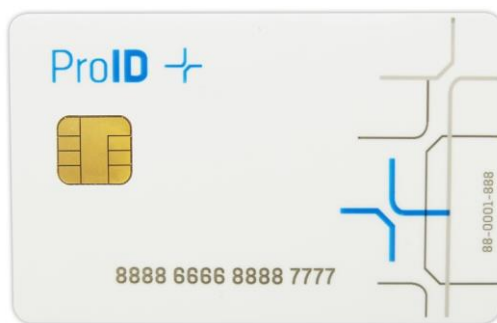
ProID+ je v souladu s Smart Card Minidriver Specification; lze jej použít v řadě aplikací, které podporují kryptografické standardy Microsoft CryptoAPI, Cryptography Next Generation, PKCS#11 nebo TokenD.

Nabízená čipová karta je ve formátu ID-1, což odpovídá přesným rozměrům a velikosti bankovní karty.

Karta ProID+ Q disponuje certifikací SSCD / QSCD. Čip společně s aplikací nahanou v čipu karty ProID+ Q podléhá certifikaci QSCD a podporuje vydání certifikátů pro kvalifikovaný elektronický podpis v režimu eIDAS.

4.3.1 Formát ID-1

Jedna karta na všechno – bezpečnost, bezkontaktní čip a držiteléské údaje na těle karty. Taková karta nabízí držiteli integraci hned několika funkcí a nejlépe zapadá do pracovního prostředí.



Obrázek 1 Čipová karta ProID+ Q formát ID-1

Karty ve formátu ID-1 mohou být – kromě kontaktního čipu – osazeny také bezkontaktním čipem, který lze v organizaci využít v rámci bezkontaktních systémů – docházkový systém, vyhrazený přístup do určitých částí budovy, kopírování atp. Taková karta se dodává jako hybridní (kontaktní a bezkontaktní čip).

Monet+ standardně podporuje dodávky hybridních karet s bezkontaktním čipem Mifare, DESFire a Emarine. Ostatní typy např. HID, ISO Prox, Indala, Cotag je třeba konzultovat. Třebíč pro obsluhu svých bezkontaktních systémů používá **bezkontaktní čip EM4102**.

Karta ve formátu ID-1 nabízí dostatečně velkou plochu pro potisk, a proto ji organizace může využít pro tisk osobních údajů a korporátního designu. V takovém případě karta slouží i jako zaměstnanecký průkaz.

4.4 ČTEČKY ČIPOVÝCH KARET

Obecně lze uvést, že karty ProID+ Q fungují s libovolnými čtečkami, které dodržují standard PC/SC. Organizace, která chce používat ProID+ může použít stávající čtečky (pokud již má čtečky kontaktních karet). Je však třeba upozornit na fakt, že ne všechny čtečky, které jsou na trhu, jsou stejně kvalitní. Monet+ provozuje vlastní Smart PKI kompetenční centrum, v rámci nějž jsou testovány čtečky různých výrobců. Srovnáním výsledků testů lze dojít k závěru, že méně kvalitní čtečky mají tyto nejčastější vady: dlouhá doba odezvy (=delší čekání na práci karty), potíže s kontakty (=kartu je nutno vkládat opakovaně), výpadky spojení s operačním systémem.

Čtečky karet pro formát ID- 1 mohou být

- ▶ Externí čtečky (viz ukázka obrázek 3) jsou připojeny k PC přes USB.
- ▶ Integrované čtečky do notebooku, PC nebo klávesnice.



Obrázek 2 Příklad externí čtečky čipových karet Gemalto IDBridge CT30

4.5 MANAŽER PROID+

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. ProID+ manažer podporuje jak karty ProID+ tak ProID+ Q v obou formátech.

4.5.1 Kartové centrum ProID+

Aplikací pro centrální personalizaci a správu čipových karet je Kartové centrum ProID+.

Kartové centrum ProID+ je implementováno jako tlustý klient a bude instalováno na 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

- ▶ **Vydání nové (trvalé) karty.** Obsluha zvolí jednoho či více uživatelů a pomocí kartového centra pro ně kompletně připravuje funkční karty: vydává na každou kartu jeden či více certifikátů (podle zvoleného „profilu“), generuje nové hodnoty PIN, resp. PUK karty, tiskne nově nastavené hodnoty PIN/PUK na PIN-formulář. Výsledkem procesu jsou kompletně připravené karty, které lze distribuovat pracovníkům a ti je mohou ihned začít používat. 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 vydává jeden či více certifikátů, obvykle se zkrácenou dobou platnosti. Aplikace tiskne nově nastavené hodnoty PIN/PUK karty. Scénář slouží pro řešení situace, kdy je třeba pracovníkovi operativně vydat kartu s certifikáty; např. pro řešení situace zapomenutí karty, ztráty karty, nových zaměstnanců. Předpokládá se, že dočasná karta překlene období, než se pracovníkovi vydá trvalá karta.
- ▶ **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.
- ▶ **Odvolání doménových certifikátů na kartách.** Obsluha může vyhledat jednu či více karet a odvolat certifikáty, které jsou evidovány k jednotlivým kartám.
- ▶ **Evidence ztráty či zničení karty.** Obsluha může vyhledat jednu či více karet, označit ji v evidenci jako ztracenou či zničenou / skartovanou; může zvolit, zda mají být zároveň odvolány certifikáty, evidované k vybraným kartám.
- ▶ **Evidence požadavků na nové karty.** Obsluha může do centrální evidence zavést požadavek na dodání nové karty konkrétnímu pracovníkovi. (Evidované požadavky jsou jednou za čas expedovány dodavateli karet, viz scénář níže.)
- ▶ **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.
- ▶ **Integrace potisku karet držitelskými údaji.** Informace o držitelích karet mohou být na kartu vytištěny v procesu vydání karty držiteli.

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 uživateli a šablonách certifikátů)

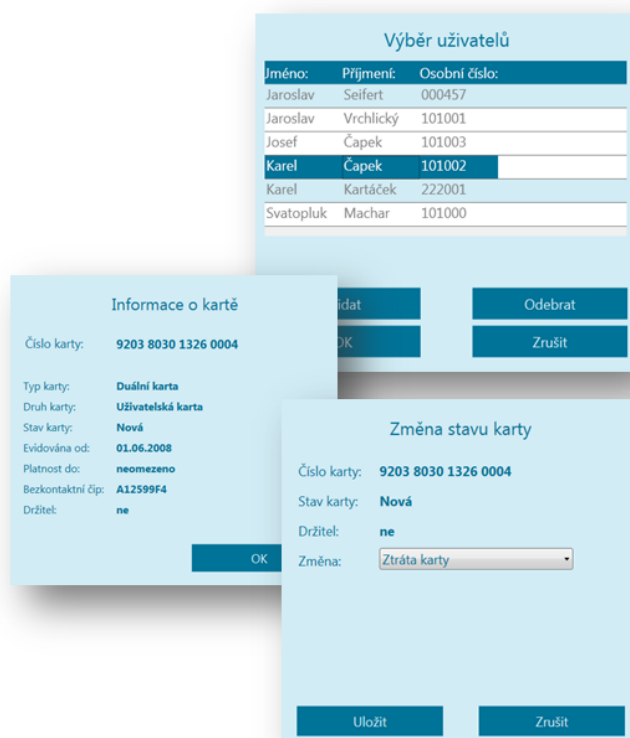
Pro přístup k uvedeným subsystémům se využívá integrovaná doménová autentizace (SSO).

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 3 Ukázka Kartové centrum ProID+

Oprávnění k použití Kartového centra

Pro použití aplikace Kartové centrum ProID+ se předpokládá využití integrované doménové autentizace: 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.

4.5.2 Card Management System (CMS) ProID+

Pro evidenci a správu karet implementujeme Card Management System ProID+ (CMS ProID+).

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



Obrázek 4 Ukázka aplikace CMS ProID+

Data karty

CMS eviduje kompletní informace o kartách

- ▶ identifikátor karty (kontaktního čipu i bezkontaktního čipu),
- ▶ typ karty (kontaktní, bezkontaktní, hybridní,...),
- ▶ druh karty (uživatelská, administrační, operátorská,...),
- ▶ 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 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 uživateli / držitelích karet,
- ▶ CMS akceptuje nastavení doménových bezpečnostních politik,
- ▶ uživatelské role CMS jsou mapovány na doménové skupiny (domain groups),

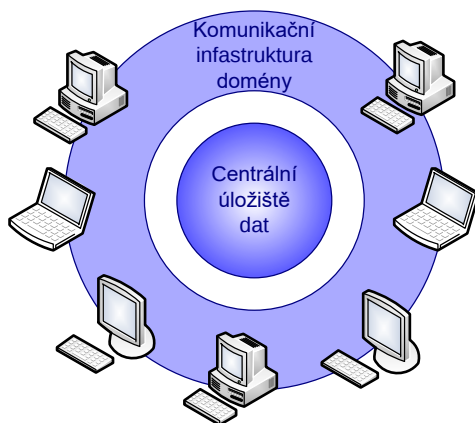
- ▶ CMS definuje oprávnění na úrovni doménových skupin,
- ▶ CMS podporuje využití integrované autentizace domény MS Windows (Single Sign On).

4.5.2.1 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 síťových 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 5 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.

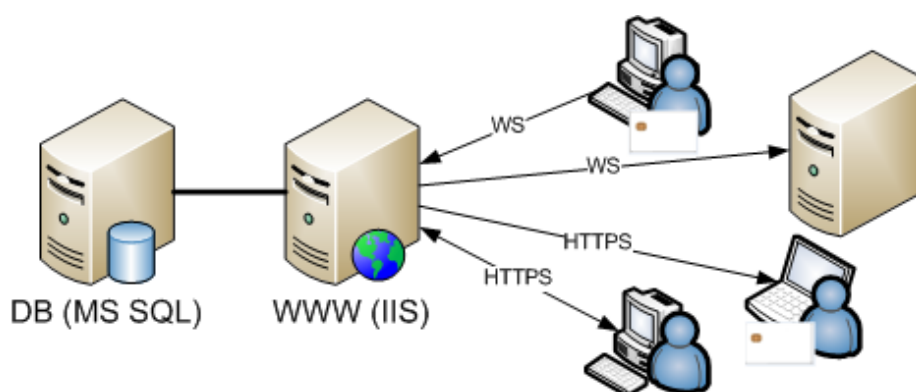
CMS také spolupracuje s dalšími moduly technologie ProID+, které pracují s čipovými kartami. Tyto moduly zasílají informace o provedených operacích do CMS. Změny stavů i informace o držitelích jsou tak automaticky promítány do centrální evidence. Díky tomu jsou údaje vždy aktuální. Centrální evidence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



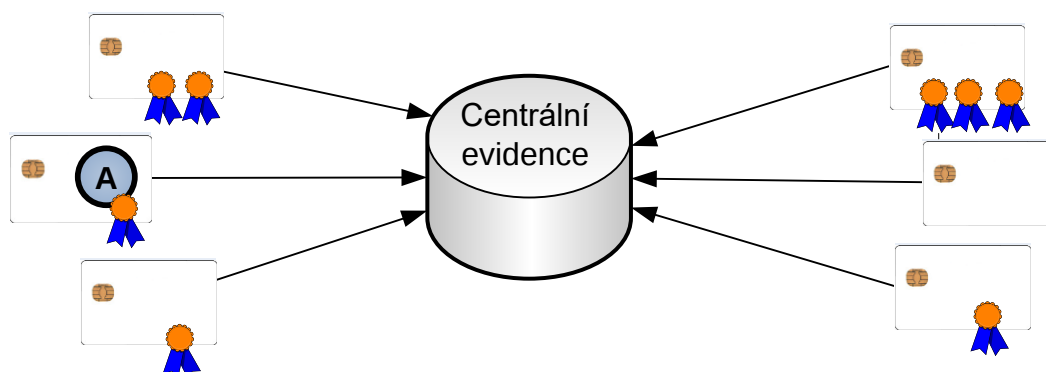
Obrázek 6 Architektura CMS ProID+

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 7 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.

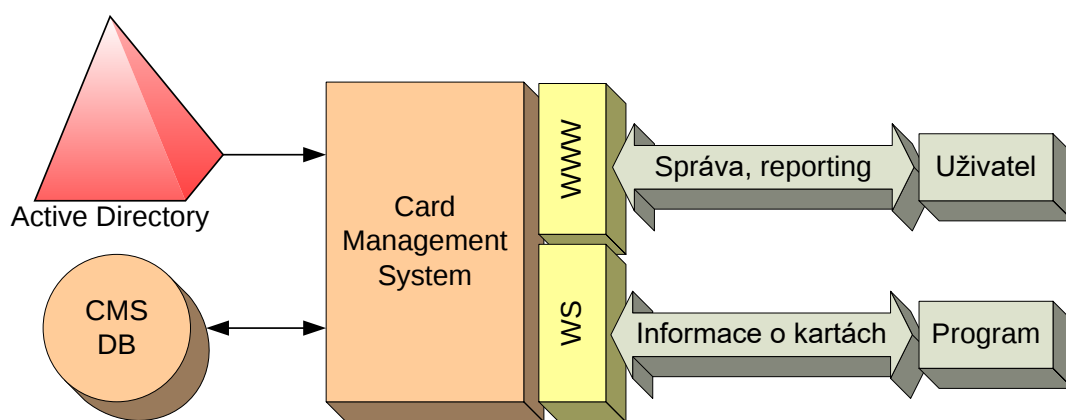
Navigace v datech CMS využívá běžných webových odkazů, menu a grafických symbolů. Ovládání webových stránek je intuitivní. Po krátkém zaškolení zvládne obsluhu stránek i méně zkušený uživatel.

Informace o uživateli

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

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

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



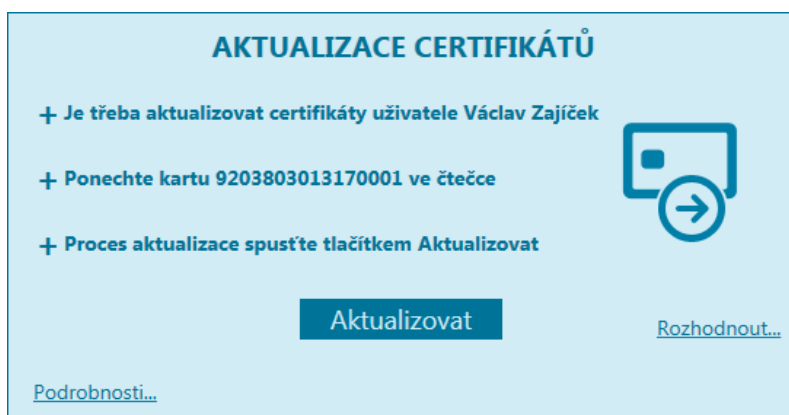
Obrázek 8 Zdroj dat o uživateli

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

4.6 ACEX

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 9 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. blíží-li 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.

4.7 POTISK ČIPOVÝCH KARET

Potisk karet je možné rozdělit do dvou základních vrstev – základní design a držitelské údaje. Přístup k potisku je pak možné realizovat následovně:

- ▶ Obě vrstvy mohou být vytištěny dodavatelsky.
- ▶ Základní design je vytištěn externě dodavatelem a v rámci organizace se dotiskují uživatelské údaje.
- ▶ Organizace si tiskne na vlastní tiskárně design karty společně s držitelskými údaji.

S ohledem na zamýšlenou emisi čipových karet doporučuje Monet+ nechat potisknout první emisi externě základním designem karty. Následný dotisk realizovat na vlastní tiskárně. Pořízená tiskárna bude zároveň podporovat tisk kompletních vrstev karty, což úřadu pomůže při potřebě vydat dotisky karet v menším počtu.

Tato nabídka obsahuje tiskárnu, která potiskne kartu trvalým způsobem a umožní vytisknout na tělo karty držitelské údaje i základní design.

4.8 IMPLEMENTACE APLIKACÍ PRO SPRÁVU KARET A ŠKOLENÍ

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 budou:

- ▶ Dokument s návrhem životního cyklu

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

- ▶ Autentizace do domény
- ▶ Podepsání dat

4.9 SERVISNÍ PODPORA

Základní servis nabízeného řešení zahrnuje podporu:

- ▶ operačních systémů na klientských stanicích Windows 7 až Windows 10
- ▶ serverových operačních systémů Windows Server 2008 R2 a vyšších
- ▶ čipových karet ProID+ Q do konce životnosti
- ▶ čteček pro práci s kartou, které splňují standard PC/SC

- ▶ instalovaných PKI aplikací pro správu životního cyklu karet a certifikátů
- ▶ formou Service Desku v režimu 5 x 8, jehož provozní doba je od 8:00 do 16:00 v pracovní dny.
- ▶ Reakční doby:
 - » Přijetí požadavku do 2 hodin od nahlášení.
 - » Dočasné řešení do 1 pracovního dne od přijetí požadavku.
 - » Vyřešení požadavku do 3 pracovních dnů od dodání dočasného řešení.
 - » Reakční doby jsou garantovány pro serverové komponenty řešení. Pro koncové stanice bude ze strany Monet+ vyvinuto maximální úsilí pro vyřešení vzniklého incidentu. Důvodem je heterogenní prostředí na vrstvě aplikační a operačních systémů u operačních stanic.

5 CENOVÁ NABÍDKA

Cenová nabídka uvádí položkové ceny. Ceny jsou uvedeny v Kč a bez DPH. Cena zahrnuje dopravu do jednoho místa určení.

Celková cena dodávky

POLOŽKA	MNOŽSTEVNÍ KATEGORIE	CENA V Kč BEZ DPH	CENA V Kč S DPH
Čipové karty ProID+ Q	280	137 200,-	166 012,-
Čtečka čipových karet Gemalto IDBridge CT30	280	89 600,-	108 416,-
Návrh životního cyklu karet a certifikátů	1	28 000,-	33 880,-
Card Management System	1 licence	65 000,-	78 650,-
Kartové centrum ProID+	1 licence	55 000,-	66 550,-
ACEx	multilicence pro 350 instalací	65 000,-	78 650,-
Vybudování doménové CA + havarijní a provozní dokumentace	1	70 000,-	84 700,-
Tiskárna karet se spotřebním materiálem	1	63 000,-	76 230,-
Implementace	1	135 000,-	163 350,-
Školení	1	10 500,-	12 705,-
Celková cena		718 300,-	869 143,-
Servisní podpora na měsíc		3980,-	4816,-

Tabulka 1 Celková cena dodávky

V Třebíči dne

Ve Zlíně dne

Za kupujícího:

Ing. Pavel Janata
Starosta města Třebíč

Za prodávajícího:

Ing. Břetislav Endrys
Předseda představenstva

Za prodávajícího:

Mgr. Jiří Beneš
Prokurista

Harmonogram implementačních prací	
Úvodní schůzka	09. 01. 2019
Zřízení vzdálených přístupů	08. 02. 2019
Zřízení serverů IIS, DB, CA	08. 02. 2019
Dodání návrhových dokumentací	15. 02. 2019
Příprava konfigurací + ověření v testovací doméně M+	22. 02. 2019
Implementace CA + PKI u zákazníka	01.03. 2019
Implementace IIS + DB + PC Správce + MSI ProID+Q - vzdálený přístup	08. 03. 2019
Školení u zákazníka + dodávka MSI ACEx	15. 03. 2019
Ověřovací provoz	15. 03. 2019
Dodání Havarijního plánu a provozní dokumentace CA	08. 03. 2019
Odsouhlasení Havarijního plánu a provozní dokumentace CA	23. 03. 2019
Předání do ostrého provozu	23. 03. 2019

V Třebíči dne

Ve Zlíně dne

Za kupujícího:

Ing. Pavel Janata
Starosta města Třebíč

Za prodávajícího:

Ing. Břetislav Endrys
Předseda představenstva

Za prodávajícího:

Mgr. Jiří Beneš
Prokurista