Kupní smlouva

uzavřená podle § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších právních předpisů (dále jen: „Smlouva“)

Čl. 1. Smluvní strany

Kupující:	**Centrum pro regionální rozvoj České republiky**
se sídlem:	U Nákladového nádraží 3144/4, 130 00 Praha 3
IČO:	04095316
zastoupen:	Ing. Zdeňkem Vašákem, generálním ředitelem
zástupce pro věci technické:	Ing. Eva Pavlíková, vedoucí OIS
Telefon, e-mailové spojení:	xxxxxxxxxxxx, E-mail: xxxxxxxxxxxxxxxxxxxx

(dále jen „**kupující**“ nebo „**smluvní strana**“)

a

Prodávající:	**MONET+,a.s.**
se sídlem:	Za Dvorem 505, 763 14 Zlín - Štípa
IČO:	26 21 77 83
DIČ:	CZ 26 21 77 83
Zapsán v obchodním rejstříku vedeném Krajským soudem v Brně, spisová značka B 3351	
Zastoupen:	Ing. Břetislav Endrys, předseda představenstva
	Ing. Jan Vavrys, člen představenstva
Bankovní spojení:	xxxxxxxxxxxxxxxxx,xxxxxxxxxxxxxxxxx
zástupce pro věci technické:	David Říhošek, drihosek@monetplus.cz,xxxxxxxxxxxxxxxxxxxx
Telefon, e-mailové spojení:	xxxxxxxxxxxxxxxxxxx,xxxxxxxxxx
Adresa pro elektronické doručování korespondence smluvních stran: xxxxxxxxxxxxxxxxxxxxxxx	

(dále jen „**prodávající**“ nebo „**smluvní strana**“)

Čl. 2. Úvodní ustanovení a účel Smlouvy

2.1. Smluvní strany uzavřely tuto Smlouvu na základě výsledků zadávacího řízení na podlimitní veřejnou zakázku s názvem „**Kartový systém**“ (dále také „zadávací řízení“ a/nebo „veřejná zakázka“).

2.2. Účelem této Smlouvy je prostřednictvím plnění specifikovaného dále v čl. 3 a Přílohách č. 1 a č. 3 této Smlouvy zajistit nový kartový systém v organizaci kupujícího odpovídající v této Smlouvě obsaženým podmínkám.

Čl. 3. Předmět Smlouvy

3.1. Prodávající se touto Smlouvou zavazuje, že dodá kupujícímu položky dále podrobně specifikované v odst. 3.2. této Smlouvy a s jejich dodáním a provozem související služby dále specifikované v odst. 3.3. a 3.4. této Smlouvy, oboje doplněné popisem v Příloze č. 1 a č. 3 této Smlouvy (dále souhrnně také „**zboží**“), převede vlastnictví ke zboží odevzdáním zboží, a kupující se zavazuje, že převezme bezvadné zboží a uhradí prodávajícímu za dodané zboží kupní cenu. Prodávající odevzdá kupujícímu zboží ve specifikaci a v množství dle této Smlouvy.

3.2. Dodávkou zboží je v první řadě myšlena dodávka kompletního kartového systému a v jeho rámci dodání karet s bezkontaktním čipem a hybridních karet (tzn. s kontaktním a bezkontaktním čipem) včetně HW a SW příslušenství pro správu řízení jejich životního cyklu. Všechny dodávané čipové karty musí být ve formátu ID-1 (velikost bankovní karty) a musí splňovat certifikaci SSCD/QSCD se zabezpečením garantovaného

dokoupení dalších karet stejného typu po dobu platnosti smlouvy v případě potřeby na straně kupujícího. Dodávka sestává z následujících položek:

3.2.1. Čipové karty ve formátu ID-1 (velikost bankovní karty). Nosičem je plastová karta bílé barvy o rozměrech 85,60 x 53,98 mm se zakulacenými rohy s poloměrem 2,88 – 3,48 mm, která odpovídá mezinárodní normě ISO/IEC 7810, která stanovuje fyzikální vlastnosti identifikačních karet – formátu ID-1. Karty budou dodány v následujících počtech:

- **2 000 ks** hybridních čipových karet, z toho:
  - 1 500 ks hybridních čipových karet pro průkaz státního zaměstnance s potiskem dle Vyhlášky č.388/2017 Sb. Pozadí lícové barvy tvoří modrá barva, která ve spodní části plynule přehází do barvy červené. Všechny texty musí být vyhotoveny bezpatkovým písmem v černé barvě. Rubová strana bude vyhrazena pro zápis jiných údajů např. zmocnění k provádění kontrolních činností. Tisk musí být stálý, nesmí se rozmazávat.
  - 500 ks hybridních čipových karet pro zaměstnanecký průkaz. Potisk bude vycházet ze vzoru průkazu státního zaměstnance (stejná pole pro tisk osobních údajů). Jiná bude barva pozadí a logo.
- **200 ks** bezkontaktních čipových karet pro potřeby návštěv, úklidu apod. Tyto karty budou bílé s logem organizace a označením „Návštěva č. …“).

Dále z celkového počtu 2 000 ks hybridních čipových karet bude v počtu 550 ks dodáno s kompletním tiskem, tzn. osobních údajů a fotografií, které budou kupujícím pro tento účel předány prodávajícímu. Dotisk (osobních údajů a fotografií) do příslušných polí na kartě u zbylých karet si kupující bude provádět sám, údaje pro tisk budou čerpány z AD.

3.2.2. **2 200 ks** pouzder včetně šňůrky s karabinkou.

3.2.3. **510 ks** externích USB čteček čipových karet, s možností garantovaného dokoupení dalších čteček stejného typu po dobu platnosti smlouvy. Čtečky musí dodržovat standard PC/SC.

3.2.4. **2 000 ks** bílých PIN formulářů pro bezpečné předání PIN a PUK uživatelům.

3.2.5. **Tiskárna** pro potisk karet (oboustranný potisk karet) včetně ovládacího SW a spotřebního materiálu na potisk a laminaci. Součástí dodávky bude i SW na editaci a přípravu dotisku na karty. SW musí být kompatibilní s OS Windows 10. SW musí obsahovat minimálně několik šablon, které umožní i hromadný tisk karet. Dotištěné údaje na kartě musí být permanentní a výsledná karta musí být v souladu s vyhláškou Ministerstva vnitra č. 388/2017 Sb. Tiskárna bude rozšířena (povinné příslušenství) o laminátor čipových karet.

3.2.6. **SW aplikace** pro správu čipových karet a certifikátů s licencí na dobu neurčitou pro 2 000 uživatelů, respektive pro 2 registrační místa pro správu čipových karet.

3.3. Nezbytnou součástí dodávky zboží jsou i dále uvedené služby:

3.3.1. **Doprava** zboží do sídla kupujícího.

3.3.2. **Implementace** zboží do systémové infrastruktury kupujícího - veškeré instalační a implementační práce nezbytné k uvedení dodávaného řešení do plného provozu v rámci systémové infrastruktury kupujícího.

Před vlastní implementací bude vypracován dokument s návrhem životního cyklu karet. Dokument bude obsahovat zejména popis (řešení):

- rolí uživatelů pro správu a použití karet,
- způsobu distribuce karet uživatelům,
- vydání a obnovy certifikátů na kartách,
- podporovaných stavů karet a jejich vlastnosti,
- řešení nestandardních stavů (zapomenutí karty, ztráta, apod.),
- aplikační scénáře (podklady pro konfigurace dodávaných aplikací),
- potisk karet.

Dokument bude dále obsahovat analýzu (revizi) stávající PKI infrastruktury kupujícího.

3.3.3. **Zaškolení** administrátorů (maximálně 5 osob).

3.3.4. Zpracování a předání **uživatelské** a **administrátorské dokumentace** ke kartovému systému.

3.3.5. Zpracování a předání podkladů na implementaci šablon pro vydání certifikátů pro autentizaci uživatelů do PC, VPN, interní elektronický podpis a případně další uživatelské akce.

3.4. Součástí předmětu plnění je rovněž zabezpečení servisní podpory zboží po celou dobu trvání této Smlouvy, zajišťující plnou funkčnost dodaného zboží, HW a SW aplikací. Součástí je rovněž upgrade a update HW a SW, vč. tzv. legislativního a technického update; podrobně viz bod 5 Přílohy č. 1 této Smlouvy.

3.5. Detailní popis předmětu plnění je obsažen v Příloze č. 1 této Smlouvy (Minimální technické požadavky kupujícího na předmět plnění) a dále v Příloze č. 3 této Smlouvy (Technická specifikace zboží a služeb). Pro případ rozporů mezi Přílohou č 1 a č. 3 smluvní strany sjednávají, že přednost má Příloha č. 1.

3.6. Předmětem této Smlouvy je dále závazek prodávajícího dodat kupujícímu, v případě požadavku kupujícího vzneseného vůči prodávajícímu po dobu platnosti této Smlouvy, dodatečné dodávky čipových karet (dle 3.2.1. výše), pouzder (dle 3.2.2. výše) či čteček (dle 3.2.3. výše), a to za jednotkové ceny sjednané v této Smlouvě.

Čl. 4. Lhůta a místo plnění

4.1. Prodávající se zavazuje, že uskuteční plnění předmětu této Smlouvy ve smyslu dodání bezvadného zboží (všech položek dle odst. 3.2. a 3.3. této Smlouvy) na místo plnění a provedení a řádné dokončení instalace a implementace zboží a uvedení zboží do provozu nejpozději do 90 kalendářních dnů ode dne nabytí účinnosti této Smlouvy.

4.2. Prodávající se zavazuje poskytovat kupujícímu HW a SW technickou podporu dle odst. 3.4. této Smlouvy po dobu 10 let ode dne předání a převzetí zboží dle odst. 8.7. písm. a) této Smlouvy.

4.3. Jako místo plnění se sjednává sídlo kupujícího.

Čl. 5. Cena

5.1. Cena za zboží a služby dle odst. 3.2. až 3.5. této Smlouvy, v množství a specifikaci dle článku 3. a Příloh č. 1 a č. 3 této Smlouvy, je stanovena v Příloze č. 2 – Tabulka cen této Smlouvy.

5.2. V celkové kupní ceně, jakož i v jednotkových cenách, jsou zahrnuty veškeré náklady prodávajícího související s poskytnutím plnění dle této Smlouvy (tedy kromě ceny samotné položky rovněž zejména náklady na dopravu do místa dodání, balné, náklady na montážní práce, náklady na likvidací odpadů, náklady na zajištění HW a SW podpory, ceny licencí apod.).

5.3. Změna celkové kupní ceny je možná pouze v případě, že při realizaci předmětu plnění této Smlouvy dojde ke změnám sazeb DPH. V tomto případě bude celková kupní cena za poskytnuté plnění (resp. cena za poskytnuté dílčí plnění) upravena podle výše sazeb DPH platných v době vzniku zdanitelného plnění. V takovém případě nebude vyhotoven dodatek k této Smlouvě. Účinnost této změny celkové kupní ceny nastává v návaznosti na účinnost změny příslušného obecně závazného daňového předpisu.

Čl. 6. Platební podmínky

6.1. Zaplacení kupní ceny za položky dle odst. 3.2. a 3.3. této Smlouvy bude provedeno jednorázově bezhotovostně po akceptaci a převzetí úplného a funkčního plnění dle odst. 3.2. až 3.4. této Smlouvy a zahájení plnění dle odst. 3.4. této Smlouvy a cena bude odpovídat součtu položek č. 1 až 10 Přílohy č. 2 této Smlouvy. Zaplacení ceny za servisní podporu dle odst. 3.4. této Smlouvy bude realizováno ročně předem a tato roční cena bude odpovídat jednotkové ceně za servisní podporu dle položky č. 11 přílohy č. 2 této Smlouvy. Úhrada kupní ceny kupujícím bude provedena na základě prodávajícím vystaveného daňového dokladu (dále tak jen „faktura“), doručeného kupujícímu, ve prospěch bankovního účtu prodávajícího, uvedeného na této faktuře. Kupující neposkytuje zálohy.

6.2. Prodávající doručí fakturu kupujícímu vždy ve dvou výtiscích neprodleně po akceptaci a převzetí zboží kupujícím, resp. v prvním měsíci nového (začínajícího) ročního období, za které je servisní podpora účtována, nejpozději však do 14 (čtrnácti) dnů po převzetí zboží kupujícím, resp. do konce prvního měsíce nového ročního období podpory. Prodávající doručí fakturu na adresu kupujícího uvedenou v záhlaví této Smlouvy. Kupující zaplatí dle faktury do 30 (třiceti) dnů ode dne jejího prokazatelného obdržení. Za den splnění platební povinnosti se považuje den odepsání placené částky (kupní ceny) z bankovního účtu kupujícího.

6.3. Faktura musí obsahovat všechny náležitosti stanovené § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a § 435 občanského zákoníku, odkaz na tuto smlouvu a věcné a cenové členění na jednotlivé položky zboží. V případě faktury za zboží dle čl. 3.2. a 3.3. této Smlouvy bude součástí faktury jako její příloha dodací list, podepsaný při převzetí zboží osobou oprávněnou jednat za kupujícího ve věcech technických, případně jiným zástupcem kupujícího pro tento účel zmocněným, seznam poskytnutých souvisejících služeb dle odst. 3.3. této Smlouvy s uvedením místa, data poskytnutí služeb a osoby jednající za kupujícího, která tyto služby za kupujícího převzala a akceptační protokol potvrzující úspěšnost implementace a funkčnost dodaného zboží.

6.4. Kupující je oprávněn před uplynutím lhůty splatnosti vrátit fakturu, která neobsahuje požadované náležitosti, nebo není doložen požadovanými a úplnými doklady, nebo obsahuje nesprávné údaje.

6.5. V případě vrácení faktury kupující písemně sdělí důvod vrácení faktury. Po vrácení faktury kupujícím je prodávající povinen vystavit a doručit kupujícímu novou fakturu s tím, že vrácením faktury lhůta splatnosti vrácené faktury zaniká. Nová lhůta splatnosti dle nové faktury v délce dle odst. 6.2. Smlouvy začne běžet po dni prokazatelného doručení řádné faktury mající všechny náležitosti stanovené touto Smlouvou a opatřené dodacím listem, podepsaným tak, jak je uvedeno v odst. 6.3. Smlouvy, a seznamem a akceptačním protokolem dle odst. 6.3. Smlouvy.

6.6. V případě, že v průběhu plnění této Smlouvy dojde ke změně registrace k dani z přidané hodnoty prodávajícího, je prodávající povinen nejpozději do 3 (tří) kalendářních dnů písemně informovat kupujícího o změně registrace k dani z přidané hodnoty (tj. informovat o zrušení registrace k dani z přidané hodnoty, nebo o podání přihlášky k registraci).

Čl. 7. Licenční ujednání

7.1. Prodávající prohlašuje, že součástí zboží je i zboží, které je předmětem ochrany autorských práv (softwarové vybavení kartového systému). K takovému zboží prodávající jeho dodáním převádí na kupujícího licenci k užívání zboží všemi způsoby užití v neomezeném rozsahu, v pochybnostech se má za to, že se jedná o licenci nevýhradní, převoditelnou, časově a místně neomezenou. Prodávající prohlašuje, že cena licence je zahrnuta v kupní ceně dle článku 5 této Smlouvy.

7.2. Prodávající dále prohlašuje, že je oprávněn licenci dle tohoto článku na kupujícího převést a v případě, že by se toto prohlášení ukázalo nepravdivým, zavazuje se uhradit veškeré škody či nároky osob, jimž svědčí autorská práva, za kupujícího, jakož i nahradit veškerou majetkovou i nemajetkovou újmu vzniklou přímo kupujícímu.

7.3. Smluvní strany se dohodly, že kupující není povinen licenci využít.

Čl. 8. Práva a povinnosti smluvních stran, dodací podmínky, předání a převzetí zboží

8.1. Prodávající je povinen:

8.1.1. dodat kupujícímu zboží originální, nové, nepoužité, bez vad, určené k použití v České republice a distribuované oficiální cestou od výrobce, spolu s doklady a dokumenty, které se ke zboží vztahují. Doklady a dokumenty, které se ke zboží vztahují, jsou uvedeny dále v odst. 8.2. této Smlouvy;

8.1.2. zajistit, aby dodané zboží včetně jeho balení a ochrany pro přepravu splňovalo požadavky příslušných platných ČSN;

8.1.3. zajistit aby instalaci a implementaci zboží prováděly osoby odborně kvalifikované.

8.2. Prodávající se zavazuje odevzdat zboží kupujícímu a jako nedílnou součást dodávky odevzdat doklady a dokumenty dle § 9 odst. 1 a § 10 zákona č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů, prohlášení o shodě ve smyslu zákona č. 22/1997 Sb., o technických požadavcích na výrobky, ve znění pozdějších předpisů, potvrzení o provedení příslušných revizí vyžadovaných obecně závaznými právními předpisy a technickými předpisy platnými pro daný typ zboží (je-li relevantní) a potřebnou technickou dokumentaci v českém nebo anglickém jazyce.

8.3. Nejpozději 2 (dva) pracovní dny před zahájením závozu zboží na místo plnění a zahájení jeho instalace, je prodávající povinen oznámit kupujícímu (resp. osobě oprávněné jednat ve věcech technických), telefonicky a písemně elektronickými prostředky (tj. e-mailem) datum a hodinu zahájení plnění kupujícímu tak, aby kupující mohl včas zajistit přístup pracovníků prodávajícího na místa plnění.

8.4. Nejpozději 2 (dva) pracovní dny přede dnem odevzdání zboží (odpovídajícího odst. 3.2. a 3.3., resp. Přílohám č. 1 a č. 3 této Smlouvy a ohledně něhož byly provedeny služby a práce dle odst. 3.4. této Smlouvy, tedy po dokončení implementace) je prodávající povinen oznámit kupujícímu (resp. osobě oprávněné jednat ve věcech technických), telefonicky a písemně elektronickými prostředky (tj. e-mailem) datum a hodinu zahájení odevzdání zboží kupujícímu. V případě sdělení prostřednictvím elektronické komunikace (emailu), se za dobu oznámení považuje den doručení oznámení kupujícímu na jeho e-mailovou adresu, uvedenou v čl. 1. této Smlouvy.

8.5. Prodávající je povinen předat zboží, ujednané touto Smlouvou, včetně dokladů a dokumentů dle odst. 8.2. Smlouvy a spolu s odevzdáním předloží dodací listy, ve kterých prodávající uvede počet odevzdávaného zboží, identifikaci odevzdávaného zboží, seznam dokumentů dle odst. 8.2. Smlouvy, datum a podpis osoby jednající za prodávajícího.

8.6. Kupující není povinen převzít částečné plnění nebo zboží s vadami, a to bez ohledu na povahu a množství těchto vad. Kupující rovněž není povinen převzít ty položky zboží, ke kterým nebyly dodány doklady a dokumenty dle odst. 8.2. této Smlouvy nebo dodací listy. Prodávající bere na vědomí, že odevzdání pouze části zboží nebo zboží s vadami nenaplní účel této Smlouvy.

8.7. Při odevzdání zboží bude za účasti obou smluvních stran provedena prohlídka a kontrola plné funkčnosti zboží. Po provedené prohlídce:

a) kupující zboží převezme, je-li v souladu s touto Smlouvou, nevykazuje-li zboží žádné vady, byly-li provedeny veškeré činnosti dle této Smlouvy (zejména dle odst. 3.4. této Smlouvy) a jsou-li připojeny doklady a dokumenty dle odst. 8.2. této Smlouvy, dodací listy, podepsané a datované osobou oprávněnou jednat za prodávajícího a návrh akceptačního protokolu potvrzujícího řádnou implementaci zboží. Kupující převezme zboží prostřednictvím osoby oprávněné jednat ve věcech technických, která při převzetí zboží doplní na všechny výtisky dodacího listu datum, podpis a ponechá si jeden výtisk podepsaného dodacího listu a podepíše akceptační protokol stvrzující řádné dokončení implementace a dalších služeb dle odst. 3.4. této Smlouvy, nebo

b) kupující zboží nepřevezme, pokud zboží nebude dodáno v požadovaném množství, jakosti nebo neodpovídá-li jinak podmínkám této smlouvy, nebo má-li zboží nebo jednotlivé věci vady, nebo nejsou provedeny činnosti dle odst. 3.4. této Smlouvy, nebo prodávající neodevzdá kupujícímu doklady a dokumenty, jmenovitě uvedené v odst. 8.2. této Smlouvy, a dodací listy nebo návrh akceptačního protokolu. O odmítnutí bude sepsán a podepsán oběma stranami zápis s uvedením všech důvodů nepřevzetí zboží, který je prodávající povinen podepsat.

8.8. Odmítne-li kupující důvodně převzetí zboží dle odst. 8.6. a 8.7. této Smlouvy, nepřechází na kupujícího nebezpečí škody na zboží.

8.9. Vlastnické právo a nebezpečí škody na zboží přechází na kupujícího převzetím zboží.

8.10. Prodávající se zavazuje během plnění Smlouvy i po ukončení Smlouvy, zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví od kupujícího v souvislosti s plněním Smlouvy, a to zejména, nikoliv však bezvýhradně, ve vztahu k systémové infrastruktuře kupujícího. Za porušení mlčenlivosti specifikované v této Smlouvě je prodávající povinen uhradit kupujícímu smluvní pokutu ve výši 50 000,- Kč, a to za každý jednotlivý případ porušení povinnosti. Povinností mlčenlivosti není dotčena povinnost prodávajícího dle odst. 13.7. a 13.8. této Smlouvy.

8.11. Kupující si vyhrazuje právo neodebrat všechno zboží, a to výlučně ze závažných důvodů na jeho straně (zejména nemožnost financování z plánovaných zdrojů či zásadní organizační změny). V takovém případě je povinen bezodkladně o této skutečnosti informovat prodávajícího a uhradit mu veškeré účelně vynaložené či jinak nezbytné náklady spojené s plněním této Smlouvy ohledně neodebraného zboží.

Čl. 9. Odpovědnost za vady zboží, záruka za jakost, podpora

9.1. Zboží má vady, pokud nemá vlastnosti, které stanoví Smlouva, nebo existují vady v dokladech a dokumentech dle čl. 8.2. Smlouvy nebo zboží má právní vady. Zárukou za jakost zboží se prodávající zavazuje, že zboží bude po dobu záruční doby způsobilé k použití pro účel dle této Smlouvy, jinak pro obvyklý účel, a zachová si vlastnosti a parametry vymezené touto Smlouvou.

9.2. Záruční doba záruky za jakost zboží se sjednává na dobu 24 (dvaceti čtyř) měsíců a běží od převzetí zboží kupujícím. Pokud je v technické a/nebo výrobní dokumentaci výrobce, a/ nebo na obalu zboží, v dokladech a dokumentech dodaných se zbožím uvedena kratší záruční doba, smluvní strany činí nesporným, že platí ustanovení o záruční době záruky za jakost, uvedená dle první věty tohoto odst. 9.2. Smlouvy. Pokud je naopak v technické a/nebo výrobní dokumentaci výrobce, a/ nebo na obalu zboží, v dokladech a dokumentech dodaných se zbožím uvedena delší záruční doba, smluvní strany činí nesporným, že se uplatní tato delší záruční doba.

9.3. Kupující uplatní práva z vadného plnění a/nebo právo ze záruky za jakost zboží písemným oznámením vady doručeným prodávajícímu. Oznámení vady obsahuje identifikaci druhu vadného zboží, popis vady nebo způsob, jakým se vada projevuje, a uplatnění nároku z vadného plnění nebo ze záruky.

9.4. V případě, že kupující uplatní nárok z vadného plnění nebo ze záruky na odstranění vady, je prodávající povinen odstranit vady ve lhůtě dle bodu 5 Přílohy č. 1 této Smlouvy.

9.5. Ve smyslu dikce § 1922, odst. 2 zákona č. 89/20012 Sb., občanského zákoníku smluvní strany vzaly za ujednané, že v případě uplatnění práva kupujícího z odpovědnosti prodávajícího za vady zboží vytknutím (oznámením) vady zboží vůči prodávajícímu, kteréžto zboží nemůže kupující užívat pro jeho vady, a/nebo uplatnění práva kupujícího vytknutím (oznámením) vady zboží vůči prodávajícímu, nesoucímu záruku za jakost zboží, kteréžto zboží nemůže kupující užívat pro jeho vady, neběží záruční doba ani lhůta pro uplatnění práv kupujícího z vadného plnění prodávajícího.

9.6. V případě, že prodávající neoprávněně odmítne odstranit vadu zboží jeho výměnou či opravou, nebo je v prodlení s odstraněním vady jeho výměnou či opravou, je kupující oprávněn vadu odstranit prostřednictvím třetí osoby, a to na náklady prodávajícího.

Čl. 10. Smluvní pokuty

10.1. Za prodlení prodávajícího s poskytnutím plnění v rozsahu a specifikaci dle čl. 3. této Smlouvy ve lhůtě stanovené v odst. 4.1. této Smlouvy, je prodávající povinen zaplatit kupujícímu za každý, byť započatý den prodlení smluvní pokutu ve výši 0,1 % z ceny zboží vč. DPH s jehož řádným dodáním a odevzdáním v souladu s čl. 8 této Smlouvy je prodávající v prodlení, a to až do úplného a řádného poskytnutí plnění dle této Smlouvy.

10.2. Za prodlení prodávajícího s odstraněním vad zboží ve lhůtách sjednaných v odst. 9.4. této Smlouvy je prodávající povinen zaplatit kupujícímu za každou započatou hodinu, v níž prodlení prodávajícího trvá, smluvní pokutu ve výši 1.000,- Kč.

10.3. Za nikoliv řádné (tedy nikoliv v souladu s odst. 3.4. této Smlouvy) poskytování HW nebo SW podpory, když k nápravě nedošlo ani k výtce uplatněné kupujícím vůči prodávajícímu, případně při opakovaném nikoliv řádném poskytování HW nebo SW podpory v období 3 po sobě jdoucích měsíců, je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 10.000,- Kč za každý jednotlivý zjištěný případ, a to i opakovaně.

10.4. Za nesplnění závazku dodatečných dodávek dle odst. 3.6. této Smlouvy je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 10.000,- Kč za každý jednotlivý zjištěný případ, a to i opakovaně.

10.5. Kupující uplatní nárok na smluvní pokuty uvedené v předchozích odstavcích vždy písemnou výzvou u prodávajícího. Prodávající je povinen zaplatit uplatněnou smluvní pokutu ve lhůtě uvedené ve výzvě, a není-li uvedena lhůta ve výzvě, tak do 10 (deseti) dnů od doručení této výzvy prodávajícímu. Uplatněnou smluvní pokutu, uvedenou v předchozím odstavci, zaplatí prodávající bez ohledu na to, vznikla-li kupujícímu škoda. Nárok na náhradu škody, způsobené kupujícímu, zůstává kupujícímu v plné výši zachován.

Čl. 11. Zánik Smlouvy

Smlouva zaniká vedle případů stanovených zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších právních předpisů, také:

a) dohodou smluvních stran, v jejímž obsahu je dohodnuto též vzájemné vyrovnání účelně vynaložených nákladů,

b) jednostranným odstoupením od Smlouvy kupujícím pro její podstatné porušení prodávajícím, kterým se rozumí:

- prodlení prodávajícího s poskytnutím plnění delší než 7 (sedm) kalendářních dnů,

- prodlení prodávajícího s odstraněním vady delším než 7 (sedm) kalendářních dnů.

c) výpovědí kupujícího ve vztahu k poskytování servisní podpory, a to i bez uvedení důvodu, s výpovědní dobou 3 měsíců; kupující je oprávněn podle tohoto ustanovení Smlouvu ukončit nejdříve po uplynutí 5-ti let od nabytí účinnosti této Smlouvy.

Čl. 12. Vyšší moc

12.1. Za okolnosti vylučující odpovědnost smluvních stran za prodlení s plněním smluvních závazků dle této Smlouvy (vyšší moc) jsou považovány takové překážky, které nastanou nezávisle na vůli povinné smluvní strany a brání jí ve splnění její povinnosti z této Smlouvy, jestliže nelze rozumně předpokládat, že by povinná smluvní strana takovou překážku nebo její následky odvrátila nebo překonala, a dále, že by v době vzniku smluvních závazků z této Smlouvy vznik nebo existenci těchto překážek předpokládala.

12.2. Za překážky dle odst. 12.1. této Smlouvy se výslovně považují živelní pohromy, jakákoliv embarga, občanské války, povstání, válečné konflikty, teroristické útoky, nepokoje nebo epidemie. Za živelní pohromy se zejména považují požár, úder blesku, povodeň nebo záplava, vichřice nebo krupobití, sesuv.

12.3. Za okolnost vylučující odpovědnost prodávajícího se výslovně nepovažuje jakékoliv porušení právních povinností prodávajícího, způsobené jeho dodavateli.

12.4. Nastanou-li okolnosti vylučující odpovědnost jedné ze smluvních stran, které způsobí či mohou způsobit podstatné zpoždění jakéhokoliv termínu nebo prodlení lhůty podle této Smlouvy, či zánik nebo zrušení závazků podle této Smlouvy, jsou smluvní strany povinny se neprodleně o těchto okolnostech vylučujících odpovědnost informovat a vstoupit do jednání ohledně řešení vzniklé situace. Prodávající ani kupující nejsou oprávněni takto vzniklé situace jakkoliv zneužít ve svůj prospěch a jsou povinni v dobré víře

usilovat o dosažení přijatelného řešení pro obě smluvní strany v co nejkratší době. V případě porušení této povinnosti jedné smluvní strany spolupracovat s druhou smluvní stranou, je tato smluvní strana v prodlení s plněním svých povinností dle této Smlouvy.

12.5. V případě, že nedojde k dohodě smluvních stran, termíny či lhůty plnění jednotlivých povinností podle této Smlouvy, dotčené okolností vylučující odpovědnost, se prodlužují o dobu, po kterou okolnost, vylučující odpovědnost, trvala.

12.6. Odpovědnost nevylučuje překážka, která vznikla teprve v době, kdy povinná strana byla v prodlení s plněním své povinnosti, či vznikla z jejích hospodářských poměrů.

12.7. Účinky okolnosti, vylučující odpovědnost, jsou omezeny pouze na dobu, dokud trvá příslušná překážka, s níž jsou tyto účinky spojeny.

Čl. 13. Závěrečná ustanovení

13.1. Všechny právní vztahy, které vzniknou při realizaci závazků vyplývajících z této Smlouvy, se řídí právním řádem České republiky.

13.2. Tuto Smlouvu lze měnit pouze písemným, číslovaným, oboustranně potvrzeným ujednáním, výslovně nazvaným dodatek ke Smlouvě, podepsaným statutárními orgány nebo zmocněnými zástupci obou smluvních stran. Jiné zápisy, protokoly apod. se za změnu Smlouvy nepovažují. Při jednání o jakékoliv změně této Smlouvy není odpověď smluvní strany, přijímající návrh na uzavření dodatku Smlouvy s doplněním nebo odchylkou, přijetím návrhu dodatku na jeho uzavření.

13.3. V případě změny v osobě oprávněné jednat za nebo jménem smluvní strany, zástupce kupujícího nebo prodávajícího oprávněného jednat ve věcech faktické realizace Smlouvy, nebude vyhotoven dodatek ke Smlouvě; smluvní strana, u které ke změně došlo, je povinna tuto změnu oznámit druhé smluvní straně. Účinnost změny nastává okamžikem doručení oznámení příslušné smluvní straně.

13.4 Smluvní strany sjednaly, že doručování se provádí na doručovací adresy uvedené v čl. 1. této Smlouvy. V případě, že smluvní strana odmítne doručovanou zásilku převzít, platí den odmítnutí převzetí za den doručení. V případě, že smluvní strana nevyzvedne zásilku v úložní době u držitele poštovní licence, má se za to, že zásilka byla doručena 3. (třetím) dnem od uložení a to, i když se smluvní strana o uložení nedozvěděla. Ujednání tohoto článku se nevztahují na doručování sjednané v odst. 6.2. této Smlouvy.

13.5. V případě změny sídla, místa podnikání, nebo doručovací adresy prodávajícího je prodávající povinen neprodleně tuto skutečnost oznámit kupujícímu. Pokud prodávající tuto povinnost nesplní, platí pro doručování písemností adresa uvedená v čl. 1. této Smlouvy.

13.6. Prodávající souhlasí se zveřejněním obsahu této Smlouvy podle povinností, které se na kupujícího vztahují ve smyslu ustanovení § 219 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, resp. dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Smluvní strany se dohodly, že uveřejnění Smlouvy v registru smluv zajistí kupující.

13.7. Prodávající je ve smyslu ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů (dále „ZFK“), osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů nebo z veřejné finanční podpory, tj. prodávající je povinen podle § 13 ZFK poskytnout požadované informace a dokumentaci kontrolním orgánům (Řídicímu orgánu Operačního programu Technická pomoc Ministerstva pro místní rozvoj ČR, Ministerstvu financí ČR, Evropské komisi, Evropskému účetnímu dvoru, Evropskému úřadu pro boj proti podvodům, Nejvyššímu kontrolnímu úřadu, příslušnému finančnímu úřadu a dalším oprávněným orgánům) a vytvořit kontrolním orgánům podmínky k provedení kontroly vztahující se k předmětné veřejné zakázce a poskytnout jim součinnost.

13.8. Prodávající je povinen uchovávat veškeré originální dokumenty související s realizací veřejné zakázky po dobu uvedenou v závazných právních předpisech upravujících oblast zadávání veřejných zakázek, nejméně však po dobu 10 let od finančního ukončení projektu, zároveň minimálně do roku 2031. Po tuto dobu je dodavatel povinen umožnit osobám oprávněným k výkonu kontroly projektů provést kontrolu dokladů souvisejících s realizací veřejné zakázky.

13.9. Prodávající na sebe přebírá nebezpečí změny okolností dle § 1765 odst. 2 zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

13.10. Prodávající není oprávněn převést jako postupitel svá práva a povinnosti z této Smlouvy nebo její část na třetí osobu ani jednostranně započítat svoje pohledávky proti pohledávkám kupujícího.

13.11. Smluvní strany prohlašují, že Smlouva byla uzavřena podle jejich vážné a svobodné vůle, že nebyly k jednání přinuceny pod hrozbou násilí ani lstí, Smlouvu si přečetly, považují obsah této Smlouvy za určitý a

srozumitelný, jsou jim známy veškeré skutečnosti, jež jsou pro uzavření této Smlouvy rozhodující, a na důkaz toho připojují ke Smlouvě své podpisy.

13.12. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti jejím uveřejněním v souladu s ustanovením § 6 odst. 1 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.

13.13. Smlouva je vyhotovena v elektronické podobě a podepsaná zaručenými elektronickými podpisy zástupců smluvních stran.

Čl. 14. Přílohy

Nedílnou součástí této Smlouvy jsou následující přílohy:

Příloha č. 1 – Minimální technické požadavky kupujícího na předmět plnění

Příloha č. 2 – Tabulka cen

Příloha č. 3 – Technická specifikace zboží

V Praze dne 7.2.2020 Ve Zlíně dne 18.2.2020

……

Ing. Zdeněk Vašák
generální ředitel
Centrum pro regionální rozvoj
České republiky

……..

MONET+,a.s.
Ing. Břetislav Endrys
Předseda představenstva

…….

MONET+,a.s.
Ing. Jan Vavrys
Člen představenstva

Příloha č. 1 – Minimální technické požadavky kupujícího na předmět plnění

1. Technické požadavky na karty

a) Karta a ovladače

Pro uložení elektronických certifikátů X.509 (generování / uložení příslušných kryptografických klíčů) budou dodány kontaktní čipové karty ve formátu ID-1:

- kontaktní čip na bázi GlobalPlatform/JavaCard s personalizovanou PKI aplikací
- bezkontaktní čip HID ISOProx II 26 bitů

Certifikované karty musí být v souladu:

- s normou ČSN EN ISO 7816, část 1-4 a
- standardem EN 419 211 a profily:
    - BSI-CC-PP-0059
    - BSI-CC-PP-0075
    - BSI-CC-PP-0071
    - BSI-CC-PP-0072
    - BSI-CC-PP-0076

b) Vlastnosti kontaktního čipu a PKI aplikace:

- Vytváření kvalifikovaného elektronického podpisu musí splňovat nařízení eIDAS.
- Vytváření elektronického podpisu na bázi certifikátů ve formě:
    - kvalifikovaného elektronického podpisu,
    - zaručeného elektronického podpisu,
    - uznávaného elektronického podpisu a
    - jiné formy elektronického podpisu.
- Klíče pro kvalifikovaný elektronický podpis musí být generovány v čipu.
- Všechny operace s privátním klíčem musí probíhat uvnitř čipu – klíč nesmí opustit prostředí karty.
- Privátní klíč uložený na kartě nesmí jít z karty vyexportovat.
- Klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu anebo mohou být na kartu importovány.
- Musí umožňovat uložení certifikátů různých certifikačních autorit.
- Čipová karta musí podporovat získání následného certifikátu prostřednictvím aplikace pro automatizovanou obnovu certifikátů.
- Generování RSA klíčů v čipu i import klíčů s certifikáty do čipu, ze souboru formátu PKCS#12.
- Generování a práce s RSA a ECC klíči v čipu.
- Archivaci privátních klíčů v procesech vydávání šifrovacích certifikátů.

Musí být podporovány minimálně tyto kryptografické algoritmy:

- Symetrické: 3DES, AES
- Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
- RSA: 1024, 2048 bitů
- Eliptické křivky: P-224, P-256, P-384, P-521

- Musí umožňovat zablokování PIN, QPIN resp. PUK po opakovaném chybném zadání PIN, QPIN resp. PUK.
- Podpora PIN, QPIN, PUK pro odblokování PIN a QPIN.
- Zabezpečená komunikace na bázi e-mailů (S/MIME, elektronický podpis a šifrování e-mailů).
- Dvoufaktorová autentizace na bázi certifikátů X.509 (do PC/NB v prostředí Microsoft AD, webových služeb, VPN, aplikací atd.).
- Algoritmy RSA, ECC a SHA-1,SHA-256, 384, 512

c) Ovládací software karty:

Čipové karty musí být dodány s ovládacím software, pro integraci kontaktního čipu karty do operačního systému. Vlastnosti ovládacího software:

- Musí podléhat specifikaci Microsoft Smart Card minidriver for Windows Base CSP V5.07 nebo vyšší.
- Musí mít podporu Microsoft CryptoAPI, Microsoft CNG i PKCS#11.

- Pro použití na OS MS Windows 10 nebo vyšších verzích.
- případné použití i na Linux – LTS (Long Term Support) verziae pro Ubuntu a RHEL (PKCS#11) OS X (PKCS#11).
- Možnost instalace z MSI balíčků (podpora obslužné a bezobslužné instalace), RPM, DEB.
- Distribuce ovládacího software přes službu MS Windows Update nebo MS Systém Center Configuration Manager.

d) Dodané karty musí být ve stavu:

- Inicializovaná PKI aplikace s PIN, QPIN a PUK.
- Předání seznamu personalizovaných karet, pro import do evidence. U každé karty musí být uvedeno číslo kontaktního čipu.
- Inicializovaná PKI aplikace s iniciálními hodnotami PIN, QPIN a PUK. Technickými prostředky bude vynuceno, aby si uživatel po přijetí karty změnil hodnotu PIN, kterou bude používat pro autorizaci operací kvalifikovaného podpisu.

e) Komodity pro vydání čipových karet:

Bezpečné předání PIN a PUK je v okamžiku vydání karty uživateli zabezpečeno mimo jiné s využitím PIN formuláře a distribuční obálky.

PIN formulář je požadován pro bezpečné vytištění a předání hodnot PIN a PUK uživateli. Požadované parametry PIN formuláře jsou následující:

- disponuje diskrétní zónou pro bezpečné vytištění hodnot PIN a PUK,
- obsahuje grafické instrukce pro správnou manipulaci s diskrétní zónou.

2. Technické požadavky na USB čtečky čipových karet:

USB čtečky pro práci s čipovou kartou musí splňovat minimálně následující technické parametry:

- použití čipové karty ve formátu Plug-in (SIM);
- dodané čtečky jsou po prvotním zkompletování dále nerozebíratelné;
- podpora ISO 7816 třída A, B a C; podpora ISO 7816 TA1 (až do 344 Kbds);
- čtení a zápis mikroprocesorových karet dle ISO 7816-1,2,3,4,T=0 a T=1;
- podpora USB full speed (12 Mbps);
- indikace stavu – jednobarevná LED dioda
- konektor USB typu A, garance 1500 připojení, napájení z USB portu;
- podpora PC/SC API rozhraní.

3. Požadavky na aplikace pro správu a podporu čipových karet a certifikátů:

a) Pro práci s čipovými kartami a certifikáty bude dodána aplikace, které bude mít tyto funkce:

- Centrální evidenci provozovaných karet, jejich držitelů, stavů a historie.
- Auditní stopu o bezpečnostně citlivých operacích, které byly prováděny s provozovanými kartami (např. vydání / odebrání / ztráta / nalezení karty, apod.). Auditní údaje musí obsahovat také čas provedené operace a informaci o uživateli, který danou operaci provedl či autorizoval.
- Informace o vydaných certifikátech na dané čipové kartě. V jednom systému jsou evidovány jak certifikáty vydané akreditovaným poskytovatelem, tak interní doménovou certifikační autoritou.
- Využívání doménové AD jako zdroj informací o uživatelích karet.
- Oprávnění přístupu k informacím v evidenci se opírá o uživatelské oprávnění v Active Directory. (Oprávnění přístupu do evidence karet jsou řízena na základě členství uživatelů v definovaných doménových skupinách.)
- Podpora využití integrované autentizace domény MS Windows (Single Sign On).
- Vyhledávání a prohlížení informací v evidenci karet.
- Podpora vydávání certifikátů z interní certifikační autority v doméně MS Windows. Certifikáty budou vydávány na základě definovaných šablon (certificate template). Podpora obvyklých mechanismů vydávání certifikátů v doméně, vč. archivace šifrovacích klíčů, certifikáty pro Smartcard Logon, automatické doplňování údajů do certifikátů z Active Directory.
- Podpora funkce pro import informací o nově dodaných kartách (Soubory s informacemi o kartách musí být dodány spolu s každou množinou nově dodaných karet.).
- Podpora navržených stavů životního cyklu karet a tím usnadnění úkonů pro správu karet.
- Běží na operačním systému MS Windows 10 nebo vyšších verzích; verze pro 32-bitové i 64-bitové systémy.
- Lokalizace do českého jazyka.

b) Aplikace pro práci s certifikáty - automatizovaná obnova a notifikace:

- Pro obnovu certifikátů z doménové certifikační autority a pro kvalifikovaný elektronický podpis, požaduje Zadavatel dodání aplikace, která uživateli karty pomůže provést obnovu (platného) certifikátu. Aplikace po vložení karty do čtečky, bude kontrolovat její obsah a v případě, že nalezne certifikát, jemuž se blíží konec platnosti, provede uživatele procesem obnovy certifikátu.
- Aplikace musí být schopna komunikovat po síti se systémem certifikační autority akreditovaného poskytovatele služeb, ale i s interní doménovou autoritu, minimálně pro:

    - odeslání elektronické žádosti o obnovu certifikátu;
    - detekci, zda byl na základě žádosti vydán certifikát;
    - stažení vydaného / obnoveného certifikátu.

Vlastnosti aplikace pro obnovu certifikátu:

- Impulsem pro spuštění procesu obnovy certifikátu je vložení karty do čtečky a následné přečtení obsahu karty.
- Pokud se po přečtení obsahu karty zjistí, že není třeba certifikát obnovovat, poběží aplikace výhradně na pozadí a nebude uživatele „obtěžovat“ svým grafickým rozhraním.
- Triviální grafické rozhraní, které zvládne obsluhovat i málo zkušený uživatel. Ergonomie aplikace musí nezkušeného uživatele provést celým procesem obnovy certifikátu, od vygenerování nového páru klíčů až po instalaci vydaného certifikátu.
- Předpokládá se, že žádost o obnovený certifikát bude autorizována elektronickým podpisem, vytvořeným pomocí klíčů, příslušným k dosud platnému certifikátu uživatele. Uživatel bude aktivní operace s kartou autorizovat zadáním PIN.
- Aplikace nemusí podporovat obnovu certifikátu v případech kdy:

    - Došlo k podstatné změně osobních údajů držitele certifikátu, které znemožňují použít údaje ze stávajícího certifikátu k obnově (pokud dojde k takové změně údajů, měla by aplikace informovat uživatele o nezbytnosti obnovy certifikátu na registračním místě).
    - Uživatel nemá k dispozici platný certifikát (certifikát byl odvolán nebo exspiroval).
    - Certifikační autorita odmítne vydat certifikát, z důvodů, daných interními procesy nebo certifikačními politikami.

- Pokud procesy certifikační autority neumožní provést obnovu certifikátu v jednom (synchronním) procesu, bude aplikace schopna rozložit proces obnovy na dva pod-procesy: vygenerování + odeslání žádosti, detekce + stažení + instalace vydaného certifikátu. V takovém případě musí být schopna realizovat druhou část procesu i na jiném počítači, než první část procesu (proces instalace certifikátu nesmí být pevně svázán s počítačem, na kterém byla vygenerována žádost o certifikát).
- Instalace aplikace prostřednictvím MSI balíčku, musí podporovat vzdálenou a bezobslužnou instalaci na počítače v doméně.
- Musí fungovat na klientských stanicích s operačním systémem MS Windows 10 nebo vyšším, verze pro 32-bitové i 64-bitové systémy.
- Lokalizace do českého jazyka.
- Systém musí umět uživatele i administrátora informovat o blížící se expiraci certifikátů prostřednictvím automatizovaných emailů.

4. Implementace PKI Zadavatele

Zadavatel provozuje ve své infrastruktuře bezpečnostní vrstvu vybudovanou na bázi PKI MS Windows, která je primárně určena pro vydávání infrastrukturních certifikátů.

Nově se plánuje vydávat uživatelské certifikáty na čipové karty za účelem zavedení primárně 2-faktorovou autentizace (náhrada autentizace jménem/heslem). Mimo přihlášení do PC budou z interní CA vydávány certifikáty pro přihlášení do VPN a interní elektronický podpis.

5. Servisní podpora:

Základní servis nabízeného řešení musí zahrnovat podporu po dobu 10 let ode dne podpisu předávacího protokolu (delší podpora je volitelná a Zadavatel ji nemusí využít):

- klientských komponent, které běží na Microsoftem podporovaných verzí OS Windows;
- SW centrálních modulů, které běží na Microsoftem podporovaných operačních systémech Windows Server 2012 a vyšších;

- konzultace nestandardních stavů chování dodaných SW a HW modulů proti definovanému stavu v uživatelských příručkách a zadávací dokumentaci;
- čipových karet do konce životnosti;
- čteček pro práci s čipovou kartou;
- instalovaných aplikací pro správu životního cyklu karet a certifikátů;
- Service Desk v režimu 5 x 8, jehož provozní doba musí být min. od 8:00 do 16:00 v pracovní dny;
- vzdálená podpora formou konzultací prostřednictvím definovaných komunikačních kanálů.

- Požadované reakční doby:
- potvrzení o přijetí požadavku do 2 hodin od nahlášení;
- dočasné řešení do 1 pracovního dne od přijetí požadavku;
- vyřešení požadavku do 5 pracovních dnů od dodání dočasného řešení;

Obecné informace k systému:

- Veškerá data budou uložena v centrální MS SQL databázi.
- Přístup ke správě, bude po síti přes web rozhraní, kde se bude využívat doménová infrastruktura a integrovaná autentizace MS Windows.
- Bude možné generovat reporty o kartách.

Čipová karta bude kupujícímu sloužit k následujícím činnostem:

1. Přístupová karta - ke vstupu do budovy (průchod turnikety) a pohybu po budově (otevírání dveří). Zde musí být zajištěna kompatibilita se stávajícím provozovaným přístupovým systémem ACCESS32, který je součástí balíku produktů označených INFOS a duálními bezkontaktními čtečkami karet podporující čtení bezkontaktních karet a tagů na frekvenci 125 kHz a 13,56 MHz od společnosti COMINFO, a.s. Jedná se o bezkontaktní čipové karty HID ISOProx II Embeddable s délkou 26 bit.

2. Přihlašování do PC/NB s operačním systémem Windows 10 a vyšším. Použití dvoufaktorové autentizace, která splňuje kritéria zákona o kybernetické bezpečnosti, normy ISO 27001 a 27002 a zajištění ochrany osobních údajů souvisejících s nařízením GDPR. Karta se bude vkládat přímo do slotu k tomu určenému v NB. U NB a PC kde tato možnost není, bude pořízena USB čtečka.

3. Prostředek pro uložení certifikátu pro elektronický podpis. Karty musí splňovat bezpečnostní kritéria a certifikace vyžadované aktuální legislativou a to nejen evropským nařízením eIDAS. Kontaktní čipy a aplikace nahraná do kontaktního čipu musí umožňovat správu kryptografických klíčů určených k vytváření kvalifikovaného elektronického podpisu.

4. Multifunkční zařízení - přístup k tiskům. Teprve po přiložení karty k multifunkčnímu zařízení (Zadavatel v současné době používá multifunkční zařízení značky Minolta) bude možné spustit tiskovou úlohu příslušného uživatele.

5. Průkaz státního zaměstnance / zaměstnanecký průkaz – průkaz státního zaměstnance musí splňovat požadavky Vyhlášky Ministerstva vnitra č. 388/2017 Sb.

Příloha č. 2 – Tabulka cen

Č.	Položka	Počet	Kusová cena v Kč bez DPH	Celková cena v Kč bez DPH	Celková cena v Kč s DPH
1	Hybridní čipová karta + statický potisk dle návrhu	2 000	610,00	1 220 000,00	1 476 200,00
2	Ochrané pouzdro včetně šnůrky	2 200	18,00	39 600,00	47 916,00
3	Bílý PIN formulář	2 000	11,00	22 000,00	26 620,00
4	Karta jen s bezkontaktním čipem (návštěva, úklid)	200	190,00	38 000,00	45 980,00
5	Tiskárna pro potisk karet + laminátor (oboustranný potisk karty), včetně spotřebního materiálu na potisk a laminaci 1000 ks karet oboustranně	1	160 000,00	160 000,00	193 600,00
6	Kontaktní čtečky čipových karet	510	240,00	122 400,00	148 104,00
7	Aplikace pro správu karet (potisk, vydávání, skartace, záloha CA, obnova a odvolání certifikátu, notifikace,..)	1	435 000,00	435 000,00	526 350 Kč
8	Návrh životního cyklu karet a certifikátů	1	32 000,00	32 000,00	38 720,00
9	Dodání podkladů k 2faktorové autentizaci + revize PKI	1	30 000,00	30 000,00	36 300,00
10	Implementace + školení	1	302 000,00	302 000,00	365 420,00
11	Servisní podpora 1 rok - karty, čtečky, aplikace, certfikační autorita	10	127 200,00	1 272 000,00	1 539 120 ,00
	Celkem			**3 673 000,00**	**4 444 330 ,00**

1 NABÍZENÉ ŘEŠENÍ PROID+

Centrum se rozhodlo do své organizace implementovat hybridní čipové karty. Bezkontaktní čip chtějí využívat na docházku zaměstnanců a další bezkontaktní systémy např. tiskové řešení, atd. Kontaktní čip využít pro kvalifikovaný elektronický podpis, přihlašování do PC a silnou dvoufaktorovou autentizaci. Požadují aktivovat životní cyklus karet a certifikátů. Jedná se o použití dvoufaktorové autentizace na bázi doménového certifikátu, centrální správy a evidence čipových karet a certifikátů. Dále bude zajištěna implementace PKI infrastruktury se základní dokumentací, aplikací pro správu karet, školení a následná servisní podpora.

1.1 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 – v případě Centra od 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.

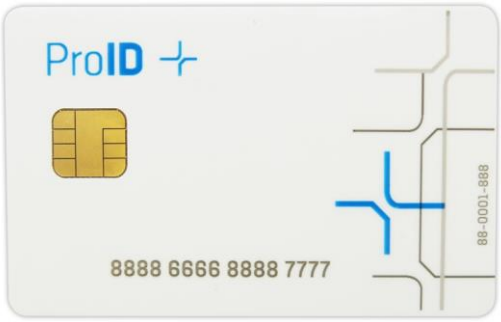
ProID+ je v souladu s Smart Card Minidriver Specification; lze jej použít v řadě aplikací, které podporují kryptografické standardy Microsoft CryptoAPI, Cryptography Next Generation, PKCS#11 nebo TokenD.

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

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

1.1.1 Formát ID-1

Jedna karta na všechno – bezpečnost, bezkontaktní čip a držitelské 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 (ilustrativní obrázek)*

Karty ve formátu ID-1 budou – kromě kontaktního čipu – osazeny také bezkontaktním čipem HID ISOPROX II s délkou 26 bit, 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).

Hybridní čipové karty budou dodány v požadovaném množství a designu dle článku 2.1.2. ze zadávací dokumentace.

Ke kartám budou dodány ochranné plastové pouzdra se šňůrkou včetně karabinky na zavěšení na krk.

Hybridní čipové karty a jejich software splňují veškeré požadavky, které jsou uvedeny v příloze č. 1 – Minimální technické požadavky kupujícího na předmět plnění.

Spolu s kartou bude uživateli předán PIN formulář s uživatelskými hodnotami PINU a PUKU.

1.2 ČTEČKY ČIPOVÝCH KARET

Čtečky karet pro formát ID- 1

- Externí čtečky (viz ukázka obrázek 2) jsou připojeny k PC přes USB.

Obrázek 2 *Externí čtečka čipových karet Gemalto IDBridge CT30*

1.3 TISKÁRNA

Nabízená tiskárna bude plně integrována s aplikací Kartové centrum ProID+. Tiskárna bude rozšířena o laminační modul, tím se zvýší odolnost potisku karty. Přes finální potisk karty je přetažena speciální laminační vrstva.

Tiskárna bude rovněž dodána se spotřebním materiálem na oboustranný potisk a laminaci 1000 ks hybridních čipových karet.

V procesu tisku bude možné vytisknout kompletní design karty nebo jen dotisk držitelských údajů.

Design karty:

- Průkaz státního zaměstnance
- Zaměstnanecký průkaz
- Karty s logem Centra a požadovaného textu, např. „Návštěva č. 1“

1.4 MANAŽER PROID+

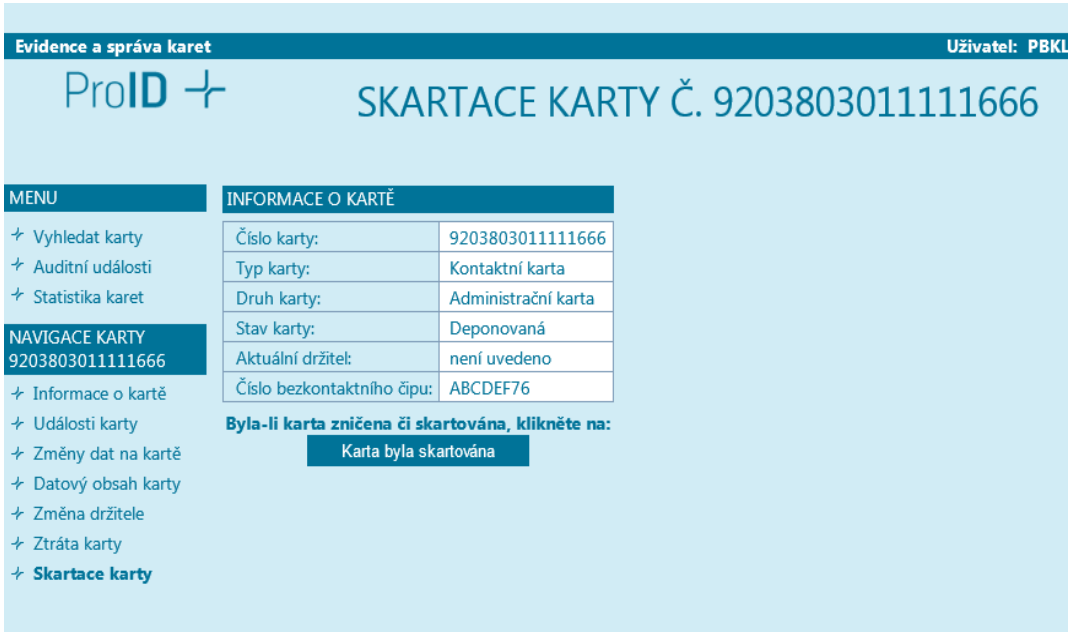
Manažer ProID+ zajišťuje snadné ovládání procesů spojených s kartami a certifikáty v organizaci. Jeho funkce jsou do organizace implementovány prostřednictvím samostatných aplikací. Následující podkapitoly popisují funkce jednotlivých aplikací.

1.4.1 Card Management System (CMS) ProID+

Pro evidenci a správu karet bude implementován 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 3 *Ukázka aplikace CMS ProID+*

Data karty

CMS eviduje kompletní informace o kartách

- identifikátor karty,
- typ karty,
- 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

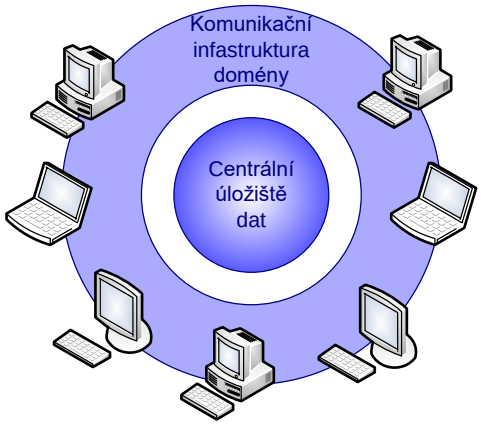
- CMS využívá doménová Active Directory jako zdroj informací o uživatelích / držitelích karet,
- CMS akceptuje nastavení doménových bezpečnostních politik,
- uživatelské role CMS jsou mapovány na doménové skupiny (domain groups),
- CMS definuje oprávnění na úrovni doménových skupin,
- CMS podporuje využití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

1.4.1.1 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 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 4 *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.

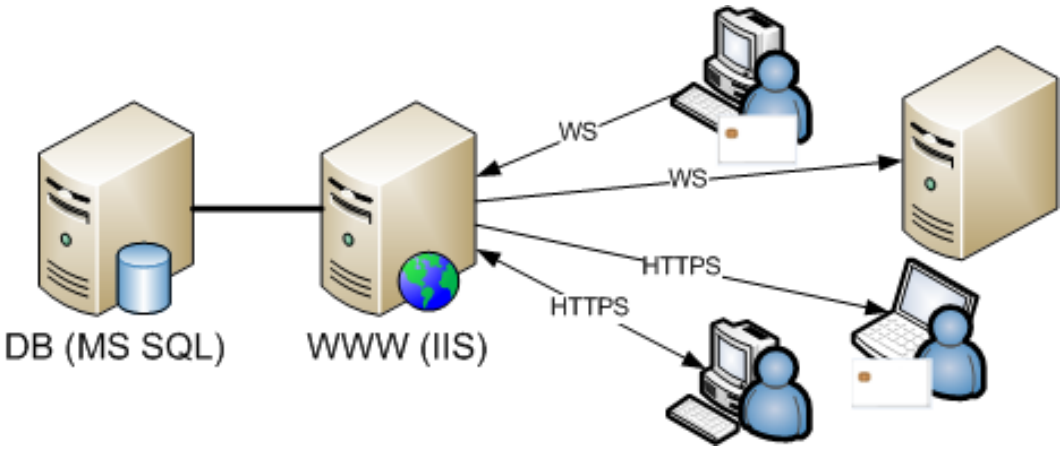
CMS také spolupracuje s dalšími moduly technologie ProID+, které pracují s čipovými kartami. Tyto moduly zasílají informace o provedených operacích do CMS. Změny stavů i informace o držitelích jsou tak automaticky promítány do centrální evidence. Díky tomu jsou údaje vždy aktuální. Centrální evidence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



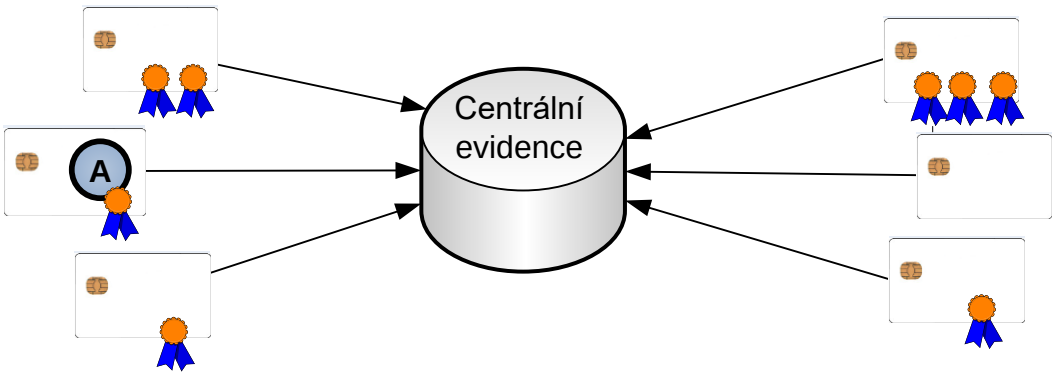
Obrázek 5 *Architektura CMS ProID+*

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 6 *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.

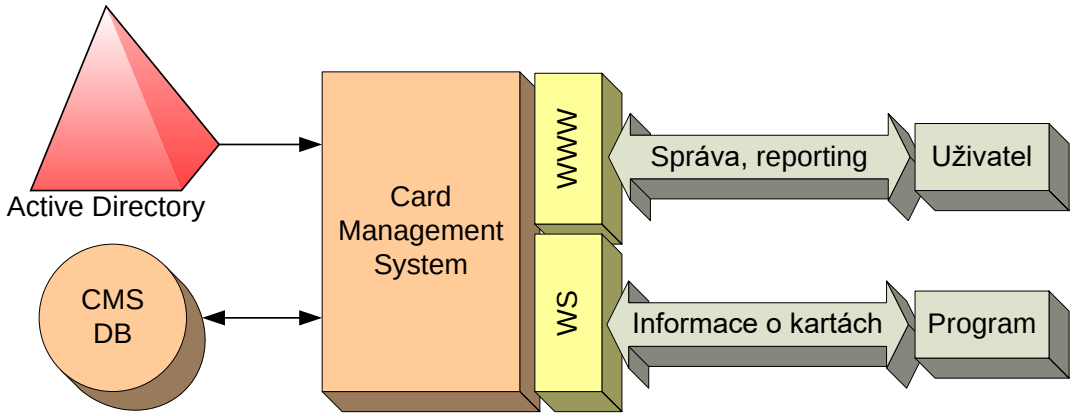
Navigace v datech CMS využívá běžných webových odkazů, menu a grafických symbolů. Ovládání webových stránek je intuitivní. Po krátkém zaškolení zvládne obsluhu stránek i méně zkušený uživatel.

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 7 *Zdroj dat o uživatelích*

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

1.4.2 Kartové centrum ProID+

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

Kartové centrum ProID+ je implementováno jako tlustý klient a je instalováno na počítači 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 uživatele a pomocí kartového centra pro něj připravuje kartu: vydává na každou kartu jeden či více doménových certifikátů (podle zvoleného „profilu“). Uživatel, který vlastní kartu, zadá hodnotu PIN a autentizuje se ke kartě. Uživatel, který obdrží novou kartu, si bude volit hodnotu PIN, QPIN a PUK. Výsledkem procesu jsou karty, připravené pro použití v doménovém prostředí, které lze distribuovat pracovníkům a ti je mohou ihned začít používat a nechat si na ně vydat certifikáty z akreditované CA. 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 doménových certifikátů, obvykle se zkrácenou dobou platnosti. Uživatel si v rámci procesu vydání karty nastaví nové hodnoty PIN QPIN a PUK. Scénář slouží pro řešení situace, kdy je třeba pracovníkovi operativně vydat kartu s doménovými 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; aplikace zároveň odvolá doménové certifikáty, evidované k vybraným kartám.
- **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.

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

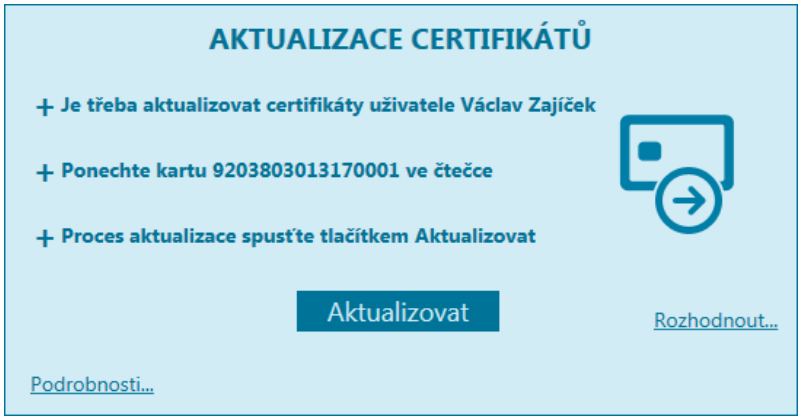
- Pro vydávání certifikátů musí být držitelem certifikátu typu enrollment agent
- Pro schvalování žádostí a odvolávání certifikátů musí mít vůči CA oprávnění Issue and Manage Certificates
- Pro čtení / zápis dat do CMS musí mít oprávnění správce karet CMS

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

1.4.3 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 8 *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.

1.4.4 SaRS

Tato komponenta má implementované standardní operace, které jsou certifikační autoritou realizovány

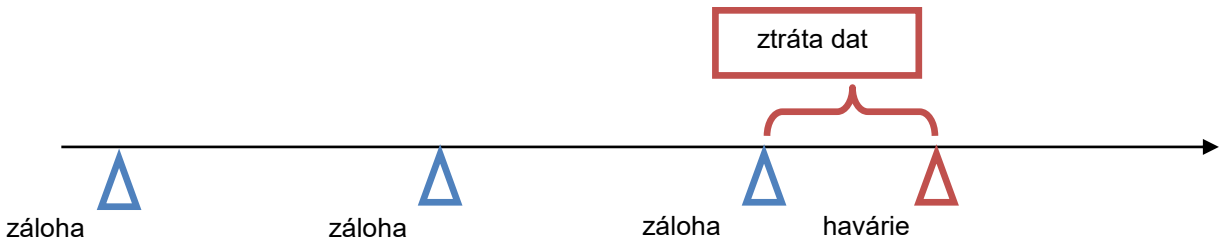
- spravuje klíče CA,
- vydává certifikáty,
- umožňuje zneplatnění certifikátů,
- vydává CRL a
- eviduje vydané certifikáty a zneplatněné certifikáty.

Pomocí nástrojů operačního systému lze také zálohovat CA tak, aby např. v případě havárie hostitelského počítače bylo možné CA obnovit a znovu-zprovoznit.

Bohužel, princip pravidelného zálohování nedokáže zabránit všem ztrátám dat při haváriích.

Jestliže dojde k havárii CA, pak všechna data vygenerovaná od poslední zálohy budou ztracena. V takovém případě může být velmi komplikované uvést CA do správného stavu

- Neví se přesně, které certifikáty byly vydány (chybějící certifikáty jsou používány, ale nelze je odvolat; CA může vydat certifikát s již použitým číslem (duplicita sériových čísel).
- Neví se přesně, které certifikáty byly zneplatněny (odvolané certifikáty jsou opět platné).
- Neví se přesně, které šifrovací klíče byly v CA zálohovány (zálohované šifrovací klíče jsou ztraceny).
- Neví se přesně, které CRL bylo vydáno.



Obrázek 9 *Nepokrytý časový úsek zálohy CA*

Právě tento typ výpadků eliminuje systém Save and Recovery System (SaRS).

Přidává k CA modul, který – v reálném čase – zapisuje do SQL databáze změny v datech CA, jako jsou

- vydání certifikátu,
- archivace šifrovacího klíče,
- zneplatnění certifikátu a
- vydání CRL.

Kromě evidence událostí jsou zaznamenávána kompletní data

- certifikáty,
- zálohované klíče a
- CRL.

Pomocí vybudované evidence lze – v případě havárie CA – provést kompletní obnovu dat CA.

Při obnově dat CA je navíc kritickým faktorem čas: CA vydává CRL na omezenou dobu platnosti. Pokud platnost CRL vyprší (a není vydáno nové CRL), jsou všechny certifikáty pokládané za nedůvěryhodné – aplikace, závislé na PKI přestanou fungovat. Pomocí systému SaRS lze obnovu dat CA významně urychlit a minimalizovat tak riziko vypršení platnosti CRL.

Použití SaRS si neklade za cíl nahradit zálohování CA, pouze doplňuje funkci, kterou pravidelné zálohování nenabízí.

Moduly SaRS

Systém SaRS se skládá z těchto modulů

- **Database Exit Module (Exit.SaRS)**
  Modul, který je integrován do procesů CA a který
  - » monitoruje činnost CA,
  - » zapisuje data CA do SaRS DB a
  - » průběžně buduje evidenci SaRS.
- **SaRS Database (SaRS DB)**
  Databázové úložiště systému SaRS. Může být hostováno v libovolné běžné relační databázi (procesy SaRS do DB přistupují přes standardní rozhraní ODBC).
- **Restore Wizard (SaRS.RW)**
  Grafická aplikace pro obnovu dat CA po havárii. Detekuje stav CA a postupně doplňuje data z evidence SaRS do CA.
  Výsledkem procesu RW je stav dat CA před výpadkem.
- **SaRS View (SaRS.View)**
  Aplikace s grafickým interface, pomocí níž lze prohlížet a konfigurovat evidenci v SaRS DB.
- **Backup synchronization (SaRS.BS)**

  Grafická aplikace, která na žádost obsluhy provede jednorázovou synchronizaci dat SQL databáze na základě dat v CA. (Např. v případě, že by Exit.SaRS nějakou dobu nebyl funkční anebo pro iniciální naplnění DB SaRS)
  - » Zkontroluje, zda jsou v SaRS DB všechna data.
  - » Chybějící data jsou do SaRS DB doplněna.
  - » Data CA zůstávají beze změny.

- **SaRS Archived Key Service (SaRSArKS)**

  Služba (service), která ukládá do SQL databáze archivované klíče, pokud je na CA aktivována separace rolí. (Při zapnuté separaci rolí není Exit.SaRS schopen z CA přečíst archivované klíče, je nutno je do SQL databáze zapisovat externí službou).

Nad databází SaRS pracují další aplikace, jako je NTFMAIL, který je popsán níže.

1.4.5 NTFMAIL

Platnost certifikátů je časově omezená. Certifikát, kterému vypršela platnost (=expiroval), je považován za neplatný a nelze ho použít v aplikacích či informačních systémech. Před vypršením platnosti je třeba vydat nový certifikát.

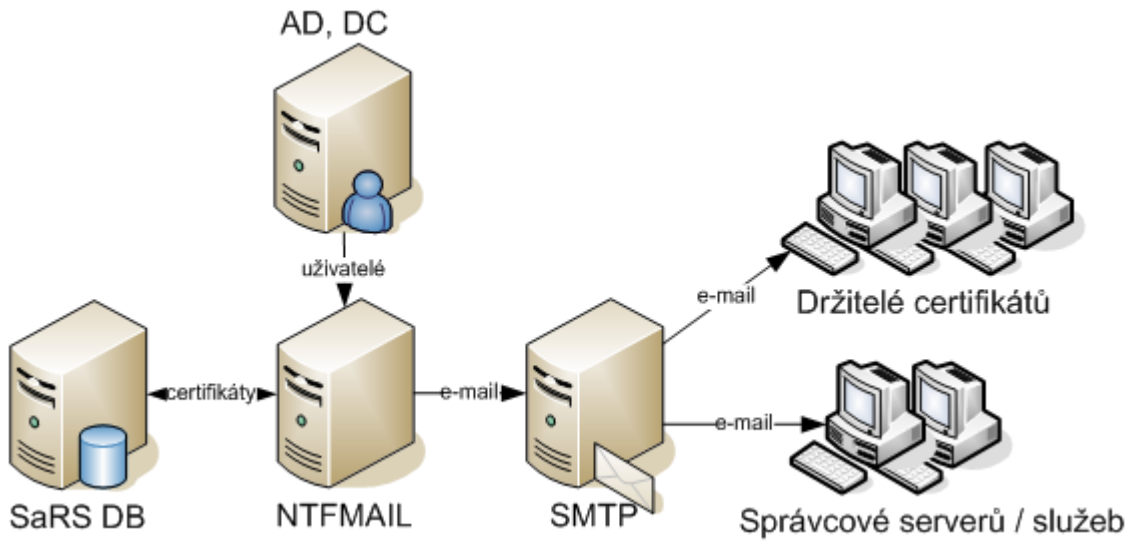
Aplikace notifikačních e-mailových zpráv (NTFMAIL) umožňuje informovat držitele certifikátů a/nebo jejich správce

- o vydání nových certifikátů nebo
- o blížícím se vypršení jejich platnosti. Držitelé si tak mohou naplánovat obnovení svých certifikátu ještě před vypršením jejich platnosti.

NTFMAIL je do prostředí implementován jako pojistka pro případ, že by aplikace ACEx z nějakého důvodu včas neobnovila certifikáty uživatele. NTFMAIL v takovém případě odešle uživateli a správcům (na sběrnou adresu) instrukce pro obnovení certifikátu. Činnost ACEx a NTFMAIL může být časově synchronizována následovně

- ACEx začne vyzývat k obnově jako první (např. 3 týdny před expirací certifikátu)
- NTFMAIL zašle e-mail, pokud si uživatel několik dní od začátku intervalu pro ACEx neobnoví certifikát. (Např. 2 týdny před expirací certifikátu.)

Architektura NTFMAIL



Obrázek 10 *Architektura NTFMAIL*

Primárním datovým úložištěm pro NTFMAIL je databáze SaRS, která slouží jako

- Zdroj informací o certifikátech (nově vydané, blížící se konec platnosti).
- Seznam již zpracovaných, resp. dosud nezpracovaných certifikátů; podle tohoto seznamu NTFMAIL eviduje, které certifikáty již byly, resp. mají být zpracovány.

Pro zjišťování informací o uživatelích slouží Active Directory.

E-mailové zprávy držitelům certifikátů odesílá NTFMAIL prostřednictvím SMTP serveru.

1.5 SLUŽBY PROID+

1.5.1 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
- Podporované stavy karet a jejich vlastnosti
- Řešení nestandardních stavů karet (zapomenutí, ztráta, zničení, ...)
- Aplikační scénáře (podklady pro konfiguraci dodávaných aplikací)

1.5.1.1 Postup zpracování návrhu životního cyklu

Zpracování návrhu životního cyklu se předpokládá následujícím způsobem:

- Před zpracováním dokumentu proběhne telekonference, kde se zástupci MONET+ dohodnou se zákazníkem na obsahu dokumentu.
- Následně vznikne dokument „Návrh životního cyklu karet“, který bude přesně popisovat dodávku pro zákazníka.
- Dokument bude předán k revizím a schválení zákazníkem v editovatelné podobě ve formátu MS Word prostřednictvím e-mailu.
- Případné vypořádání revizí a komentářů bude řešeno telekonferenčně.
- Na základě schváleného dokumentu Návrh životního cyklu karet bude provedena implementace u zákazníka

1.5.2 Doménová certifikační autorita

Centrum provozuje ve své infrastruktuře bezpečnostní vrstvu vybudovanou na bazi PKI MS Windows, která je primárně určena pro vydávání infrastrukturních certifikátů. Součástí nabídky je kontrola stavu nynějšího PKI u zadavatele. Po provedení revize bude Centru předložen dokument o zjištěném stavu a parametry, které bude potřeba dokonfigurovat v návaznosti na aktivaci hybridních čipových karet

1.5.3 Implementace aplikací pro správu karet a školení

Podkladem pro implementaci a konfiguraci aplikací budou odsouhlasené dokumenty:

- Dokument s návrhem životního cyklu
- Revizní dokument o prověření aktuálního stavu PKI
- Dokument s přehledem šablon certifikátů

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

- Vydání nové karty a doménového certifikátu
- Autentizace do domény
- Podepsání dat
- Vyhledání a přehled informací o kartě v systému CMS
- Obnova doménového certifikátu pomocí aplikace ACEx

1.5.4 Servisní podpora

Nabízená servisní podpora je nabízena v základním režimu 8 x 5 v pracovní dny. Servisní podpora začíná běžet od okamžiku předání díla po dobu 10 let.

Předmětem servisní podpory jsou

- SW moduly:
  - Kartové centrum ProID+
  - Card Management System (CMS) ProID+
  - ACEx
  - SaRS
  - NTFMail
- Dodaný HW:
  - Čipová karta ProID+
  - Čtečka čipových karet IDBridge CT30 výrobce Gemalto
  -

Základní servisní podpora nabízeného řešení ProID+ zahrnuje

- Software maintenance klientských komponent ProID+ na Microsoftem podporovaných verzích OS Windows. Přehled informací o životním cyklu Windows je k dispozici na adrese https://support.microsoft.com/cs-cz/help/13853/windows-lifecycle-fact-sheet
- Software maintenance centrálních modulů, které běží na Microsoftem podporovaných serverových operačních systémech Windows Server (aktuálně 2008 R2 a vyšších).
- Konzultace nestandardních stavů chování dodaných SW a HW modulů proti definovanému stavu v uživatelských příručkách a zadávací dokumentaci. (Včetně podpory implementace driverů čipových karet a čteček.)
- Evidence všech nahlášených incidentů objednatele.

Komunikace s oddělením podpory zhotovitele - Service Desku

- Zhotovitel provozuje podporu formou Service Desku (SD) 2. úrovně v režimu 5 x 8, jehož provozní doba je v pracovních dnech od 8:00 do 16:00. Objednatel si sám zajišťuje uživatelskou podporu 1. úrovně.
- SD poskytuje vzdálenou podporu formou konzultací prostřednictvím definovaných komunikačních kanálů.

Servisní kontakt	Dosažitelnosti (čas) v pracovní dny	Telefon	E-mail
Service Desk 2. úrovně	8.00 – 16.00	+420 739 685 921	support@monetplus.cz

Reakční doby Service Desku

- Přijetí požadavku do 2 hodin od nahlášení incidentu v rámci provozní doby SD
- Analýza nahlášeného incidentu do 1 pracovního dne od přijetí požadavku v rámci provozní doby SD.
- Odstranění chyby v SW modulech zhotovitele do 5 pracovních dnů od přijetí požadavku v rámci provozní doby SD.
- Reakční doby jsou garantovány pouze pro centrální komponenty řešení. Pro koncové stanice bude ze strany zhotovitele vyvinuto maximální úsilí pro vyřešení vzniklého incidentu. Důvodem je možné heterogenní prostředí u koncových stanic objednatele.

  Reakční doby jsou garantovány pouze v případě splnění všech definovaných požadavků na součinnost ze strany objednatele a to bez odkladu. V opačném případě se reakční doby prodlužují o dobu čekání na součinnosti.

Požadavky na součinnost

Zhotovitel může požádat o vzdálený přístup do informačního systému Objednatele pro urychlení analýzy incidentu. Objednateli nevzniká povinnost tomuto požadavku vyhovět.

V případě umožnění vzdáleného přístupu zhotovitel nemá právo jakýmkoliv způsobem vstupovat do jiných informačních systémů objednatele než do těch, které jsou předmětem plnění této Smlouvy nebo s ním bezprostředně souvisí. Dodání všech service deskem požadovaných informací ohledně nahlášeného incidentu. Může zahrnovat obrázky zachycující incidentní stav, provozní logy podporovaných modulů, či popis navození daného incidentního stavu včetně popisu prostředí, ve kterém dané moduly operují. Objednatel zajistí pracovníky s potřebným oprávněním k dotčeným systémům k provedení operací analýzy nebo odstranění incidentu.

Podpora neobsahuje

- Výjezd k zákazníkovi