

MHMP/INF/1423/2006  
9224

**Smlouva o poskytnutí služby „Řešení PKI pro čipovou kartu“  
uzavřená podle uzavřená podle § 269 odst. 2 Obchodního zákoníku č. 513/1991 Sb.,  
v platném znění  
č. objednatele INO/40/05/001121/2006  
č. zhotovitele 246/06**

Níže uvedeného dne, měsíce a roku uzavřely

**Hlavní město Praha**

se sídlem: Mariánské nám. 2/2, 110 01 Praha 1  
zastoupené: Ing. Ivanem Seyčkem, ředitelem odboru informatiky Magistrátu hl. m. Prahy  
IČ: 00064581, DIČ: CZ00064581  
Bank. spojení: PPF banka, a.s., číslo účtu: 27-5157998/6000

(dále jen „objednatel“)

a

**MONET+, a. s.**

se sídlem: Za Dvorem 505, 763 14 Zlín - Štípa  
zastoupená: Mgr. Jiřím Benešem, obchodním ředitelem, zmocněným zástupcem  
IČ: 26217783, DIČ: CZ26217783  
Bank. spojení: KB, č. ú.: 1547260257/0100

(dále jen „zhotovitel“)

**Čl. I.**

**Popis předmětu smlouvy a cíl poskytnuté služby**

1. Předmětem smlouvy je závazek zhotovitele realizovat pro objednatele službu „Řešení PKI pro čipovou kartu“ (dále jen „Služba“), a to za podmínek dohodnutých touto smlouvou a v souladu s vyhodnocením veřejné zakázky (dále jen „VZ“) uveřejněné a vyhlášené na centrální adrese dne 28.6.2006 dle zákona č. 40/2004 Sb. o veřejných zakázkách a rozhodnutí objednatele o přidělení VZ na služby ze dne 29.09.2006 č.j. MHMP/INF/1423/2006.
2. Služba bude provedena v rozsahu stanoveném touto smlouvou, jejími přílohami – příloha č. 1 - Servisní smlouva, příloha č. 2 - Licenční smlouva, které tvoří nedílnou součástí této smlouvy a zadávací dokumentací VZ.
3. **Zhotovitel realizuje Službu na vlastní odpovědnost.** Realizací části Služby může zhotovitel pověřit třetí osobu **jen se souhlasem objednatele.** Za výsledek těchto činností však odpovídá objednateli stejně jako by je provedl sám.
4. Předmětem Služby jsou níže uvedené služby a dodávky:
  - a) poskytnutí software PKI appletu a middleware (obslužného software) dle technické specifikace uvedené v příloze č. 3, která je nedílnou součástí této smlouvy, a to na nosiči v přenositelném binárním kódu odpovídajícím technické specifikaci,
  - b) dodávku technického řešení zápisu appletu na kontaktní čip karty dle technické specifikace uvedené v příloze č. 4, která je nedílnou součástí této smlouvy,

2

Za Dvorem 505, 763 14 Zlín - Štípa  
IČO: 26217783, DIČ: CZ26217783  
tel.: +420577 110411, fax: +420577 914557

- c) udělení licence k softwaru PKI appletu a middleware v počtu 50 000 a v rozsahu určeném touto smlouvou,  
d) poskytnutí podpory a údržby dodaného softwaru PKI appletu a middleware, a to v rozsahu specifikovaném přílohou č. 1, která je nedílnou součástí této smlouvy jako smlouva servisní.

## **Čl. II.**

### **Cena a platební podmínky**

**1. Cena je stanovena v členění:**

A) Cena za SW licence PKI appletu a obslužného middleware v počtu 50 000  
cena bez DPH: **9.690.000,- Kč**  
sazba DPH - 19 %, vyčíslení DPH: **1.841.100,- Kč**  
celková cena včetně DPH: **11.531.100,- Kč**  
(viz. Čl. I. odst. 4 písm. a) a písm. c))

B) Cena za technické řešení zápisu PKI appletu do čipové karty  
cena bez DPH: **4.228.700,- Kč**  
sazba DPH - 19 %, vyčíslení DPH: **800.453,- Kč**  
celková cena včetně DPH: **5.032.153,- Kč**  
(viz. Čl. I. odst. 4 písm. b))

C) Podpora a údržba dodaného softwaru PKI appletu, middleware a technického řešení zápisu PKI appletu do čipové karty (včetně poskytování upgrade po dobu trvání servisní smlouvy) v rozsahu určeném touto smlouvou  
cena za 1 měsíc podpory a údržby bez DPH: **177.699,- Kč**  
sazba DPH - 19 %, vyčíslení DPH: **33.763,- Kč**  
cena za 1 měsíc podpory a údržby včetně DPH: **211.462,- Kč**  
  
cena za 48 měsíců podpory a údržby bez DPH: **8.529.552,- Kč**  
sazba DPH - 19 %, vyčíslení DPH: **1.620.614,- Kč**  
celková cena za 48 měsíců podpory a údržby včetně DPH: **10.150.166,- Kč**

**Celková cena za plnění veškerých služeb činí:**  
cena bez DPH: **22.448.252,- Kč**  
sazba DPH - 19 %, vyčíslení DPH: **4.262.167,- Kč**  
celková cena včetně DPH: **26.713.419,- Kč**

Celková výše uvedená cena je podrobně rozepsána v Servisní a Licenční smlouvě, které tvoří přílohu č. 1 a č. 2 této smlouvy a je konečná. Celková cena jako taková zahrnuje veškeré související náklady k poskytované službě.

2. Cena uvedená v odst. 1 tohoto článku může být měněna pouze v souvislosti se změnou sazeb DPH či jiných daňových předpisů majících vliv na cenu předmětu plnění ke dni účinnosti příslušných daňových zákonů.
3. Sjednaná cena v sobě zahrnuje veškeré náklady zhotovitele za realizaci služby či dodávky dle této smlouvy včetně jejích příloh. Odměna je splatná na základě řádně vystaveného daňového dokladu (faktury) do 30 dnů od doručení objednateli. Faktura se vystavuje vždy do 15. dne následujícího měsíce po měsíci, ve kterém byla služba nebo

její poměrná část řádně dokončena nebo poskytnuta a tato skutečnost musí být potvrzena objednatelem v akceptačním protokolu.

4. Faktura musí mít náležitosti stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty v platném znění. Objednatel má právo vrátit fakturu zhotoviteli v případě, že nebude obsahovat veškeré požadované náležitosti. V takovémto případě nastává splatnost až doručením nově vystavené opravené faktury, která splňuje veškeré náležitosti. Dnem zdanitelného plnění je den podepsání akceptačního protokolu objednatelem. Dnem úhrady je den odepsání fakturované částky z účtu objednatele ve prospěch účtu zhotovitele.
5. Objednatel neposkytuje zhotoviteli žádné zálohy.
6. Nesplní-li zhotovitel jakoukoliv povinnost při plnění této smlouvy v termínu dle této smlouvy či jejích příloh v maximální 10-ti denní dodatečné lhůtě od písemné výzvy objednatele k plnění, má objednatel právo krátit smluvní odměnu až o 15% z fakturované částky.
7. Zhotovitel je povinen doručit veškeré faktury ve trojím vyhotovení na adresu objednatele, uvedenou v záhlaví smlouvy.

### **Čl. III.**

#### **Termíny plnění**

1. Zhotovitel se zavazuje realizovat služby v následujících termínech a rozsahu plnění:
  - a) dodávka appletu a middleware do: 30-dní od uzavření smlouvy
  - b) dodávka technického řešení zajištění uložení appletů na karty: 30-dní od uzavření smlouvy
  - c) poskytnutí podpory a údržby: po dobu čtyř kalendářních let od data dodávky dle 1. a) a b) v rámci tohoto článku na základě uzavření servisní smlouvy, která tvoří přílohu č. 1 a je nedílnou součástí této smlouvy.
  - d) pokud objednatel neposkytne potřebnou součinnost uvedenou v příloze č. 4 této smlouvy je zhotovitel oprávněn požadovat posun termínu plnění o dobu, po kterou nebyla součinnost poskytnuta
2. Objednatel se zavazuje předat do 10 dnů od podpisu smlouvy personalizační profil PKI appletu a customizaci middleware definované dle požadavků uvedených v příloze č. 6 této smlouvy.

### **Čl. IV.**

#### **Povinnosti zhotovitele**

1. Zhotovitel se zavazuje, že zajistí pro objednatele právo používat patenty, ochranné známky, licence, průmyslové vzory, know-how, software a práva z duševního vlastnictví nezbytně se vztahující k dílu, které jsou nutné pro provoz a využití díla. Zhotovitel je výrobcem a vykonavatelem majetkových práv předmětného software PKI appletu, middleware a technického řešení zápisu na kontaktní čip. Zhotovitel udělí objednateli licence k softwaru PKI appletu a middleware (včetně následných jejich upgradů) a dodá technické řešení pro zápis software PKI appletu do kontaktního čipu.
2. Zhotovitel se zavazuje provádět servisní služby v rozsahu stanoveném přílohou č. 1 – Servisní smlouva, která je nedílnou součástí této smlouvy.

3. Zhotovitel se zavazuje, že po celou dobu plnění smlouvy bude mít uzavřenu pojistnou smlouvu na škody způsobené při výkonu podnikatelské činnosti, a to na minimální pojistné plnění 10 mil. Kč. Ověřená fotokopie pojistné smlouvy tvoří přílohu č. 5 této smlouvy o dílo a je její nedílnou součástí.

#### **Čl. V.**

##### **Ochrana důvěrných informací**

1. Smluvní strany se zavazují, že pro jiné účely, než je plnění předmětu této smlouvy a jednání směřující k plnění povinností a výkonu práv vyplývajících z této smlouvy, jiné osobě nesdělí, nezpřístupní, pro sebe nebo pro jiného nevyužijí obchodní tajemství druhé smluvní strany, o němž se dověděly nebo doví tak, že jim bylo nebo bude svěřeno nebo se jim stalo jinak přístupným v souvislosti s plněním této smlouvy, obchodním či jiným jednáním, které spolu vedly nebo povedou.
2. Obchodním tajemstvím se pro účely této smlouvy rozumí veškeré skutečnosti obchodní, výrobní či technické povahy související s činností smluvních stran, zejména veškerá průmyslová práva a know-how, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu, nejsou v obchodních kruzích běžně dostupné a mají být podle vůle smluvních stran utajeny.
3. Smluvní strany se zavazují, že ke skutečnostem, tvořícím obchodní tajemství, umožní přístup pouze pracovníkům a osobám, které se smluvně zavázaly mlčenlivostí o skutečnostech tvořících obchodní tajemství.
4. Smluvní strany jsou povinny zachovávat obchodní tajemství i po skončení tohoto smluvního vztahu po dobu, po kterou trvají skutečnosti obchodní tajemství tvořící.
5. Smluvní strany se zavazují, že informace získané od druhé smluvní strany nebo při spolupráci s ní nevyužijí k vlastní výdělečné činnosti a ani neumožní, aby je k výdělečné činnosti využila třetí osoba.

#### **Čl. VI.**

##### **Smluvní pokuty**

1. Za každé jednotlivé prokazatelné porušení povinností uvedených v článku V. odst. 1), 3), 4), 5) této smlouvy je zhotovitel povinen zaplatit smluvní pokutu ve výši 500.000,- Kč (slovy: pět-set-tisíc-korun českých.)
2. Uplatněním smluvní pokuty není vyloučeno právo objednatele na uplatnění náhrady škody v plném rozsahu.

#### **Čl. VII.**

##### **Předčasné ukončení smlouvy**

1. Tato smlouva může být předčasně ukončena pouze písemnou dohodou podepsanou oprávněnými zástupci obou smluvních stran, výpovědí objednatele se sjednanou měsíční výpovědní lhůtou, která počíná běžet prvním dnem měsíce následujícího po doručení výpovědi nebo odstoupením od smlouvy jednou ze smluvních stran dle tohoto článku.
2. Obě smluvní strany jsou od této smlouvy oprávněny odstoupit v případě, že druhá smluvní strana podstatným způsobem poruší svoje smluvní povinnosti. Odstoupení musí být provedeno písemným oznámením adresovaným smluvní straně, která podstatně

- porušuje smluvní povinnosti, učiněným bez zbytečného odkladu poté, kdy se o tomto porušení odstupující smluvní strana dověděla.
3. Za podstatné porušení smluvní povinnosti se pro účely této smlouvy považuje zejména:
    - a) neodstranění vad a právních vad ze strany zhotovitele, a to ani po uplynutí přiměřené dodatečné lhůty poskytnuté objednatelem,
    - b) jestliže realizovaná služba nebude min. po dobu šesti měsíců odpovídat specifikacím výslovně uvedeným v ZD,
    - c) porušování osobnostních autorských práv nebo zákonných ustanovení ze strany zhotovitele.
  4. Odstoupením od smlouvy zanikají všechna práva a povinnosti smluvních stran z této smlouvy. Strany sjednávají účinky odstoupení ex nunc, smlouva je tak ukončena s účinky od doručení odstoupení druhé smluvní straně. Odstoupení od smlouvy se nedotýká nároku na náhradu škody, ani nároků na smluvní pokuty, tyto mají podle vůle smluvních stran zůstat zachovány i v případě odstoupení od smlouvy.
  5. V případě předčasného ukončení této smlouvy se obě strany zavazují, že vypořádají své vzájemné závazky na základě dohody s ohledem na rozpracovanost díla.

#### **Čl. VIII.** **Právní vady Služby**

1. Dodávka, která je součástí poskytnuté Služby má právní vady, jestliže je zatížena právem třetí osoby.
2. Služba má právní vady i v případě, kdy právo třetí osoby vyplývá z průmyslového nebo jiného duševního vlastnictví, které nepožívá právní ochrany podle právního řádu státu, na jehož území má sídlo nebo podniká objednatel, popřípadě zhotovitel, nebo na jehož území má být Služba realizována.
3. Nárok z právních vad nevzniká pouze v případě, jestliže zadavatel o právu třetí osoby věděl v době uzavření smlouvy a s tímto omezením vyslovil předem písemný souhlas.
4. Zhotovitel je povinen na vlastní náklady učinit všechna opatření nezbytná k odstranění právní vady Služby. Zhotovitel nese veškeré náklady a hradí veškeré oprávněné nároky třetích osob.

#### **Čl. IX.** **Vady Služby**

1. Služba má vady, jestliže její provedení neodpovídá výsledku určenému ve smlouvě a schválenému v předávacích protokolech.
2. Zhotovitel odpovídá za vady, jež má Služba v době jeho předání. Za vady Služby, na něž se vztahuje záruka za jakost, odpovídá zhotovitel v rozsahu této záruky.
3. Zhotovitel odpovídá za vady Služby vzniklé po době uvedené v odstavci 2 tohoto článku, jestliže byly způsobeny prokazatelně porušením jeho povinností.
4. Zhotovitel je povinen předat Službu v provedení, které je stanoveno v této smlouvě.
5. Není-li v této smlouvě dostatečně přesně stanoven způsob provedení Služby, je zhotovitel povinen předat Službu v provedení, jež se hodí pro účel, k němuž se taková Služba zpravidla užívá nebo pro účel, k němuž chce Službu užívat objednatel.
6. Jestliže zhotovitel předá Službu se souhlasem objednatele před dobou stanovenou pro její předání, může až do této doby předat chybějící část nebo předat náhradní Službu za

předanou vadnou Službu nebo vady předané Služby opravit v pouze v případě, že tímto nebude narušena koordinace mezi ostatními dodavateli částí veřejné zakázky.

7. Zhotovitel se své odpovědnosti zproští, prokáže-li, že vada má původ nebo vznikla v důsledku poskytnutí nesprávných informací objednatele nebo neoprávněným zásahem objednatele popřípadě třetí osobou do softwaru, hardwaru či systémového prostředí. Na případnou nevhodnost pokynů je zhotovitel povinen objednatele upozornit. Objednatel se zavazuje poskytnout zhotoviteli při zjišťování původu vady potřebnou součinnost.
8. Nezproští-li se zhotovitel odpovědnosti, odstraní zjištěnou vadu na své náklady.
9. Způsob hlášení vad zhotoviteli, kategorizace vad a doba reakce zhotovitele na vady, postup při odstraňování a následná opatření jsou stanovena v **příloze č.1** této smlouvy.

## **Čl. X.**

### **Záruka za jakost**

1. Zhotovitel odpovídá - ručí za jakost poskytnuté služby a dodávek, které mohou být součástí jím poskytnuté Služby. Tím se pro účely této smlouvy rozumí závazek uchazeče, že realizovaná služba popř. dodávka bude po celou záruční dobu způsobilá pro použití ke smluvenému účelu, jinak k obvyklému účelu, a že si zachová smluvené, jinak obvyklé vlastnosti.
2. Obě smluvní strany se dohodly, že v tomto případě činí záruční doba 2 roky tj. 24 měsíců. Po tuto dobu bude zhotovitel vykonávat pro objednatele bezplatný záruční servis, pokud touto smlouvou není stanoveno jinak.
3. Záruční doba k jednotlivým částem plnění počíná běžet dnem podepsání příslušného akceptačního protokolu o dokončení jednotlivých částí poskytnuté Služby v rozsahu a dle termínů stanovených touto smlouvou včetně jejích dodatků.
4. Povinnosti zhotovitele vyplývající z předchozích ustanovení o záruce se nevztahují pouze na provedení údržby, opravy nebo výměnu způsobenou výhradně:
  - a) v případě živelných pohrom, jako např. požár způsobený úderem blesku, povodeň atd.,
  - b) opravou nebo servisním zásahem provedeným jinou osobou než osobou určenou zhotovitelem,
  - c) násilným poškozením.
5. Závady je objednatel oprávněn nahlásit faxem, telefonem nebo písemně. Závada se považuje za nahlášenou v okamžiku, kdy zhotovitel výslovně potvrdí přijetí jejího oznámení. Zhotovitel je povinen potvrdit nahlášení závady do 16 hodin. V případě, že tak neučiní, je nahlášení závady považováno za potvrzené. Závady, budou odstraňovány v souladu s touto smlouvou nebo jejími přílohami.
6. Kontakty pro nahlášení závady jsou následující:  
Ing. Martin Langer,  
Mgr. Petr Sklenář  
telefonní číslo: +420 577 110 454  
faxové číslo: +420 577 110 557  
e-mailová adresa: [support@cryptoplus.cz](mailto:support@cryptoplus.cz)
7. Zhotovitel umožní objednateli využívat telefonní konzultační linku v pracovní dny od 8:00 do 17:00 hodin na telefonním čísle +420 577 110 454.
8. Zhotovitel ručí po dobu platnosti této smlouvy za to, že média (datové nosiče) nebudou při běžném používání vykazovat materiálové a výrobní vady. Pokud k takovéto vadě dojde, zhotovitel neprodleně nahradí vadná média (datové nosiče) bezvadnými.

9. Pokud se během instalace nebo provozu předmětného systému zjistí, že předmětný software nesplňuje technické předpoklady prezentované při testování software a deklarované v technické dokumentaci, potom objednatel poskytne písemnou výzvou zhotoviteli dodatečnou lhůtu 7 dnů od doručení písemné výzvy pro odstranění takovýchto nesrovnalostí. Jestliže zhotovitel neodstraní závady ani v této lhůtě, potom je objednatel oprávněn od této smlouvy odstoupit.

## **Čl. XI.**

### **Nároky z právních a jiných vad Služby**

1. Zhotovitel je povinen realizovat Službu bez právních nebo jiných vad.
2. V případě, že Služba realizovaná zhotovitelem bude vykazovat vady, může objednatel:
  - a) požadovat odstranění vad předáním náhradního plnění za plnění vadné a požadovat odstranění právních vad,
  - b) požadovat odstranění vad, jestliže vady jsou opravitelné, nebo
  - c) požadovat přiměřenou slevu z ceny za poskytnuté služby, případně dodávky.
3. Neodstraní-li zhotovitel vady v přiměřené dodatečné lhůtě nebo oznámí-li před jejím uplynutím, že vady neodstraní, může zadavatel odstoupit od smlouvy nebo požadovat přiměřenou slevu z ceny za poskytnuté plnění.
4. Nárok na slevu z ceny za služby a dodávky, které jsou jejich součástí odpovídá rozdílu mezi hodnotou, kterou by měla realizovaná služba nebo dodávka bez vad, a hodnotou, kterou měla služba nebo dodávka provedená s vadami, přičemž pro určení hodnot je rozhodující doba, v níž se mělo uskutečnit řádné plnění.
5. Do doby odstranění vad není zadavatel povinen platit část ceny za poskytnuté služby nebo dodávky, která by odpovídala jeho nároku na slevu, jestliže by vady nebyly odstraněny.
6. Nároky z vad realizované služby nebo dodávky se nedotýkají nároku na náhradu škody nebo na smluvní pokutu.

## **Čl. XII.**

### **Další ujednání**

1. Veškerá korespondence a dokumenty budou v rámci plnění předmětu smlouvy předávány osobně, faxem, nebo poštou doporučenou zásilkou. Písemnosti odeslané faxem musí být následně v nejbližší pracovní den odeslány doporučenou poštou. Písemnosti zaslané e-mailem budou považovány za doručené, jen pokud adresát výslovně potvrdí jejich přijetí rovněž e-mailem. Automatické potvrzení o doručení/přečtení zprávy zasílané bez zásahu uživatele příslušným počítačovým programem se za potvrzení přijetí zprávy nepokládá. V případě ohlašování vad, se za řádně nahlášenou vadu považuje rovněž vada, která byla nahlášena telefonicky na kontaktních číslech uvedených v této smlouvě.
2. Korespondence odeslaná doporučenou zásilkou se doručuje na adresu účastníka uvedenou v této smlouvě. Pokud v průběhu plnění této smlouvy dojde ke změně adresy některého z účastníků, je povinen tento účastník změnu do 10 dnů písemně oznámit. Nebyl-li adresát na uvedené adrese zastížen, písemnost se prostřednictvím poštovního doručovatele uloží na poště. Nevyzvedne-li si účastník zásilku do deseti kalendářních dnů od uložení, považuje se poslední den této lhůty za den doručení, i když se účastník o doručení nedozvěděl.

3. Veškeré smluvní pokuty dle této smlouvy jsou splatné do 10 dnů od doručení písemné výzvy k jejímu uhrazení smluvní straně, která odpovídající smluvní povinnost porušila, a budou uhrazeny bezhotovostním převodem na bankovní účet oprávněné smluvní strany uvedený v záhlaví této smlouvy. Nárok na uhrazení smluvní pokuty se nedotýká nároku na náhradu škody způsobené porušením povinností a tato náhrada škody se hradí v plné výši bez ohledu na výši smluvní pokuty.
4. Každá ze stran této smlouvy odpovídá druhé straně za škodu vzniklou porušením povinností vyplývajících z této smlouvy, nebo zaviněným porušením právních předpisů. Odpovědnosti se strana zproští, jestliže byla škoda způsobena objektivně neodvratitelnou událostí, které nemohlo být zabráněno ani při vynaložení veškerého úsilí, které lze požadovat za daných podmínek konkrétního případu (vyšší moc).

### Čl. XIII. Závěrečná ustanovení

1. Právní vztahy vzniklé z této smlouvy nebo s touto smlouvou související se řídí, pokud z této smlouvy nevyplývá něco jiného, zejména ustanoveními obchodního zákoníku a dalšími právními předpisy. V případě, že by se stalo některé ustanovení smlouvy neplatným, zůstávají ostatní ustanovení i nadále v platnosti, ledaže právní předpis stanoví jinak. Práva a povinnosti smluvních stran z této smlouvy přecházejí na jejich právní nástupce.
2. Osoby odpovědné jednat za objednatele:  
ve věcech technických: Ing. Jiří Chytil, tel. 236002676  
email: [Jiri.Chytil@cityofprague.cz](mailto:Jiri.Chytil@cityofprague.cz)  
ve věcech smluvních: Ing. Ivan Seyček, tel. 236002804 ,  
email: [Ivan.Seycek@cityofprague.cz](mailto:Ivan.Seycek@cityofprague.cz)
3. Osoby odpovědné jednat za zhotovitele  
ve věcech technických: Mgr. Jiří Kutálek, tel. +420 577 110 411  
email: [jiri.kutalek@monetplus.cz](mailto:jiri.kutalek@monetplus.cz)  
ve věcech smluvních: Ing. Vladimír Záhorec, tel. +420 577 110 411  
email: [vladimir.zahorec@monetplus.cz](mailto:vladimir.zahorec@monetplus.cz)
4. Tuto smlouvu lze měnit, doplňovat nebo rušit pouze písemně, a to číslovanými dodatky, podepsanými oběma smluvními stranami.
5. Smluvní strany se dohodly, že žádná z nich není oprávněna postoupit svá práva a povinnosti, vyplývající z této smlouvy bez předchozího písemného souhlasu druhé smluvní strany, s výjimkou peněžitých pohledávek za druhou smluvní stranou.
6. Smluvní strany se zároveň zavazují, že všechny informace, které jim byly svěřeny druhou smluvní stranou, nezpřístupní třetím osobám pro jiné účely, než pro plnění závazků stanovených touto smlouvou.
7. Tato smlouva spolu se všemi přílohami a případnými dodatky představuje kompletní a úplná ujednání mezi smluvními stranami a nahrazuje všechny dosavadní smlouvy, dohody a ujednání, vztahující se k předmětu této smlouvy, která byla v minulosti učiněna v písemné, popřípadě ústní formě.
8. Smluvní strany výslovně souhlasí s tím, aby tato smlouva byla uvedena v Centrální evidenci smluv ( CES ), která je veřejně přístupná a která obsahuje údaje o číselném označení smlouvy a data jejího podpisu, údaje o smluvních stranách a předmětu smlouvy. Smluvní strany prohlašují, že skutečnosti uvedené v této smlouvě nepovažují za obchodní tajemství ve smyslu § 17 obchodního zákoníku a udělují svolení k jejich užití a zveřejnění bez stanovení jakýchkoli dalších podmínek.



9. Zhotovitel je povinen nakládat se všemi daty poskytnutými objednatelem ke zpracování jako s informacemi důvěrnými. Budou-li data poskytnutá objednatelem podléhat režimu zvláštní ochrany podle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, jsou obě smluvní strany povinny zabezpečit splnění všech ohlašovacích povinností, které citovaný zákon vyžaduje, a obstarat předepsaná povolení. Bude-li nezbytné pro plnění této smlouvy splnit ohlašovací povinnosti dle cit. zákona, realizace předmětu plnění se pozastavuje na dobu do řádného splnění takových povinností a obě smluvní strany se zavazují vyvinout veškerou součinnost ke splnění těchto ohlašovacích povinností. Zhotovitel se zavazuje, že pokud se v souvislosti s realizací předmětu této smlouvy při plnění svých povinností setkají jeho pověřeni pracovníci s osobními údaji ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, učiní veškerá opatření, kromě zachování povinnosti mlčenlivosti dle tohoto odstavce, aby nedošlo k neoprávněnému nebo nahodilému přístupu k těmto údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jejich jinému zneužití. Zhotovitel nese plnou odpovědnost za případné porušení této povinnosti.
10. Tato smlouva je vyhotovena v pěti stejnopisech, z nichž každý stejnopis má platnost originálu. Zhotovitel obdrží jeden stejnopis a objednatel čtyři stejnopisy.
11. Smlouva nabývá platnosti a účinnosti dnem podpisu smluvními stranami.
12. Smluvní strany tímto prohlašují, že neexistuje žádné ústní ujednání, žádná smlouva či řízení týkající se některé smluvní strany, které by nepříznivě ovlivnilo splnění závazků vyplývajících z této smlouvy. Zároveň svým podpisem potvrzují, že veškerá prohlášení a dokumenty podle této smlouvy jsou pravdivé, úplné, přesné, platné a právně vynutitelné.
13. Smluvní strany dále prohlašují, že si smlouvu, včetně jejích příloh pečlivě přečetly, všem ustanovením smlouvy rozumí a na důkaz svého souhlasu učiněného vážně a svobodně smlouvu vlastnoručně podepisují.
14. Nedílnou součástí této smlouvy jsou tyto přílohy:

- Příloha č. 1 - Servisní smlouva  
Příloha č. 2 - Licenční smlouva  
Příloha č. 3 - Technická specifikace PKI appletu a obslužného software (middleware)  
Příloha č. 4 - Technická specifikace řešení zápisu appletu na kontaktní čip  
Příloha č. 5 - Fotokopie pojistné smlouvy  
Příloha č. 6 - Personalizační profil PKI appletu a customizace middleware  
Příloha č. 7 - Plná moc

V Praze dne 25. října 2006

Ve Zlíně, dne: 25.10.2006

*Objednatel*

Objednatel



*Zhotovitel*

Zhotovitel

**MONET+, a.s.** 

Za Dvorem 505, 763 14 Zlín - Štípa  
IČO: 26217783, DIČ: CZ26217783  
tel.: ++420 577 110 411, fax: ++420 577 914 557

**Příloha č. 1 Servisní smlouva**  
ke smlouvě „Smlouva o poskytnutí služby „Řešení PKI pro čipovou kartu“  
objednatele INO/40/05/001121/2006, č. zhotovitele 246/06

Níže uvedeného dne, měsíce a roku uzavřely

**HLAVNÍ MĚSTO PRAHA**

se sídlem: Mariánské nám. 2/2, 110 01 Praha 1  
zastoupené: Ing. Ivanem Seyčkem, ředitelem odboru informatiky Magistrátu hl. m. Prahy  
IČ: 00064581, DIČ: CZ00064581  
Bank. spojení: PPF banka, a.s., číslo účtu: 27-5157998/6000

(dále jen „objednatel“)

a

**MONET+, a. s.**

se sídlem: Za Dvorem 505, 763 14 Zlín - Štípa  
zastoupená: Mgr. Jiřím Benešem, obchodním ředitelem, zplnomocněným k podpisu  
IČ: 26217783, DIČ: CZ26217783  
Bank. spojení: KB, č. ú.: 1547260257/0100

(dále jen „zhotovitel“)

tuto

**Servisní smlouvu**

která tvoří přílohu č. 1 ke smlouvě „o Poskytnutí služby „Řešení PKI pro čipovou kartu““ č.  
smlouvy č. objednatel INO/40/05/001121/2006, č. zhotovitele 246/06  
č. objednatel INO/40/05/001122/2006, č. zhotovitele S246/06

**Čl. I.**

**Předmět smlouvy**

Předmětem smlouvy je závazek zhotovitele za podmínek dohodnutých touto smlouvou a v souladu se zadávací dokumentací, poskytnout objednateli podporu a údržbu dodaného softwaru PKI appletu, middleware a technického řešení zápisu appletu do kontaktního čipu to v rozsahu specifikovaném v příloze č.1 smlouvy o poskytnutí služby „Řešení PKI pro čipovou kartu“, jejíž je tato Servisní smlouva přílohou.

## **Čl. II.**

### **Cena**

1. Cena za poskytnutí služeb je stanovena v rozsahu stanoveném smlouvou „o Poskytnutí služby „Řešení PKI pro čipovou kartu“, jejíž je tato Servisní smlouva přílohou.
2. Součástí dohodnuté ceny jsou veškeré služby a veškeré náklady na služby poskytované dle této smlouvy, podrobně specifikované v technické specifikaci služeb v příloze č. 2 této Servisní smlouvy.

## **Čl. III.**

### **Platební podmínky**

Cena za poskytování služeb bude zhotovitelem fakturována měsíčně dle smlouvy „o Poskytnutí služby „Řešení PKI pro čipovou kartu“, jejíž je tato Servisní smlouva přílohou.

## **Čl. IV.**

### **Plnění**

1. Zhotovitel bude zajišťovat plnou podporu pro objednatele při údržbě, rozšiřování a doplňování dodaných softwarových a hardwarových částí po dobu 4 let od dodání PKI appletu a dalších částí od doby od zahájení plnění, dle podmínek uvedených v příloze č. 1 Servisní smlouvy, a to svými pracovníky v pracovních dnech od 8 hodin do 17 hodin.
2. Podrobný rozpis plnění je přílohou č. 2 této Servisní smlouvy včetně dalších technických podmínek jeho poskytování.
3. Zhotovitel je povinen proškolit pracovníky a další osoby zajišťující poskytování služeb dle této smlouvy v oblasti bezpečnosti práce a požárních předpisů.
4. Pracovníci jsou povinni se seznámit s pravidly užívání prostorů MHMP a tyto dodržovat.

## **Čl. V.**

### **Rozsah servisních služeb**

1. Zhotovitel zajistí poskytování služeb help-desku v souladu se specifikací v rámci přílohy č. 2 této servisní smlouvy.
2. Zhotovitel bude provádět upgrade poskytnutého SW v souladu s přílohou č. 2 této servisní smlouvy.

## **Čl. VI.**

### **Nahlašování poruch a konzultace**

1. Technické závady dodaného software ohlašuje objednatel do 15-dnů od jejich zjištění:  
a) Telefonem: +420 577 110 411;  
Faxem: +420 577 914 557;  
Emailem: support@cryptoplus.cz. - příjem 24 hodin denně,

b) osobním předáním zprávy o závadě, při které zhotovitel písemně potvrdí datum a čas předání

Kontaktní osoby:

Ing. Martin Langer, Mgr. Petr Sklenář

2. Hlášení chybového stavu bude obsahovat tyto údaje: v mimopracovní době informaci o zajištění přístupu, jméno, příjmení a aktuální kontakt na osobu objednatele, která je oprávněná jednat se zhotovitelem ve věcech týkajících se poskytování služeb, jméno, příjmení a aktuální spojení na nahlášující osobu, přibližný popis chybového stavu.
3. Zhotovitel umožní telefonické konzultační a poradenské služby týkající se běžných provozních záležitostí v době od 8-17 hodin.

## **Čl. VII.**

### **Servisní doba**

1. Servis je prováděn v pracovních dnech pondělí - pátek od 8 do 17 hodin.
2. Zhotovitel se zavazuje zahájit odstranění akutního chybového stavu výrazně degradující kvalitu poskytovaných služeb nejpozději do 24 hodin od nahlášení chybového stavu, provedeného objednatelem dle dohodnutého způsobu. Akutním chybovým stavem jsou závady ústředí bezprostředně ohrožující provoz dodaného software.
3. Zhotovitel je povinen odstranit ostatní chybové stavy, které nejsou specifikovány v předchozím bodě jako akutní, nejpozději do 72 hodin od nahlášení chybového stavu, provedeného objednatelem dle dohodnutého způsobu.
4. Výše uvedené reakční doby se zhotovitel zavazuje plnit v případě, že jsou dodrženy podmínky stanovené v příloze č. 1 této servisní smlouvy.

## **Čl. VIII.**

### **Práva a povinnosti objednatele**

1. Objednatel se zavazuje zpřístupnit prostory pro účely servisních zásahů, popř. úprav informačního systému, po vzájemné dohodě i v mimopracovní dobu.
2. Objednatel je povinen informovat zhotovitele o změnách ve vnitřních předpisech pro správu informačního systému písemně a s nejméně 20 denním předstihem, než pravidla vstoupí v platnost.
3. Objednatel se zavazuje poskytnout zhotoviteli potřebné podklady, odborné konzultace a potřebnou součinnost k plnění předmětu této smlouvy.
4. Objednatel se zavazuje, že bude využívat materiály a analýzy spojené s plněním předmětu smlouvy pouze pro své interní potřeby a neposkytne je jako celek nebo jeho část třetí straně bez písemného souhlasu zhotovitele.

## **Čl. IX.**

### **Smluvní pokuta**

1. Nesplní-li zhotovitel jakoukoliv svoji povinnost při plnění předmětu smlouvy (poskytování servisu) v dohodnutém termínu, zaplatí zhotovitel objednateli smluvní pokutu ve výši 5 000,- Kč za každý den prodlení.

Nesplní-li zhotovitel jakoukoliv svoji povinnost při plnění této servisní smlouvy v maximálně 10-ti denní dodatečné lhůtě od písemně oznámené výzvy k plnění, zaplatí objednateli smluvní pokutu ve výši 15% z ceny plnění.

3. Objednatel je oprávněn smluvní pokutu, případně náhradu škody, na které mu v důsledku porušení závazku zhotovitele vznikl právní nárok, započíst do kterékoliv úhrady, která přísluší zhotoviteli dle příslušných ustanovení smlouvy.
4. Smluvní pokuta je splatná do 15-ti kalendářních dnů od okamžiku každého jednotlivého porušení této smlouvy.
5. Veškeré smluvní pokuty dle této smlouvy budou uhrazeny bezhotovostním převodem na bankovní účet oprávněné smluvní strany uvedený v záhlaví této smlouvy. Nárok na uhrazení smluvní pokuty se nedotýká nároku na náhradu škody způsobené porušením povinností a tato náhrada škody se hradí v plné výši bez ohledu na výši smluvní pokuty.
6. Každá ze stran této smlouvy odpovídá druhé straně za škodu vzniklou porušením povinností vyplývajících z této smlouvy, nebo zaviněným porušením právních předpisů. Odpovědnosti se strana zproští, jestliže byla škoda způsobena objektivně neodvratitelnou událostí, které nemohlo být zabráněno ani při vynaložení veškerého úsilí, které lze požadovat za daných podmínek konkrétního případu (vyšší moc).

#### Čl. X.

##### Závěrečná ustanovení

1. Vztahy neupravené touto servisní smlouvou se řídí úpravou vztahů uvedených ve smlouvě „„o Poskytnutí služby „Řešení PKI pro čipovou kartu“““
2. Veškeré změny a doplňky smlouvy mohou být provedeny jen formou písemných číslovaných dodatků, podepsanými oběma stranami.
3. Smlouva nabývá platnosti a účinnosti dnem podpisu smluvními stranami.
4. Nedílnou součástí Servisní smlouvy jsou tyto přílohy:  
Příloha č. 1 Podmínky poskytování servisních služeb  
Příloha č. 2 Technická specifikace servisních služeb

V Praze dne 25. října 2006

Ve Zlíně dne: 25.10.2006

*Loau Jdr*

Objednatel



*Beneš*

Zhotovitel

**MONET+, a.s.** ®

Za Dvorem 505, 763 14 Zlín - Štýpa  
IČO: 26217783, DIČ: CZ26217783  
tel.: ++420 577 110 411, fax: ++420 577 914 557

**Příloha č. 1 Servisní smlouvy č. objednatele INO/40/05/001122/2006, č. zhotovitele S246/06, která tvoří přílohu č. 1 ke smlouvě „Smlouva o poskytnutí služby „Řešení PKI pro čipovou kartu““ č. objednatele INO/40/05/001121/2006, č. zhotovitele 246/06**

### **Podmínky poskytování servisních služeb**

Zhotovitel se zavazuje poskytovat služby podpory za následujících podmínek:

- Předmětné softwarové a hardwarové produkty budou používány pouze způsobem, který je popsán v dodané uživatelské, administrátorské či implementační dokumentaci.
- Objednatel zajistí ochranu počítačů před viry nebo jinými programy, které by mohly narušovat integritu systémů.
- Objednatel zajistí provozní prostředí, které neohrožuje provoz počítačů – teplota v rozmezí 10-28°C, neprašné a nevlhké prostředí.
- Systém budou obsluhovat jen osoby, které prošly školením a jsou pro provoz systému způsobilé.
- Objednatel zajistí přístup do prostor pro účely servisních zásahů, po dohodě i v mimopracovní dobu.
- Objednatel bude informovat dodavatele o změnách ve vnitřních předpisech pro správu informačního systému nebo o dalších plánovaných organizačních či jiných změnách, které jakkoli souvisí s provozovaným systémem. Objednatel je povinen takto informovat nejméně 20 dnů než uvedené změny budou realizovány.
- Objednatel se zavazuje poskytnout dodavateli potřebné podklady, odborné konzultace a potřebnou součinnost k provádění servisních činností.
- Nahlášení problémových stavů bude probíhat pouze dohodnutým způsobem.

**Příloha č. 2 Servisní smlouvy č. objednatele INO/40/05/001122/2006, č. zhotovitele 6246/06, která tvoří přílohu č. 1 ke smlouvě „Smlouva o poskytnutí služby „Řešení PKI pro čipovou kartu““ č. objednatele INO/40/05/001121/2006, č. zhotovitele 246/06**

### **Technická specifikace servisních služeb**

Zhotovitel bude zajišťovat podporu pro objednatele při údržbě, rozšiřování a doplňování dodaných softwarových a hardwarových částí po dobu 4 let. Podpora bude zajišťována k předmětu této nabídky pro zajištění bezproblémového chodu všech dodaných částí.

### **Seznam poskytovaných služeb podpory**

- Zajištění úpravy software v případě legislativních změn. Zhotovitel se zavazuje v případě legislativních změn do 30 dnů od jejich zveřejnění poskytnout úpravu předmětného software pokud tomu nebudou bránit velmi závažné technologické či jiné omezení.
- Vzdálená podpora Help-desk a Hot-line v rozsahu:
  - Poskytování všech potřebných aktuálních verzí použitého software,
  - Poskytování a aktualizace servisní dokumentace,
  - Poskytování a aktualizace servisních a diagnostických nástrojů.
- Zajištění technologického rozvoje produktu
  - Update dodaného PKI appletu a middleware *CryptoPlus ProID* jako reakce na případně vzniklé problémové stavy,
  - Úprava dokumentace k novým verzím poskytnutého software,
  - Úprava bezpečnostní dokumentace k novým verzím poskytnutého software,
  - Zajištění portace softwarového produktu na nové verze Internet Explorer a na nové verze prohlížečů Netscape / Mozilla,
  - Konzultační podpora portace softwarových produktů na nové typy čtecích zařízení.
- Řešení chybových stavů
  - Zajištění nápravy kritických chyb,
  - Zajištění nápravy chyb, které nemají kritickou povahu.
- Školení pracovníků a trvalý přenos know-how na pracovníky objednatele. Pracovníci objednatele budou proškoleni také v oblasti bezpečnosti práce a požárních předpisů souvisejících s předmětem dodávky.

**Příloha č. 2 Licenční smlouva**

ke smlouvě „Smlouva o poskytnutí služby „Řešení PKI pro čipovou kartu““, č.  
objednatele INO/40/05/001121/2006, č. zhotovitele 246/06

Níže uvedeného dne, měsíce a roku uzavřely

**HLAVNÍ MĚSTO PRAHA**

se sídlem: Mariánské nám. 2/2, 110 01 Praha 1  
zastoupené: Ing. Ivanem Seyčkem, ředitelem odboru informatiky Magistrátu hl. m. Prahy  
IČ: 00064581, DIČ: CZ00064581  
Bank. spojení: PPF banka, a.s., číslo účtu: 27-5157998/6000

(dále jen „nabyvatel licence“)

a

**MONET+, a. s.**

se sídlem: Za Dvorem 505, 763 14 Zlín - Štípa  
zastoupená: Mgr. Jiřím Benešem, obchodním ředitelem, zplnomocněný k podpisu  
IČ: 26217783, DIČ: CZ26217783  
Bank. spojení: KB, č. ú.: 1547260257/0100

(dále jen „poskytovatel licence“)

**Licenční smlouvu**

v souladu s ust. § 46 a násl. zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), která tvoří přílohu č. 2 ke smlouvě „o Poskytnutí služby „Řešení PKI pro čipovou kartu““ č. smlouvy č. objednatel INO/40/05/001121/2006, č. zhotovitele 246/06  
č. objednatel LIC/40/05/001123/2006, č. zhotovitele L246/06

**Čl. I.**

**Účel smlouvy, specifikace software**

1. Poskytovatel licence je výrobcem a vykonavatelem majetkových práv software PKI appletu, middleware a technického řešení zápisu na kontaktní čip (dále také jen „software“). Podrobný popis software PKI appletu a middleware tvoří nedílnou přílohu č. 1 smlouvy „o Poskytnutí služby „Řešení PKI pro čipovou kartu““, jejíž je tato Licenční smlouva přílohou. Poskytovatel udělí nabyvateli licence k softwaru PKI appletu a middleware (včetně následných jejich upgradů) a dodá technické řešení pro zápis software PKI appletu do kontaktního čipu, přičemž podrobný popis požadavků na zápis je specifikován v nedílné příloze č. 2 této smlouvy „o Poskytnutí služby „Řešení PKI pro čipovou kartu““, jejíž je tato Servisní smlouva přílohou.
2. Účelem této smlouvy je upravit vzájemná práva a povinnosti smluvních stran v souvislosti s poskytnutím práv k užití softwaru PKI appletu, middleware a technického řešení zápisu PKI appletu na kontaktní čip v rozsahu určeném touto smlouvou.



Ujednání smluvních stran obsažená v této smlouvě mají nabyvateli licence umožnit využití licence v rozsahu určeném touto smlouvou.

4. Licence bude poskytnuta k využití pro 50 000 čipových karet v rozsahu nezbytném pro kvalitní provoz Servisního kartového centra.

## **Čl. II.**

### **Předmět Smlouvy**

1. Touto smlouvou a za podmínek stanovených v zadávací dokumentaci poskytuje poskytovatel licence nabyvateli licence k užívání PKI appletu a obslužného middleware pro užití na 50 000 čipových karet současně. Obslužný middleware může být využíván na neomezeném počtu osobních počítačů, nicméně vždy jen držitelem čipové karty, na které je uložen PKI applet.
2. Poskytovatel licence se dále zavazuje dodat nabyvateli licence technické řešení zápisu PKI appletu na kontaktní čip, a to za podmínek stanovených v příloze č. 2, která je nedílnou přílohou smlouvy o poskytnutí služby „Řešení PKI pro čipovou kartu“, jejíž je tato Licenční smlouva přílohou.
3. Licence se poskytuje na dobu trvání majetkových práv poskytovatele licence.

## **Čl. III.**

### **Cena**

1. Cena uvedená ve smlouvě „o Poskytnutí služby „Řešení PKI pro čipovou kartu“ za poskytnutí licence bude členěna následovně:

a) Cena za SW licence PKI appletu a middleware

cena bez DPH:	9.690.000,- Kč
sazba DPH – 19 %, vyčíslení DPH:	1.841.000,- Kč
celková cena včetně DPH:	11.531.100,- Kč

b) Cena za technické řešení zápisu PKI appletu do kontaktního čipu

cena bez DPH:	4.228.700,- Kč
sazba DPH – 19 %, vyčíslení:	803.453,- Kč
celková cena včetně DPH:	5.032.153,- Kč

### **Cena celkem**

cena bez DPH:	13.918.700,- Kč
sazba DPH - 19%, vyčíslení DPH:	2.644.453,- Kč
celková cena včetně DPH:	16.563.253,- Kč

2. Sjednaná cena v sobě zahrnuje veškeré náklady poskytovatele licence.
3. Pokud nabyvatel licence bude mít výhrady k předanému software, má právo požadovat od poskytovatele licence odstranění nedostatků. Odstranění nedostatků nese poskytovatel licence na své náklady, nemá právo požadovat v tomto případě náhradu nákladů od objednatele spojených s odstraněním nedostatků. Nabyvatele licence má povinnost na nedostatky upozornit písemnou formou neprodleně po jejich zjištění.

#### **Čl. IV.**

##### **Prohlášení a odpovědnost poskytovatele licence**

1. Poskytovatel licence výslovně prohlašuje, že ošetřil veškerá práva k duševnímu vlastnictví v rozsahu nezbytném k naplnění účelu smlouvy, zejména, že je oprávněn poskytnout nabyvateli licence právo užít poskytnuté software k účelům stanoveným ve smlouvě.
2. Poskytovatel licence odpovídá za právní a finanční ošetření případných práv třetích osob k software, a to takovým způsobem, aby mohlo být software nabyvatelem licence bez dalšího užíváno k účelu dle smlouvy. Předchozí věta se vztahuje zejména na práva třetích osob vyplývající z autorského zákona a na práva třetích osob v případě, že software bude obsahovat označení či motiv, které je chráněno jako ochranná známka ve smyslu zákona o ochranných známkách.
3. Poskytovatel licence odpovídá za to, že užití software nabyvatelem licence k účelu dle této smlouvy neodporuje právu třetí osoby na ochranu osobnosti. Poskytovatel licence dále prohlašuje, že získal případná oprávnění od příslušných nositelů práv k zapracování jejich děl do software.
4. Poskytovatel licence odpovídá za to, že užití software nebude v rozporu s obecně závaznými právními předpisy.
5. Poskytovatel licence výslovně prohlašuje, že užitím software dle této smlouvy nedojde k zásahu do práv třetích osob. V případě, že k zásahu do práv třetích osob dojde, zavazuje se poskytovatel licence, že nahradí škodu, která nabyvateli licence vznikne v souvislosti s nároky třetích stran z důvodu porušení jejich chráněných práv.
6. Pokud není poskytovatel licence držitelem výhradních a neomezených autorských práv k software, uvede v příloze č. 1 této smlouvy licenční či obdobnou smlouvu, kterou prokazuje, že je oprávněn nejméně do data 31.12.2016 nebo bez časového omezení, nakládat s použitými programovými částmi (software), které jsou majetkem třetích osob.

#### **Čl. V.**

##### **Předání a převzetí software**

1. Poskytovatel licence je povinen software předat nabyvateli licence ve lhůtě nejdéle do 30 kalendářních dnů od uzavření této smlouvy. Spolu se softwarem je poskytovatel licence povinen předat nabyvateli licence veškeré související podklady umožňující řádné užití software jako např. písemnou technickou dokumentaci, bezpečnostní dokumentaci apod. Pokud objednatel neposkytne potřebnou součinnost uvedenou v Příloze č. 4 této smlouvy je zhotovitel oprávněn požadovat posun termínu plnění o dobu, po kterou nebyla součinnost poskytnuta
2. Nabyvatel licence je povinen software a související podklady převzít. O předání a převzetí software bude smluvními stranami sepsán stručný písemný protokol.

**Čl. VI.**  
**Smluvní pokuty**

1. V případě, že poskytovatel licence bez vážných důvodů nedodrží termíny dle čl. V. odst. 1 této smlouvy, nebo termín sjednaný účastníky smlouvy na společném jednání, je povinen zaplatit smluvní pokutu ve výši 50.000,- Kč za každý den prodlení, a to až do splnění své povinnosti
2. Smluvní pokutu je povinna smluvní strana uhradit bez ohledu na to, zda a v jaké výši vznikla druhé straně v této souvislosti škoda, která je vymahatelná samostatně vedle smluvní pokuty, a to v plné výši.


**Čl. VII.**  
**Závěrečná ustanovení**

1. Nabyvatel licence je oprávněn požadovat od poskytovatele licence předložení dokumentů osvědčujících plnění jeho závazků dle této smlouvy.
2. Vztahy neupravené touto licenční smlouvou se řídí úpravou vztahů uvedených ve smlouvě „o Poskytnutí služby „Řešení PKI pro čipovou kartu“, zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.
3. Tato smlouva může být měněna jen se souhlasem smluvních stran, a to formou písemných číslovaných dodatků, podepsaných oběma smluvními stranami.
4. Platnosti a účinnosti tato smlouva nabývá dnem podpisu oběma smluvními stranami.
5. Smluvní strany tímto prohlašují, že neexistuje žádné ústní ujednání, žádná smlouva či řízení týkající se některé smluvní strany, které by nepříznivě ovlivnilo splnění závazků vyplývajících z této smlouvy. Zároveň svým podpisem potvrzují, že veškerá prohlášení a dokumenty podle této smlouvy jsou pravdivé, úplné, přesné, platné a právně vynutitelné.
6. Smluvní strany dále prohlašují, že si smlouvu pečlivě přečetly, všem ustanovením smlouvy rozumí a na důkaz svého souhlasu učiněného vážně a svobodně smlouvu vlastnoručně podepisují.

Ve Zlíně dne: 25.10.2006

V Praze dne

**MONET+, a.s.**   
Za Dvorem 505, 763 14 Zlín - Štípa  
IČO: 28217783, DIČ: CZ28217783  
tel.: +420 577 110 411, fax: +420 577 914 557

  
.....  
Poskytovatel licence

  
.....  
Nabyvatel licence



**Technická specifikace PKI appletu a obslužného software (middleware)** ke smlouvě „Smlouva o poskytnutí služby „Řešení PKI pro čipovou kartu““ č. objednatele INO/40/05/001121/2006, č. zhotovitele 246/06

## **Specifikace technického řešení PKI appletu**

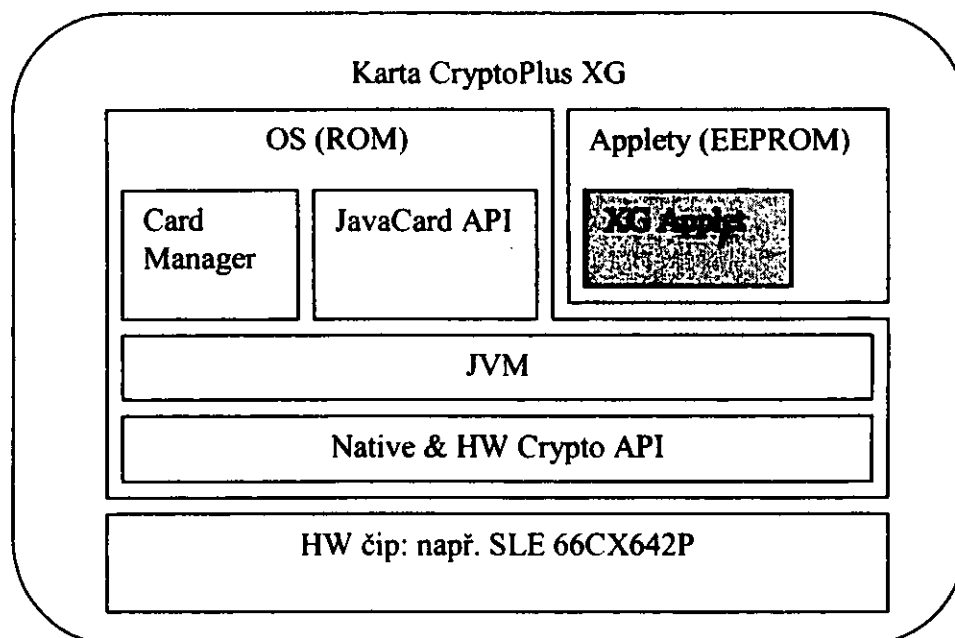
Zhotovitel dodá PKI applet *CryptoPlus XG*.

Applet *CryptoPlus XG* bude dodán s middleware *CryptoPlus ProID* a tvoří tak nedělitelný celek PKI řešení na čipové kartě.

## **Základní popis appletu *CryptoPlus XG***

*CryptoPlus XG* představuje PKI applet pro čipovou kartu s interním funkčním rozhraním, které je optimalizováno pro klientské PKI aplikace, založené na certifikátech X.509.

Vnitřní architektura čipové karty s appletem *CryptoPlus XG*:



Funkčním jádrem *CryptoPlus XG* je tzv. XG Applet, který realizuje ISO 7816-4 kompatibilní souborový systém doplněný o funkce související s PKI.

Applet *CryptoPlus XG* je možno provozovat na HW platformách, které splňují následující specifikaci čipu:

- Vyhovění Java Card, Open Platform 2.0.1, ISO 7816
- Certifikace čipu dle CCEAL5 a / nebo FIPS140-1 level2
- Existence kryptografického koprocesoru pro podporu symetrické (DES, 3DES) i asymetrické (RSA) kryptografie
- Paměť o velikosti 64kB

- Soulad s normami ČSN EN ISO7816, část 1-4, podpora protokolů T=0 a/nebo T=1, ČSN EN ISO/IEC 10373
- Podpora klíčů RSA až do velikosti 2 048 bitů
- Podpora HW ochrany proto fyzickému a časovému útoku
- PseudoHW generátor náhodných čísel resp. true random number generátor
- Minimální množina algoritmů:
  - Symetrická kryptografie:
    - javacard.security.KeyBuilder.TYPE\_DES\_TRANSIENT\_RESET
    - javacard.security.KeyBuilder.LENGTH\_DES3\_2KEY
    - javacard.security.Signature.ALG\_DES\_MAC8\_NOPAD
    - javacardx.crypto.Cipher.ALG\_DES\_ECB\_NOPAD
  - Asymetrická kryptografie:
    - javacard.security.KeyPair
    - javacard.security.KeyBuilder.TYPE\_RSA\_PUBLIC
    - javacard.security.KeyBuilder.TYPE\_RSA\_CRT\_PRIVATE
    - javacard.security.KeyBuilder.LENGTH\_RSA\_512 (je-li vyžadován klíč RSA512)
    - javacard.security.KeyBuilder.LENGTH\_RSA\_1024 (je-li vyžadován klíč RSA1024)
    - javacard.security.KeyBuilder.LENGTH\_RSA\_1536 (je-li vyžadován klíč RSA1536)
    - javacard.security.KeyBuilder.LENGTH\_RSA\_2048 (je-li vyžadován klíč RSA2048)
    - javacardx.crypto.Cipher.ALG\_RSA\_NOPAD
  - Hashovací algoritmy:
    - javacard.security.MessageDigest.ALG\_MD5
    - javacard.security.MessageDigest.ALG\_SHA
  - Generátor čísel:
    - javacard.security.RandomData.ALG\_SECURE\_RANDOM
  - Podpora změny Histo-bytu ATR
    - visa.openplatform.OPSystem.setATRHistBytes
  - Paměťové nároky:
    - Transient memory: min 600 B pro applet, doporučujeme 1kB
    - Podpora transient paměťových alokací
      - javacard.framework.JCSystem.CLEAR\_ON\_DESELECT
      - javacard.framework.JCSystem.CLEAR\_ON\_RESET
    - APDU buffer min. 260 B (celé APDU: 5 byte hlavička + 255 byte data)
    - Transaction buffer min. 300 B
    - Persistent memory: min 20 kB volné paměti pro applet a jeho data

## Popis funkcí appletu

### Základní vlastnosti

Vlastnost	Popis
Applet, verze	CryptoPlus XG applet, v1.10
Kryptografické algoritmy	<ul style="list-style-type: none"> <li>• RSA 1024, 1536, 2048 bitů               <ul style="list-style-type: none"> <li>○ HW generování klíče</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>○ import klíče</li> <li>○ elektronický podpis s výpočtem haš na kartě (MD5, SHA-1), padding na kartě (EMSA-PKCS1-v1_5, EMSA-PKCS1 bez DER kódování OID hašovací funkce)</li> <li>○ elektronický podpis s výpočtem haš mimo kartu (MD5, SHA-1, SHA256, SHA384, SHA512, RIPEMD128, RIPEMD160), padding na kartě (EMSA-PKCS1-v1_5, EMSA-PKCS1 bez DER kódování OID hašovací funkce)</li> <li>○ elektronický podpis s výpočtem haš mimo kartu (spojení hodnot haš SHA-1, MD5), padding na kartě (EMSA-PKCS1 bez DER kódování OID hašovací funkce)</li> <li>○ dešifrování dat (symetrických klíčů) RSA klíčem s odstraněním paddingu RSAES-PKCS1-V1_5</li> <li>○ obecná operace s RSA klíčem (bez paddingu) – umožňuje realizaci vlastního paddingu v SW</li> <li>• výpočet haš SHA-1 a MD5 pro použití v operaci vytvoření elektronického podpisu</li> <li>• 3DES algoritmus (klíč 112 bitů) pro <ul style="list-style-type: none"> <li>○ šifrování PIN (ECB režim)</li> <li>○ šifrování importovaného privátního klíče (ECB režim)</li> <li>○ zajištění integrity přenášení APDU příkazů (CBC-MAC režim)</li> </ul> </li> <li>• HW true random number generátor</li> </ul>
Souborový systém	<ul style="list-style-type: none"> <li>• ISO 7816-4 s podporou „secure messaging“</li> <li>• 2-úrovňová hierarchie adresářů</li> <li>• podpora selekce přes AID (i částečný název)</li> <li>• podpora globálních i aplikačních PIN objektů (až 8 objektů na adresář)</li> <li>• různé typy 3DES klíčů</li> <li>• implementované bezpečnostní politiky pro uložení RSA klíčů (privátní klíče nelze exportovat, import, pokud je možný, pak pouze s použitím šifrovaného kanálu)</li> <li>• optimalizováno pro výkon (s ohledem na použití JavaCard)</li> <li>• podpora životního cyklu (personalizační fáze, uživatelská fáze – pozor, tyto fáze jsou nad rámec fází definovaných v OpenPlatform)</li> </ul>

## Skupiny příkazů *CryptoPlus XG* appletu

### Administrativní příkazy

Příkaz	Stručný popis
Append Record	Přidá záznam do strukturovaného souboru
Create File	Vytvoří nový soubor nebo adresář
Erase Card	Inicializuje souborový systém, veškerá paměť je nulována
Freeze Access Conditions	Modifikuje přístupové podmínky na soubor
Get Challenge	Generuje náhodná čísla
Get Info	Vrací různé informace o kartě nebo o souborech
Get Response	Vrací data připravena v rámci předchozího příkazu
Read Binary	Čte data z transparentního datového souboru
Read Record	Čte záznam ze strukturovaného souboru
Select File	Změní adresář nebo otevře soubor
Select Admin Key	Ustaví administrativní klíč sezení
Set Card Status	Mění fázi životního cyklu karty
Set Secret Code	Mění nebo odblokuje PIN
Update Binary	Modifikuje obsah transparentního datového souboru
Update Record	Mění záznam strukturovaného souboru
Verify	Autentizace ke kartě
Write Binary	Provede „WRITE“ zápis do transparentního datového souboru

### Příkazy pro transakce

Příkaz	Stručný popis
Select Trans Key	Ustaví transakční klíč sezení (s použitím tzv. „Log Key“)

### Příkazy pro PKI

Příkaz	Stručný popis
Create Private Key File	Vytvoří chráněný prostor pro privátní RSA klíč
Generate Key Pair	Provede HW generování RSA klíče
InitHashedData	Nastaví hodnotu haš, která se má podepsat
Load Private Key	Importuje privátní RSA klíč
PSO_Decipher	Pomocí privátního RSA klíče dešifruje blok dat (s volitelným odstraněním PKCS#1 paddingu)
PSO_ComputeDigitalSignature	Vytvoří elektronický podpis
PSO_HashData	Provádí výpočet haš z dat (data mohou být posílána po blocích)
PSO_InitOperation	Inicializuje operaci s RSA klíčem

## *CryptoPlus XG* – parametry a vlastnosti kryptografických funkcí

### Šifrovací algoritmy

Algoritmus	Délka klíče	Režim	Poznámka
RSA	1024, 1536, 2048	RSAES-PKCS1-V1_5-Decrypt	Rozšifrování symetrického klíče s paddingem PKCS#1 v1.5, typ 2

24-2

RSA	1024, 1536, 2048	RAW Encrypt (PKCS#1 RSADP)	Základní operace s privátním klíčem bez kontroly formátu vstupních a výstupních dat – použitelná pro vytváření vlastního paddingu pomocí SW.
3DES	112	ECB	Zajištění utajení dat při komunikaci mezi obslužným SW a kartou. Šifrovaná data jsou: <ul style="list-style-type: none"> <li>• privátní RSA klíč při importu</li> <li>• hodnota PIN při požadavku na šifrovaný přenos</li> </ul>
3DES	112	CBC-MAC	Zajištění integrity přenosu APDU příkazů.

### Podpisová schémata

Asymetrický algoritmus	Délka klíče	Padding	Hašovací funkce
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	SHA-1, výpočet hodnoty haš proveden na čipu
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	SHA-1, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	SHA-1, výpočet hodnoty haš proveden na čipu
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	SHA-1, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	MD5, výpočet hodnoty haš proveden na čipu
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	MD5, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	MD5, výpočet hodnoty haš proveden na čipu
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	MD5, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	RIPEMD160, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	RIPEMD160, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	RIPEMD128, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID	RIPEMD128, výpočet hodnoty haš proveden v



		hašovací funkce	SW
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	SHA256, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	SHA256, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	SHA výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	SHA výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	SHA384, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	SHA384, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	spojení SHA1 a MD5 (tzv. SSL), výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	vytvoření paddingu v SW	výpočet hodnoty haš proveden v SW

### Algoritmy generování asymetrických klíčů

Asymetrický algoritmus	Délka klíče	Metoda generování náhodných čísel
RSA	1024, 1536, 2048	True random

### Hašovací funkce

Jméno haš funkce	Výstupní délka (bitů)
SHA-1	160
MD5	128

### Podporované standardy, normy a protokoly

- PKCS#1
- PKCS#7 (s využitím SW)
- PKCS#10 (s využitím SW)
- PKCS#11 (SW rozhraní)
- PKCS#12 (s využitím SW)
- SSL, TLS, S/MIME, EAP (s využitím SW)
- X.509v1 – v3
- CSP (Cryptographic Service Provider, SW rozhraní)

Q

- ISO 7816-1,2,3,4
- protokol T=0
- SHA-1, MD5, RIPEMD128, RIPEMD160, SHA256, SHA384, SHA512
- 3DES, RSA
- JavaCard 2.1.1
- OpenPlatform 2.0.1' level 2

## ***CryptoPlus ProID middleware***

*CryptoPlus ProID* middleware je soubor knihoven, které zprostředkují operačnímu systému funkce PKI čipových karet. Zároveň poskytují rozhraní pro použití *CryptoPlus ProID* dalším aplikacím. Aplikace a systémy pak mohou využívat *CryptoPlus ProID* např. pro:

- autentizaci
- zabezpečení dat (elektronický podpis, šifrování)
- bezpečné uložení citlivých aplikačních dat
- atd...

Pro použití PKI dat implementuje *CryptoPlus ProID* dvě standardizovaná rozhraní:

- **Cryptographic service provider (CSP)** pro použití přes CryptoAPI Microsoft, buď přímo anebo prostřednictvím high-level komponent, jako je např. CAPICOM. CSP je standardně digitálně podepisováno společnostmi Microsoft.
- **PKCS#11** pro non-Microsoft aplikace

Pro automatickou registraci certifikátů do Windows implementuje *CryptoPlus ProID* vlastní Certificate Store Provider. Ten po vložení karty uživateli automaticky zaregistruje všechny certifikáty, uložené na kartě. Po vyjmutí karty jsou certifikáty automaticky odregistrovány.

Použití statických dat pro řešení Single Sign-On je implementováno proprietárními algoritmy aplikace *PassPro Tools*.

*CryptoPlus ProID* middleware umožňuje pracovat současně s několika čtečkami připojenými k počítači.

Použití *CryptoPlus ProID* je vázáno na čipové karty, v nichž je implementován PKI applet *CryptoPlus XG*.

*CryptoPlus ProID* je kompletně lokalizován do:

- češtiny
- angličtiny
- slovenštiny
- němčiny

Uživatel si může použitý jazyk zvolit pomocí grafického uživatelského rozhraní.

...případě zájmu je Zhotovitel připraven nad rámec této nabídky lokalizovat produkt do dalších jazyků.

*CryptoPlus ProID* middleware bude dodáno na CD ve dvou vyhotoveních, zároveň bude také umožněn přístup na web server pro stažení instalačního balíčku v aktuální verzi.

Pro uložení dat se využívá standardních formátů:

- X.509 pro formát certifikátů
- PKCS#12 pro uložení páru klíčů a certifikátu. Tento formát je využíván při importu RSA klíčů na kartu *CryptoPlus ProID*

Pro šifrování, integritu apod. jsou užívány standardní algoritmy:

- Asymetrická šifra RSA
- Symetrické šifrování: 3DES, DES, RC2, RC4, RC5
- Hashovací funkce: SHA-1, RIPEMD160, MD5

Pro integraci karet *CryptoPlus ProID* do operačních systémů, resp. aplikací jsou dodána standardní rozhraní:

- Cryptographic Service Provider (CSP) pro použití v OS Windows a aplikacích kompatibilních se standardy Microsoftu
- Certificate Store Provider pro automatickou registraci certifikátů z karty do OS Windows
- PKCS#11 pro použití v „non-Microsoft“ aplikacích

Pro komunikaci operačního systému se čtečkou karet se využívá standardních rozhraní:

- PC/SC pro integraci čtečky do OS Windows
- PC/SC Lite pro integraci čtečky do OS Linux. (Instalace ovladačů čtečky do Linuxu je závislá na verzi použité distribuce Linuxu, resp. na verzi jádra.)

## **Komponenty *CryptoPlus ProID* middleware**

*CryptoPlus ProID* middleware je souborem následujících komponent:

- Knihovny pro operační systém
  - Cryptographic Service Provider (CSP) - implementace kryptografického rozhraní pro operační systém MS Windows a CryptoAPI.
  - Knihovna PKCS#11 – implementace standardního kryptografického rozhraní hardwarového tokenu pro aplikační využití.
  - Certificate Store Provider – podpora pro automatickou registraci certifikátů z karty do operačního systému MS Windows.
  - Podpůrné knihovny, používané ostatními komponentami.
- *PassPro Tools* – software pro automatizované přihlašování do aplikací pomocí údajů z karty.
- *Správce karty* – grafická aplikace pro správu dat na kartě.
- Instalační software pro grafickou anebo bezobslužnou instalaci.

## PassPro Tools

*PassPro Tools* je jednoduchý **Single Sign-On** subsystém pro autentizaci uživatele do non-PKI aplikací. Je navržen pro starší typy aplikací, do nichž se uživatel autentizuje jménem a heslem.

*PassPro Tools* umožní uživateli zaznamenat si jména a hesla do bezpečného úložiště – na čipovou kartu, kde musí být vytvořeny kontejnery pro uložení statických dat. Použití autentizačních údajů je chráněno pomocí PIN (stejný PIN jako pro PKI objekty).

Kromě **bezpečného uložení** umí *PassPro Tools* autentizační údaje **automaticky použít**:

- detekuje zobrazení formuláře pro přihlášení uživatele
- nalezne na kartě autentizační údaje pro daný formulář
- automaticky vyplní údaje do formuláře
- automaticky stiskne tlačítko spouštějící proces přihlášení uživatele

Tento postup zajistí automatické přihlášení uživatele do:

- standardních aplikací (EXE)
- webových formulářů (pouze v prohlížeči MS Internet Explorer)

## Správce karty

*Správce karty* je klientská grafická utilita pro práci s daty na kartě *CryptoPlus ProID*. Pomocí *Správce karty* lze:

- zobrazit data uložená na kartě
- mazat data z karty
- importovat data na kartu
- exportovat (některá) data z karty do souboru
- měnit PIN, PUK karty
- odblokovat kartu
- atd...

Program také umožňuje vygenerovat diagnostiku *CryptoPlus ProID*, která může být při potížích cenným zdrojem informací pro pracovníky podpory *CryptoPlus ProID*.

Použití webového rozhraní zjednodušuje ovládání programu pro méně zkušené uživatele.

## Kompatibilita CryptoPlus ProID s aplikacemi třetích stran

aplikacích třetích stran.

V následujícím přehledu jsou uvedeny vybrané aplikace, které byly úspěšně testovány na kompatibilitu a interoperabilitu s *CryptoPlus ProID* middleware.

### Klientská autentizace webovým prohlížečem na HTTPS spojení

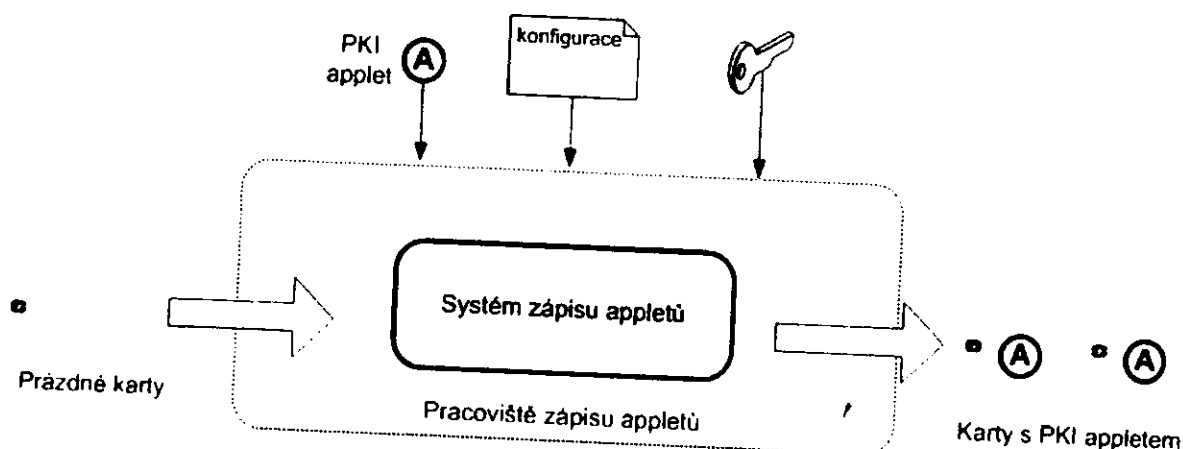
- MS Internet Explorer (od verze 5)
- Netscape (od verze 4.7)
- Mozilla (od verze 0.9, vč. Firefox)
- **Autentizace do domény MS Windows (2000 i 2003)**
  - Smart Card Logon
  - pomocí *Run as*

- Terminálové služby (*Terminal Services*) – MS Windows Server i Citrix Metaframe
- přes Wi-Fi
- přes RAS
- přes VPN
- **Elektronický podpis a šifrování e-mailů**
  - MS Outlook
  - MS Outlook Express
  - Mozilla (vč. Thunderbird)
  - Netscape
  - Novell GroupWise
- **Elektronický podpis webových formulářů**
  - MS Internet Explorer (od verze 5, s použitím CAPICOM)
  - Netscape (od verze 4.7)
  - Mozilla (od verze 0.9)
- **Certifikační autority**
  - MS Windows Server 2000 i 2003
  - Entrust
  - Baltimore (UniCERT) WebRAO
  - Novell Certificate Server 2
  - První certifikační autorita (I.CA)
  - CA České pošty (PostSignum)
  - AEC (Trustport)
  - CA EVPU (*pozn.: první akreditovaná CA na Slovensku*)
  - ...
- **Bezpečné uložení klíče, podpora šifrování**
  - AreaGuard (SODATSW)
  - Protect (ICZ)
  - PGP (od verze 8)
  - SafeEnterprise ProtectFile
  - Entrust Desktop Solutions
- **Elektronický podpis maker a dokumentů**
  - MS Office (od verze 2000)

## **Specifikace technického řešení zápisu appletu do čipové karty**

### **Technický popis řešení zápisu appletu**

PKI applet bude do kontaktních čipů zapisován na *pracovišti zápisu appletů*.



**Schéma Systému zápisu appletů**

Vstupem *pracoviště zápisu appletů* budou:

- Prázdné karty (bez appletu)
- Klíče pro zápis appletu a způsob použití těchto klíčů
- PKI applet
- Konfigurace zápisu appletu

Výstupem procesu budou karty s PKI appletem.

Vzniklá karta bude plně kompatibilní s dodaným middleware. Pro ověření funkčnosti vzniklé karty budou nahrány na kartu certifikáty ve formátu CX.509.

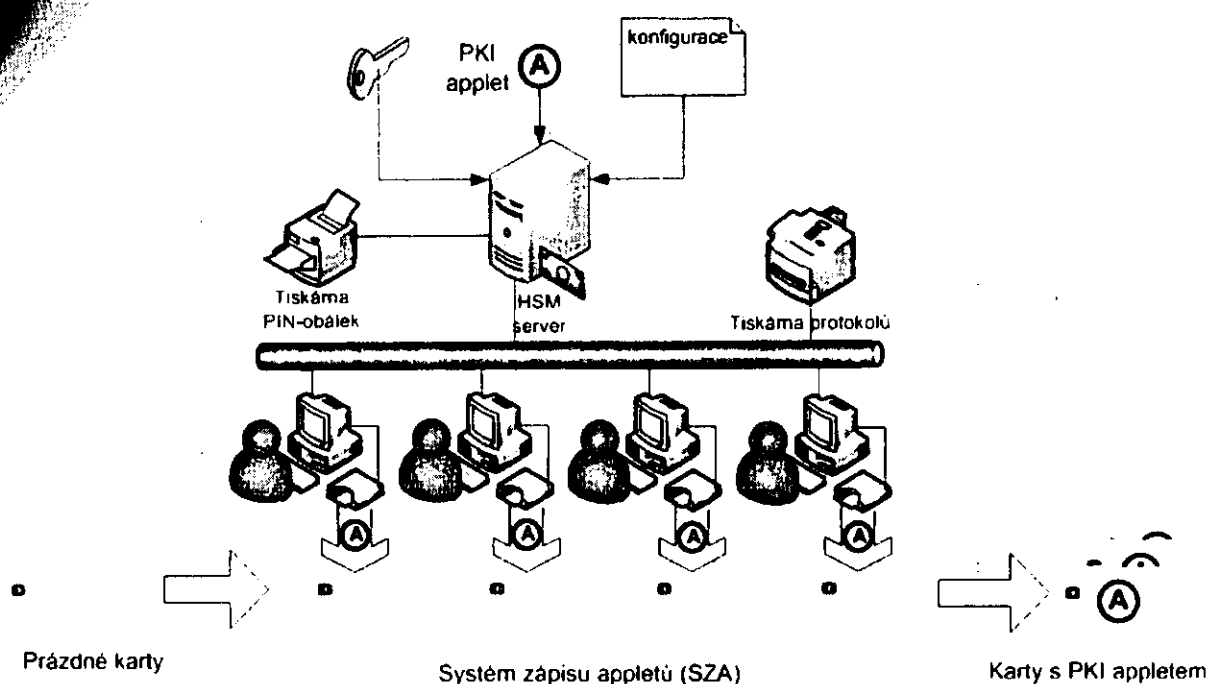
Zápis appletu do čipů bude proveden *Systémem zápisu appletů*, který dodá zhotovitel.

Kromě *Systému zápisu appletů* dodá zhotovitel také: PKI applet a konfiguraci *Systému zápisu appletu*.

Prázdné karty a klíče pro zápis appletů zajistí objednatel. Objednatel zajistí také informace, potřebné pro konfiguraci – zejména informace o práci s klíči dodaných karet.

### **Systém zápisu appletů**

Zhotovitel dodá *Systém zápisu appletů*, který bude řídit a realizovat zápis PKI appletů do kontaktních čipů.



**Detailní schéma Systému zápisu appletů**

**Systém zápisu appletů (SZ) se skládá z těchto komponent:**

- **Obslužné pracoviště zápisu appletů (OPZA).** Počítač s připojenou čtečkou čipových karet. Na počítači je instalován *Modul realizace zápisu appletů karty (MRZAK)*, který řídí proces zápisu appletu do kontaktních čipů karet. *OPZA* při svých operacích využívá *HSM*. Vkládání karet do čtečky zajišťuje lidská obsluha.
- **HSM server.** Server, v němž je instalován *Host Security Module (HSM)*. *HSM* je bezpečný hardware, který slouží k ukládání citlivých informací (zejména klíčů). *HSM* také provádí kryptografické operace s klíči. Server pro modul *MRZAK* poskytuje podpůrné kryptografické funkce související s operací zápisu appletu.
- Tiskárna pro tisk protokolů, např. protokoly o zavedení klíčů do *HSM*, protokoly o provedení personalizace, atp.
- Tiskárna PIN-obálek. Jehličková tiskárna, která do neprůhledných PIN-obálek tiskne hesla pro autentizaci k *HSM*.

### **Funkce HSM serveru**

*HSM server* je bezpečnostním pilířem *SZ*. V *HSM serveru* je instalován kryptografický modul, jehož hlavní úkoly jsou:

- Bezpečné uložení a ochrana klíčů.
- Bezpečné zálohování / obnova klíčů.
- Výpočet kryptogramů pro autentizaci *OPZA* k prázdné kartě.
- Výpočet kryptogramů pro záměnu klíče na kartě.
- Dešifrování PKI appletu.
- Další podpůrné kryptografické funkce související se zápisem appletu.

Na disku *HSM serveru* je uložen zašifrovaný a podepsaný PKI applet, který je zapisován do kontaktních čipů.

Služby *HSM serveru* využívají *OPZA*, jeden *HSM server* je schopen paralelně obsloužit několik *OPZA*.

7

Na *HSM serveru* je aktivován také tiskový server, který mohou při tisku využívat *OPZA*.

### **Funkce OPZA**

Na *Obslužném pracovišti zápisu appletů (OPZA)* se provádí samotný zápis appletu do čipové karty. Na *OPZA* je instalován softwarový *Modul realizace zápisu appletů karty (MRZAK)*. *MRZAK* je grafická aplikace, pomocí níž obsluha provádí zápis appletů do čipových karet.

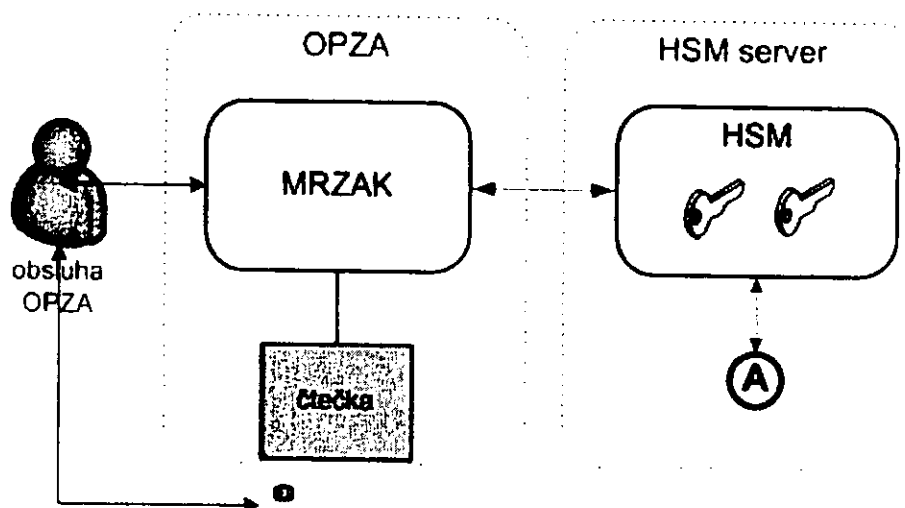


Schéma obslužného pracoviště

Mezi základní funkce *MRZAK* patří:

- Řízení a kontrola procesu zápisu appletu do čipové karty.
- Řízení a ovládání čtečky, včetně detekce chybových a problémových stavů.
- Transfer dat do čtečky a karty:
  - řídicí signály pro čtečku
  - řídicí signály pro čipovou kartu
  - data pro čipovou kartu (PKI applet)
  - ...
- Zpracování odezvy od čtečky a karty.
- Žurnálování procesů.
- Grafická konzola obsluhy, pomocí níž lze mimo jiné
  - vizualizovat informace o probíhajícím procesu zápisu appletů
  - převzít plnou kontrolu nad zápisem appletů
  - řídit procesy zápisu appletů (start, pozastavení, obnova, ukončení, ...)
  - signalizovat možné problémy procesu zápisu appletu (chybové hlášení, varování, ...)
- Bezpečná komunikace s HSM.
- Využití kryptografických služeb HSM.

Pro správnou funkci *MRZAK* je nutno:

- instalovat a konfigurovat *MRZAK* na počítači *OPZA*
- instalovat na *OPZA* funkční čtečku čipových karet
- navázat spojení *MRZAK* s HSM serverem.



Předpokládá se, že obsluhu pro MRZAK zajistí objednatel. Školení obsluhy provede zhotovitel.

### Fyzická struktura Systému zápisu appletů

Fyzicky se SZA skládá z počítačů, spojených navzájem do sítě LAN:

- *HSM server* běží na počítači s operačním systémem MS Windows 2003 Server Standard edice. Je dodán v provedení, které je určeno do rack-u. V *HSM serveru* je instalován kryptografický modul Protect Server Gold CSA 8000 PL220. Na *HSM serveru* běží mj. tiskový server pro ostatní počítače v síti. Díky tomuto tiskovému serveru mohou *OPZA* tisknout na *tiskánu protokolů*.
- Všechna *OPZA* jsou desktopová PC s LCD monitorem, klávesnicí a myší. Běží pod operačním systémem MS Windows XP Professional SP2. Ke každému *OPZA* je přes USB konektor připojena čtečka čipových karet typ Gemplus GemPC Twin USB.
- K *HSM serveru* je připojena jehličková tiskárna EPSON LQ630 pro tisk do PIN-obálek.
- Do sítě je připojena *tiskárna protokolů* HP LaserJet 1320n dostupná všem PC SZA

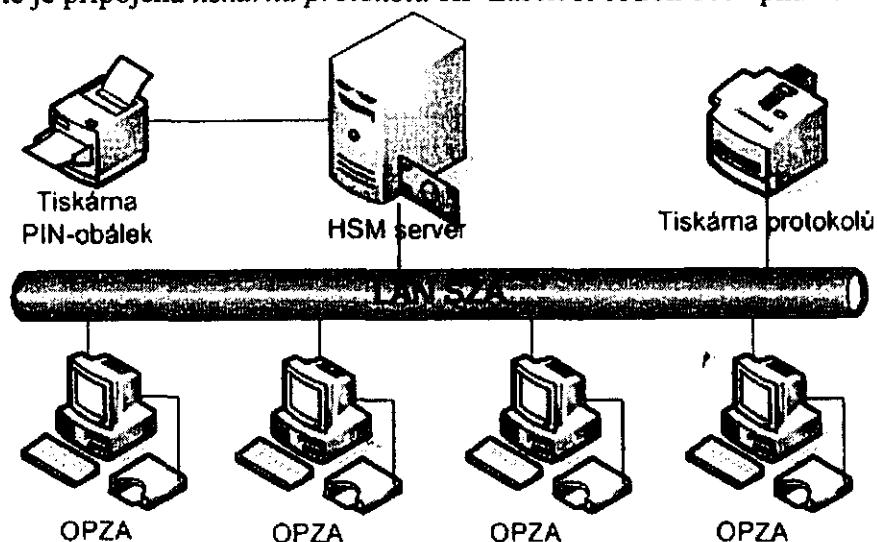


Schéma síťového propojení SZA

### PIN a PUK karet po uložení PKI appletu

Předpokládá se, že prázdné PKI karty budou před vydáním v SKC dále personalizovány. Proto budou mít všechny karty po zápisu appletů nastaveny stejné (známé) hodnoty PIN a PUK:

PIN = 1111

PUK = 44444444

Návazné procesy SKC pak mohou díky znalosti PIN a PUK do kontaktního čipu zapisovat PKI objekty.

Před vydáním karty držiteli by SKC mělo nastavit kartě náhodný PIN i PUK. Jejich hodnoty by měly být vytištěny do neprůhledné PIN-obálky a spolu s kartou předány držiteli.

Součástí dodávky zhotovitele proto bude také:

- softwarový modul (knihovna, DLL) pro vygenerování a nastavení náhodných hodnot PIN a PUK karty,
- dokumentace technologie nastavení nových hodnot PIN a PUK PKI karty.

Dodaný software umožní volajícímu procesu zjistit nově vygenerované hodnoty pro vytištění do PIN-obálek. Software bude určen pro operační systém MS Windows.

Generování a zápis PIN a PUK bude realizován prostřednictvím standardního PC/SC rozhraní čtečního/zapisovacího zařízení.

### **Technické parametry HSM**

HSM modul Gold CSA 8000 PL220 je kryptografický PCI adaptér navržený pro bezpečné použití v kritických aplikacích. HSM modul splňuje vysoké požadavky na bezpečnost a aplikační přizpůsobivost.

#### **Charakteristické parametry:**

##### **Bezpečnost**

- V procesu certifikace FIPS 140-2 level 3
- Automatický výmaz paměti při detekci pokusu o fyzické vniknutí do modulu
- 4MB baterií zálohované bezpečné paměti pro uložení klíčů, certifikátů a dalších citlivých dat (baterie zajišťuje i zdroj energie pro mechanismy detekce a reakce na fyzické útoky)
- True Random Number Generator generátor náhodných čísel (splňuje kritéria ANSI X9.31 a je certifikován na FIPS 140)
- Podpora čipových karet pro transfer a zálohu klíčů
- Přímé propojení se čtečkou čipových karet a PIN pad zařízením

##### **Výkon**

- Jsou dostupné modely s různým výkonem
- Redundance pro škálovatelnost a rozložení výkonu a vysokou spolehlivost
- Podpora vícevláknového zpracování operací v rámci jednoho procesu (thread-safe)

##### **Správa**

- GUI aplikace pro správu (založené na Java)
- Řádkové utility pro správu (vhodné pro scripty)
- Nástroje pro bezpečnou aktualizaci firmware v produkčním prostředí
- Vzdálená správa síťových HSM

##### **Nástroje**

- PKCS#11 rozhraní
- Java JCA/JCE provider
- CSP pro Microsoft CryptoAPI
- implementace OpenSSL engine
- EFT command set pro podporu zpracování platebních transakcí
- SDK pro vývoj vlastních aplikací

##### **Kryptografické algoritmy**

- Symetrické – AES, DES, 3DES, CAST-128, RC2, RC4, SEED, další na vyžádání; podpora režimů zahrnuje ECB, CBC, OFB64, CFB-8 (BCF), další na vyžádání
- Asymetrické – RSA (do 4096 bitů), DSA, ECDSA (do 512 bitů), Diffie Hellman (DH), další na vyžádání

Kompletní výpis algoritmů, vč. podpisových a autentizačních schémat je popsán v příručkách jednotlivých kryptografických knihoven

#### Připojení

- PCI 2.2 rozhraní (32 nebo 64 bitů, 33 nebo 66MHz)
- podpora 3.3V i 5V úrovní

#### Rozměry

- 231mm x 18,7mm x 105,5mm

#### Napájení

- +3,3V/655mA, +5V/645mA, +12V/27mA

#### Provozní prostředí

- teplota 0° – 40°C
- relativní vlhkost 5 – 95% (nekondenzující)

### **Použitý server pro provoz HSM**

Pro instalaci HSM serveru bude použit HP ProLiant DL360R04p X3.0-2MB/800, 1GB SCSI. Tento server bude umístěn v RACKu objednatele, součástí dodávky není monitor, klávesnice, myš.

#### Charakteristické vlastnosti:

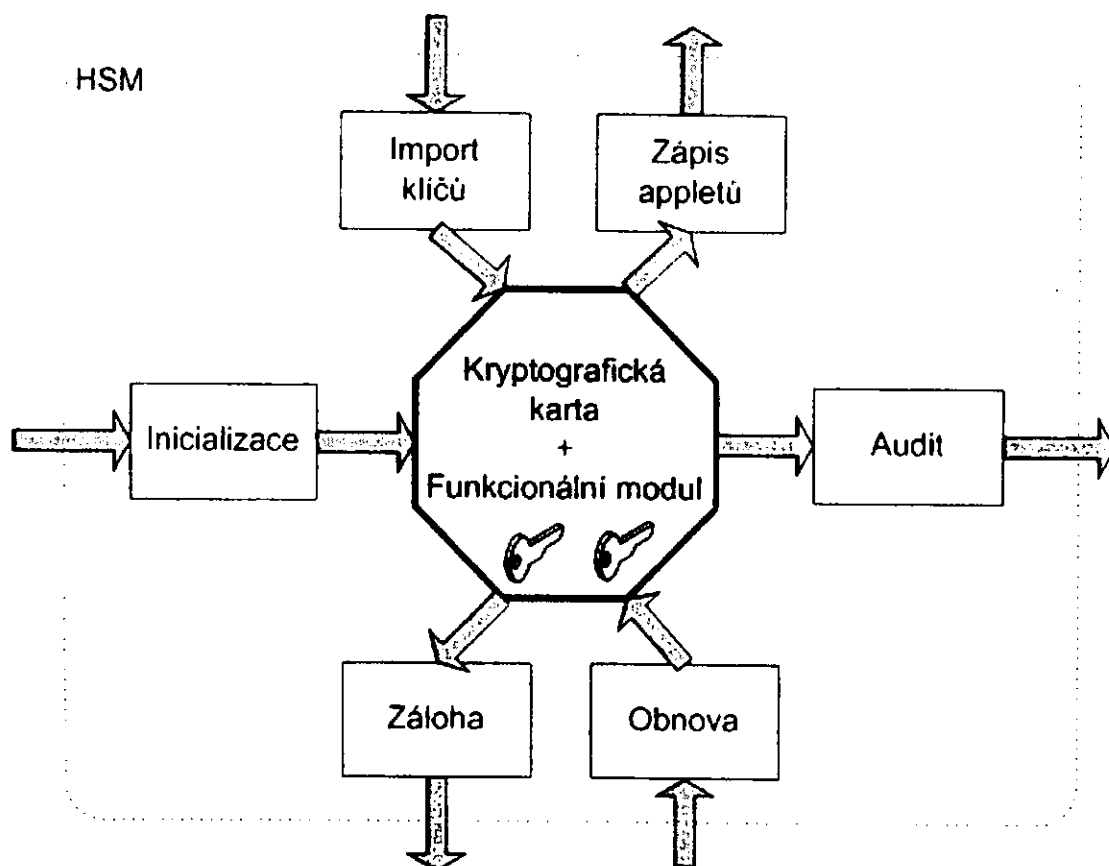
- Processor: Intel Xeon Processor 3.0-GHz/800MHz / 2-MB level 2 cache
- Memory: 1 GB (2 x 512 MB) PC2-3200 DDR2 400 SDRAM
- Network Controller: Embedded NC7782 Dual Port PCI-X 10/100/1000T Gigabit network adapter
- Storage Controller: Embedded U320 Smart Array 6i Controller
- Remote Management: Integrated Lights-Out (iLO) Standard Management (embedded)
- Power Supply One 460W power supply (redundant power supply optional)
- 460W HP redundant power supply with IEC cord only
- 72.8GB 15,000 rpm, U320 Universal Hot Plug drive, 1"
- HP DVD+R/RW 8X Slim

### **Modulární struktura HSM**

*Systém zápisu appletů (SZA)* je vybaven HSM pro zabezpečení zápisu appletů.

Podpora zápisu appletů však není jedinou funkcí HSM. HSM implementuje také řadu servisních funkcí, které obecně souvisí se správou klíčů:

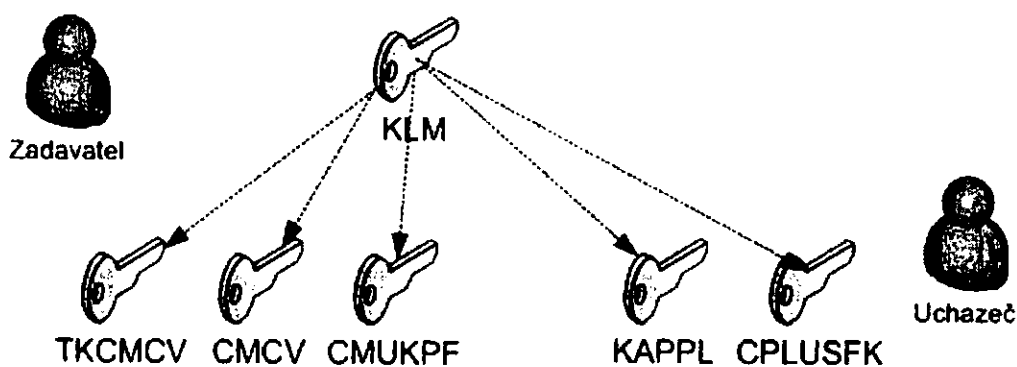
- *Inicializace* HSM – zajistí správnou inicializaci kryptografických tokenů na HSM, inicializaci bezpečnostního režimu HSM, generování KLM klíčů se zálohou na čipové kartě, tisk PIN obálek s hesly, atp..
- *Import klíčů* do HSM, pro bezpečné zavedení nových klíčů.
- *Záloha*, pro bezpečné zálohování klíčů. Klíče jsou před zálohováním zašifrovány (wrapovány) klíčem KLM.
- *Obnova*, pro bezpečnou obnovu klíčů. Obnovované klíče jsou do HSM vkládány zašifrované (wrapované) klíčem KLM. Po zavedení HSM provede dešifrování (unwrap) klíče. Klíč KLM je v případě potřeby rekonstruován z čipových karet.
- *Audit*, pro zaznamenání a kontrolu operací s klíči.



#### Modulární struktura HSM

Jádrem HSM je bezpečný hardware (kryptografická karta). Pro podporu zápisu appletů je nutno do kryptografické karty zavést *funkcionální modul* – software pro řízení jádra HSM.

#### Seznam klíčů v HSM



#### Schéma použitých klíčů v HSM

V HSM systému zápisu appletů budou uloženy tyto klíče:

- **KLM (Key Local Master)** – Master klíč HSM používaný pro zálohování ostatních klíčů. Je generován v HSM, rozložen Shamirovým algoritmem na čipové karty. Vlastníkem klíče a správcem čipových karet s jeho komponentami je SKC.

- **CMCV** (*Card Manager – Card Vendor*)– klíč/klíče chránící zápis/mazání appletů na dodané (čisté) kartě. Tento klíč musí být k dispozici, aby bylo možné do karet ukládat applety. Je obvyklé, že CMCV dodává dodavatel karet. Předpokládá se, že držitelem klíče bude SKC. Hodnota klíče bude vložena do HSM pověřenými pracovníky SKC. Klíč CMCV nikdy neopustí prostředí HSM (s výjimkou prováděné zálohy, šifrované klíčem KLM). Vlastníkem a držitelem klíče CMCV je SKC. Držitelem klíče CMCV může být také dodavatel karet.
- **TKCMCV** (*Transport Key – Card Manager – Card Vendor*). Šifrovací klíč pro bezpečné zavedení klíče CMCV do HSM. Vlastníkem a držitelem klíče TKCMCV je SKC. Držitelem klíče TKCMCV může být také dodavatel karet.
- **CMUKPF** (*Card Manager – UKP Family*) – rodinný klíč UKP pro ochranu zápisu/mazání appletů na kartě se zapsaným appletem (pro budoucí přihrávání dalších appletů na kartu). Klíč bude vygenerován přímo v HSM a jeho hodnota bude předána pověřeným pracovníkům SKC na třech PINových obálkách k uchování pro případné budoucí použití. (Místo generování v HSM je možné klíč do HSM ručně vložit). Vlastníkem a držitelem klíče CMUKPF je SKC.
- **KAPPL** (*Key Applet*) – klíč, kterým je zašifrována binární podoba appletu. Klíč KAPPL obecně slouží k šifrování dat (nejen binárního kódu appletu). Klíč je generován přímo v HSM, hodnota je při generování rozložena do tří obálek, které převezmou pracovníci zhotovitele. Vlastníkem a držitelem klíče je zhotovitel.
- **CPLUSFK** (*CryptoPlus Family Key*). Rodinný klíč appletu *CryptoPlus ProID* pro vytváření bezpečného kanálu mezi PKI kartou a čtečkou, např. při importu privátního klíče na kartu. Od CPLUSFK budou v procesu zápisu appletu diverzifikovány klíče pro jednotlivé karty. Vlastníkem a držitelem klíče je zhotovitel.

## Zavedení klíčů do HSM

Některé klíče budou generovány přímo v HSM, jiné budou do HSM ceremoniálně zavedeny. V následujících podkapitolách budou uvedeny podrobnosti zavedení / generování jednotlivých klíčů.

Postup zavedení klíčů, jejich vlastníkem je zhotovitel není uveden.

### Key Local Master (KLM)

KLM se generuje v HSM a je zálohován na N karet z nichž M postačuje k rekonstrukci klíče. Používá se například rozdělení na 3 karty, z nichž 2 postačují k rekonstrukci. Při poškození některé karty tak zůstávají 2 karty, z nichž lze KLM rekonstruovat.

### Card Manager – Card Vendor (CMCV)

CMCV je nutno do HSM ceremoniálně zavést. HSM podporuje 2 mechanismy zavedení klíče CMCV:

- CMCV do HSM zavedou 3 bezpečnostní úředníci, každý bezpečnostní úředník zavede pouze jeden fragment CMCV1, CMCV2 a CMCV3. V HSM bude z fragmentů sestaven kompletní CMCV = CMCV1 XOR CMCV2 XOR CMCV3. (V tomto případě není nutno použít klíče TKCMCV.)
- CMCV bude do HSM zaveden zašifrovaný klíčem TKCMCV a algoritmem 3DES. V HSM bude CMCV dešifrován pomocí TKCMCV. Šifrovaný CMCV = 3DES[TKCMCV](CMCV).

Pro kontrolu úspěšného zavedení HSM vypočte a zobrazí kontrolní sumu klíče CMCV:  
Kontrolní suma = 3 MSB z 3DES[CMCV](00 00 00 00 00 00 00 00)

Poznámka: 3 MSB jsou horní 3 byte z vygenerovaného kryptogramu (*Most Significant Bytes*).

### **Transport Key – Card Manager – Card Vendor (TKCMCV)**

V případě, že bude klíč CMCV zaváděn do HSM jako zašifrovaný, bude nutno před zavedením CMCV zavést do HSM klíč TKCMCV.

TKCMCV do HSM zavedou 3 bezpečnostní úředníci, každý bezpečnostní úředník zavede pouze jeden fragment TKCMCV1, TKCMCV2 a TKCMCV3. V HSM bude z fragmentů sestaven kompletní TKCMCV = TKCMCV1 XOR TKCMCV2 XOR TKCMCV3.

Pro kontrolu úspěšného zavedení HSM vypočte a zobrazí kontrolní sumu klíče TKCMCV:  
Kontrolní suma = 3 MSB z 3DES[TKCMCV](00 00 00 00 00 00 00 00)

### **Card Manager – UKP Family (CMUKPF)**

Klíč CMUKPF se do HSM může dostat těmito způsoby:

- bude vygenerován přímo v HSM a jeho hodnota bude předána pověřeným pracovníkům SKC na třech PINových obálkách k uchování pro případné budoucí použití.
- CMUKPF do HSM zavedou 3 bezpečnostní úředníci, každý bezpečnostní úředník zavede pouze jeden fragment CMUKPF1, CMUKPF2 a CMUKPF3. V HSM bude z fragmentů sestaven kompletní CMUKPF = CMUKPF1 XOR CMUKPF2 XOR CMUKPF3.

Pro kontrolu úspěšného zavedení HSM vypočte a zobrazí kontrolní sumu klíče CMUKPF: Kontrolní suma = 3 MSB z 3DES[CMUKPF](00 00 00 00 00 00 00 00)

- CMUKPF bude do HSM zaveden zašifrovaný transportním klíčem a algoritmem 3DES. V HSM bude CMUKPF pomocí transportního klíče dešifrován.

### **Výměna klíčů pro zápis appletů**

V průběhu zápisu PKI appletu bude klíč CMCV nahrazen klíčem, odvozeným od CMUKPF.

Správce karty používá 3 klíče:

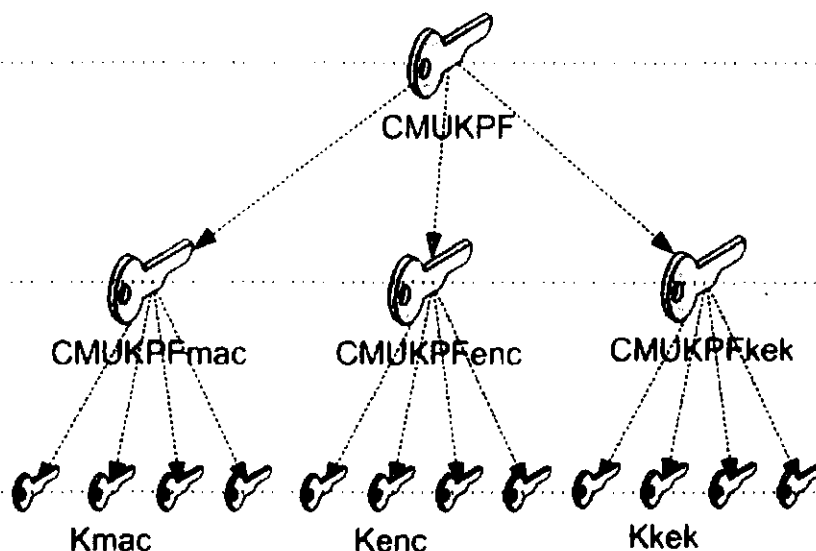
- klíč *Kmac* pro zajištění integrity,
- klíč *Kenc* pro utajení (šifrování) a
- klíč *Kkek* pro výměnu klíčů.

Platí, že všechny klíče karet budou odvozeny z jediného rodinného klíče CMUKPF podle

- typu klíče a
- unikátního čísla kontaktního čipu karty (*Card Reference Number, CRN*).

Typ klíče

CRN



#### Schéma výměny klíčů pro zápis appletů

Klíče *Správce karty*, které budou do čipu zapsány, budou generovány následovně:

- $K_{enc} = \text{divkey} (CMUKPF, CRN, TYP\_ENC)$
- $K_{mac} = \text{divkey} (CMUKPF, CRN, TYP\_MAC)$
- $K_{kek} = \text{divkey} (CMUKPF, CRN, TYP\_KEK)$

Funkce *divkey* provede nejprve diverzifikaci rodinného klíče CMUKPF podle typu klíče, následně teprve provede diverzifikaci podle konkrétního čísla karty.

Z klíče CMUKPF je tedy možné vypočítat tři podřízené rodinné klíče: CMUKPFenc, CMUKPFmac a CMUKPFkek a ty používat podle druhého způsobu odvození klíčů pro klíče karty. Toto řešení umožňuje např. předat třetí straně klíče, které umožní šifrovaný zápis appletu na kartu (klíče CMUKPFenc a CMUKPFmac), ale neumožní změnu klíče, protože HSM nebude mít k dispozici klíč CMUKPFkek ani výchozí rodinný klíč CMUKPF (ze kterého by bylo možné odvodit CMUKPFkek).

Detailní popis diverzifikace klíčů bude uveden v dokumentaci, která bude součástí dodávky zhotovitele.

### Podrobný popis procesu zápisu appletu

Proces zápisu appletu je řízen programem MRZAK, resp. obsluhou programu MRZAK.

Proces zápisu appletu do čipové karty se skládá z posloupnosti několika kroků:

- MRZAK požádá obsluhu o vložení další (prázdné) karty.
- Obsluha vloží kartu do čtečky, na čip karty jsou připojeny elektrické kontakty.
- MRZAK detekuje přítomnost karty ve čtečce. Oznámi obsluze zahájení procesu zápisu appletu, zaznamená událost do žurnálu a spustí proces zápisu.
- Kontaktnímu čipu se zapne napájení, zkontroluje se ATR karty a podle možností se urychlí komunikace s kartou pro zajištění maximální možné rychlosti zápisu appletu.
- MRZAK požádá HSM o výpočet kryptogramu pro autentizaci ke kartě. HSM vygeneruje kryptogram na základě údajů od MRZAK a klíče CMCV.
- MRZAK se autentizuje ke kartě.
- MRZAK požádá HSM o výpočty kryptogramů pro změnu klíče na kartě. S využitím služeb HSM je autentizační klíč pro nahrávání / mazání appletů bezpečně (šifrovanou

komunikací) změněn na klíč, který je vypočten jako jedinečný pro každou kartu z CRN a rodinného klíče CMUKPF.

- **MRZAK** požádá HSM o vlastní provedení zápisu appletu na čipovou kartu. HSM dešifruje applet pomocí klíče KAPPL a vygeneruje sekvenci binárních dat pro kartu. Vlastní ukládání appletu probíhá s využitím ustanoveného bezpečného spojení, applet se zapisuje na kartu s využitím šifrování.
- **MRZAK** podle konfiguračních dat provede instalaci appletu. V tomto kroku je alokován prostor pro data spravovaná appletem a je změněno ATR karty pro možnost snadného rozpoznání karty UKP.
- **MRZAK** s využitím služeb HSM provede vytvoření logické struktury karty (prostor pro klíče, certifikáty, root certifikáty, data, nastavení přístupových podmínek pro operace) podle konfiguračních dat. Konfigurační data budou vycházet z akceptovaného customizačního protokolu. Kartě se v tomto kroku přidělí CLN (*Card Logical Number*). Do čipu se bezpečným způsobem zavede klíč, odvozený od CPLUSFK. Vytvořená struktura se uzamkne proti možnosti následných změn.
- Je ukončena komunikace s kartou a je vypnuto napájení.
- Zpracování (zápis PKI appletu) karty je u konce. **MRZAK** tuto událost zaznamená do žurnálu.
- **MRZAK** oznámí obsluze dokončení procesu zápisu appletu. Požádá o vyjmutí karty ze čtečky.
- Zpracování pokračuje zápisem appletu do další karty – viz bod 1.

### **Autentizace k HSM**

Pro běžnou práci s modulem HSM je prováděna standardní autentizace heslem, pro citlivé operace (například vkládání klíčů na lokální konzole HSM) je zapotřebí kooperace více osob, např. jedna osoba má heslo pro přihlášení do systému a následně HSM vyžaduje dvě hesla osob pro autorizaci vložení klíče.

### **Autentizace do OPZA**

Autentizace a řízení přístupu do počítače *Obslužného pracoviště zápisu appletů* (OPZA) je realizováno prostředky operačního systému, na němž *OPZA* běží.

Obsluha *OPZA* i správce *Serveru HSM* se budou do počítačů autentizovat jménem a heslem. Obsluha *OPZA* nebude mít přístup (možnost autentizovat se) na *Server HSM*.

Předpokládá se, že Zadavatel deleguje pracovníka pověřeného správou uživatelských účtů pro *OPZA* i *HSM server*. Tento pracovník musí být držitelem oprávnění lokálního správce všech počítačů SZA.

### **Doba odezvy zápisu appletu**

Systém zápisu appletů bude dostatečně dimenzován, aby byl schopen v krátké době uložit PKI applet do velkého množství karet.

Na pracovišti *OPZA* bude možno zapsat PKI applet do kontaktního čipu za 90 sekund (v čase je započítána cca 20s manipulační rezerva). Jedno *OPZA* tedy bude schopno za 1 hodinu zapsat applety do 40 karet.

Zápis 1 appletu do 1 karty:

90 s

- Počet appletů, zapsaných na 1 *OPZA* za 1 hodinu:

40



- Počet appletů, zapsaných na 1 *OPZA* za den (8 hodin): 320
- Počet appletů, zapsaných na 1 *OPZA* za měsíc (20 prac. dní): 6400

Nabídka předpokládá, že budou dodána 4 pracoviště *OPZA*. Výkon celého systému charakterizují následující údaje:

- Počet appletů, zapsaných na 1 *OPZA* za 1 hodinu: 160
- Počet appletů, zapsaných na 1 *OPZA* za den (8 hodin): 1280
- Počet appletů, zapsaných na 1 *OPZA* za měsíc (20 prac. dní): 25600

**Dodané technické řešení bude schopno při jednosměnném provozu kompletně zpracovat dávku 50.000 čipových karet v průběhu 2 měsíců.**

Pozn.: Kompletním zpracováním dávky karet se rozumí zápis PKI appletů do všech dodaných karet. Doba zpracování dávky je časový interval od převzetí „prázdných“ karet do předání karet s PKI appletem. Předpokládá se, že klíče a konfigurace potřebné pro zápis appletů budou do SZA, resp. *HSM Serveru* zavedeny před převzetím karet.

Pokud by bylo třeba proces zápisu appletu urychlit, lze to provést těmito způsoby:

- Zavedením vícesměnného provozu na pracovištích *OPZA*.
- Zvýšení počtu pracovišť *OPZA*. Systém SZA lze škálovat v rozsahu od stávajících 4 *OPZA* až do 200 *OPZA*. Při dalším zvětšování počtu *OPZA* by bylo vhodné implementovat do systému výkonnější HSM.

## **Požadavky na součinnost ze strany MHMP**

Implementace řešení zápisu PKI appletů do kontaktních čipů vyžaduje součinnost zhotovitele a objednatele (resp. MHMP) v těchto oblastech:

- Objednatel zajistí hybridní čipové karty dle specifikace v ZD.
- Objednatel zajistí od dodavatele karet klíč CMCV pro zápis appletů do čipu.
- Při podpisu smlouvy objednatel zhotoviteli sdělí přesný typ použitých karet, způsob předání klíčů CMCV a způsob diverzifikace klíčů pro jednotlivé karty. Bez těchto údajů není zhotovitel schopen zahájit přípravu implementace.
- Objednatel zajistí místo v rack-u pro uložení *HSM Serveru*
- Objednatel zajistí síťové prvky (IP adresy, kabely, switche, routery) k propojení počítačů SZA. Zadavatel zajistí oddělení LAN SZA od okolních informačních systémů.
- Objednatel zajistí prostory pro instalaci SZA, včetně elektrických sítí. Do těchto prostor musí být umožněn přístup pracovníkům zhotovitele – alespoň k provedení implementace řešení.
- Objednatel deleguje pracovníky pro ceremonii zavedení / převzetí klíčů HSM.
- Objednatel zajistí správu lokálních uživatelských účtů na počítačích SZA. Vyhradí uživatelské účty pro přístup pracovníků zhotovitele. Alespoň pro implementaci řešení musí mít zhotovitel oprávnění administrátora do počítačů *OPZA* i *HSM Serveru*.
- Objednatel zajistí obsluhu počítačů *OPZA* pro provádění zápisu appletů.
- Objednatel do 10 dnů od podpisu smlouvy předá definovaný personalizační profil PKI appletu a customizaci middleware dle přílohy č. 6 této smlouvy. Zhotovitel se zavazuje poskytnout potřebnou konzultační podporu.

**Příloha č. 5**

**Pojistná smlouva (ověřená fotokopie)** ke smlouvě „Smlouva o poskytnutí služby „Řešení PKI pro čipovou kartu““ č. objednatele INO/40/05/001121/2006, č. zhotovitele 246/06

O P I S

**AIG**

**AIG Czech Republic**

A Member of American International Group, Inc.



**Pojistitel**

**AIG CZECH REPUBLIC pojišťovna, a.s.**

zapsána v obchodním rejstříku vedeném Městským soudem v Praze,  
oddíl B, vložka 7340, IČ 26 47 76 96

**se sídlem:**

Praha 1, V Celnici 1031/4, PSČ 110 00, Česká republika

**jednající:**

Bc. Jindřich Bajer, zmocněný pro záležitosti smluvní

a

**Pojistník**

**MONET+, a. s.**

zapsána v obchodním rejstříku vedeném Krajským soudem v Brně,  
oddíl B, vložka 3351, IČ 26 21 77 83

**se sídlem:**

Zlín, Štípa, Za Dvorem 505, PSČ 763 14

**jednající:**

Ing. Miroslav Janda, místopředseda představenstva

**adresa pro  
doručování:**

Zlín, Štípa, Za Dvorem 505, PSČ 763 14

**uzavírají prostřednictvím**

**zplnomocněného  
makléře**

**Aura Lloyd s.r.o.**

zapsána v obchodním rejstříku vedeném Městským soudem v Praze,  
oddíl C, vložka 84047, IČ 264 65 019

**Pojistnou smlouvu č. 7100 4498 06**

## **POJIŠTĚNÍ PROFESNÍ ODPOVĚDNOSTI**

Podpisy vyjadřují strany souhlas s dále uvedenou *pojistnou smlouvou*, *pojistník* potvrzuje správnost údajů uvedených v příloženém dotazníku a dále potvrzuje, že se seznámil s příloženými pojistnými podmínkami a že s nimi souhlasí.

**Pojistník:**

**Pojistitel:**

Ve Zlíně dne 24.03.2006

V Praze dne 27.března 2006

**Podpis:**

**Jméno:**

Ing. Miroslav Janda

**Funkce:**

Místopředseda představenstva

*Jindřich Bajer*

Bc. Jindřich Bajer

Upisovatel pojištění finančních rizik

**Razítko**

**MONET+, a.s. ®**

Za Dvorem 505, 763 14 Zlín - Štípa  
IČ: 26217783, DIČ: CZ26217783  
tel.: +420 577 110 411, fax: +420 577 914 557

**AIG**

**AIG CZECH REPUBLIC**

pojišťovna, a.s.

V Celnici 1031/4, PSČ 110 00, Praha 1

IČ: 26 47 76 96

-10-



NÁLEŽITOSTI POJISTNÉ SMLOUVY Č. 7100 4498 06

**Pojistná doba**

Pojistná smlouva se sjednává na dobu určitou.

Pojištění vznikne dnem 01/ 04/ 2006

a je sjednáno na *pojistnou dobu*, která skončí dnem

31/ 03/ 2007

**Pojištěný**

MONET+, a.s. zapsána v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl B, vložka 3351, IČ 26 21 77 83

**Odborné služby poskytované pojištěným**

Poskytování software dle výpisu z obchodního rejstříku vedeném Krajským soudem v Brně, oddíl B, vložka 3351, IČ 26 21 77 83.

**Pojistná událost**

*Pojistnou událostí se pro účely těchto podmínek rozumí uplatnění nároku vůči pojištěnému tak, jak je definováno v podmínkách.*

Pojistným nebezpečím je právními předpisy stanovená odpovědnost *pojištěného*, jejíž rozsah je blíže specifikován v *podmínkách*.

**Limit pojistného plnění**

Limit pojistného plnění

15 000 000,- Kč za jednu a za všechny *pojistné události* v průběhu *pojistné doby*

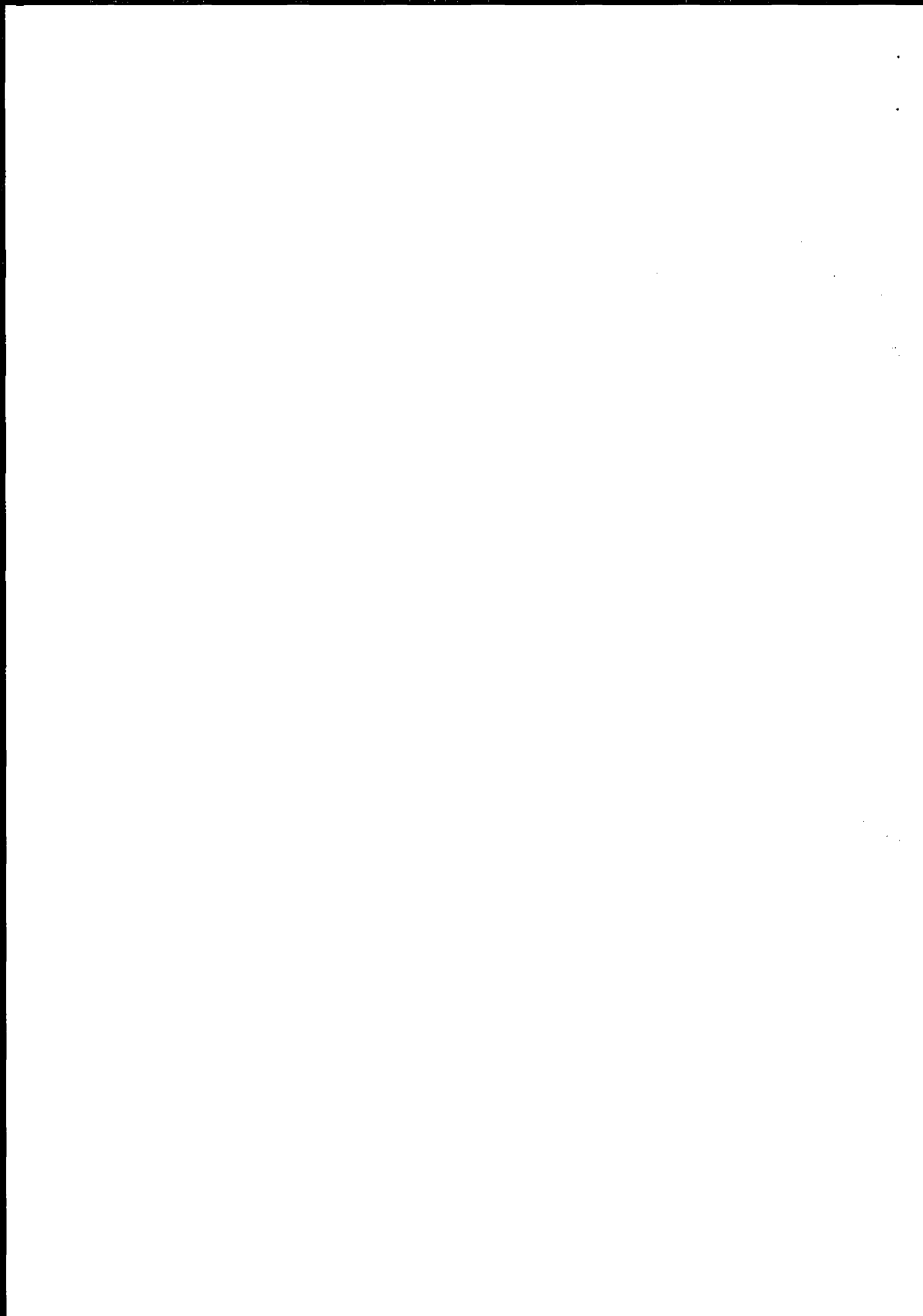
Limit pojistného plnění v souvislosti se zachraňovacími náklady podle §32, odst. 2 zákona o pojistné smlouvě

250 000,- Kč

**Vlastní vrub**

Vlastní vrub

500 000,- Kč z každé *pojistné události*



## Pojistné

Pojistné	324 000,- Kč
	počet splátek čtyři
	po Kč 81 000,-
	splatnost do:
1. splátka	24.04.2006
2. splátka	01.07.2006
3. splátka	01.10.2006
4. splátka	01.01.2007

## Splatnost pojistného

Pojistné je splatné na účet *pojistitele* č. 201 850 0205/2600 Citibank a.s., Evropská 178, Praha 6, konstantní symbol 3558, ref./var. symbol: 7100449806, v termínech splatnosti stanovených v této *pojistné smlouvě*.

## Přílohy pojistné smlouvy

Příloha 1:	Pojistné podmínky pro pojištění profesní odpovědnosti CZPI-01-01/2005
Příloha 2:	Výpis z obchodního rejstříku <i>pojistníka</i>
Příloha 3:	Kopie vyplněného dotazníku <i>pojištěného</i>

## Smluvní ujednání

### Vyluka investičního poradenství

Dodatečně k ustanovení článku 4 *podmínek* se ujednává, že se pojištění nevztahuje na nárok, který by *poškozený* vznesl vůči *pojištěnému* v souvislosti se svojí neúspěšnou investicí (týkající se nejenom cenných papírů a/nebo nemovitého majetku), uskutečnou na základě doporučení nebo prognózy doporučené *pojištěným*, nebo na takový nárok, který lze takové investici přisoudit a která se uskutečnila na základě doporučení nebo prognózy doporučené *pojištěným*. Tato vyluka se však nevztahuje na právní radu poskytnutou *pojištěným* ve spojitosti s takovým investičním doporučením nebo prognózou

### Vyluka počítačového viru

Dodatečně k ustanovení článku 4 *podmínek* se ujednává, že se pojištění nevztahuje na nárok přímo nebo nepřímo vyplývající z počítačového viru, který byl zaveden *pojištěným* nebo jinou osobou, která vlastní nebo odpovídá za počítačový systém nebo s vědomím *pojištěného* nebo této jiné osoby;

### Vyluka neoprávněného přístupu nebo použití

Dodatečně k ustanovení článku 4 *podmínek* se ujednává, že se pojištění nevztahuje na nárok vyplývající ze skutečnosti, že *pojištěný* porušil bezpečnostní opatření k zabránění neoprávněného přístupu nebo použití počítačového systému nebo programu.

### Článek 19. DEFINICE se doplňuje o následující pojem:

**Počítačový systém nebo program** znamená jakýkoliv počítač, zařízení na zpracování dat, média nebo jejich část, nebo systém pro uchování a nabytí dat, nebo komunikační systém, síť, protokol nebo jeho





část, nebo zařízení k uchování dat, mikročip, integrovaný obvod, taktovací systém pracující v reálné čase nebo podobné zařízení nebo jakýkoliv počítačový software (včetně aplikačního software, operačních systémů, runtime prostředí nebo kompilátorů), firmware nebo mikrokód

#### **Ujednání o slevě za víceleté trvání pojištění**

Procentní sleva z pojistného: 3,5%  
Doba platnosti tohoto ujednání 5 let

počátek platnosti: 01/04/2006  
konec platnosti: 31/03/2011

*Pojistitel* na základě tohoto ujednání poskytne *pojistníkovi* uvedenou slevu na pojistném za každý rok trvání tohoto ujednání dopředu na začátku *pojistného období*. Vždy ke konci sjednané *pojistné doby* mohou být příslušné *pojistné částky* nebo limity nebo jiné podmínky *pojistné smlouvy* upraveny.

V případě, že *pojistná smlouva* nebude obnovena nebo znovu uzavřena po celou dobu platnosti tohoto ujednání, *pojistník* je povinen vrátit *pojistiteli* poskytnutou slevu.

Sleva za víceleté trvání pojištění bude poskytnuta pouze v případě bezeškodního průběhu pojištění.

Pozn.: Toto ujednání v žádném případě neupravuje trvání *pojistné doby* uvedené v *pojistné smlouvě*. Výše uvedená „doba platnosti tohoto ujednání“ stanovuje období, během kterého je za případný dlouhodobý pojistný vztah poskytována sleva.

#### **Limit pojistného plnění v souvislosti se zachraňovacími náklady**

Zachraňovacími náklady ve smyslu tohoto ustanovení se rozumí účelně vynaložené náklady, které *pojistník* vynaložil v souladu s §32, odst. 2 zákona o pojistné smlouvě. *Pojistitel* však uhradí pouze takové náklady, které *pojistník* vynaložil v souvislosti s *odbornými službami* poskytovanými *pojištěným* a tyto služby jsou pojištěnou činností. *Pojistitel* neuhradí zachraňovací náklady vynaložené na takové činnosti či služby poskytované *pojištěným*, které jsou standardně vyloučeny v *pojistných podmínkách* nebo *pojistné smlouvě*.

#### **Vyluka válečného konfliktu**

Dodatečně k ustanovení článku 4 *podmínek* se ujednává, že se pojištění nevztahuje na *nárok*, který je zcela nebo částečně, přímo nebo nepřímo způsoben, založen či vyplývá:

- a) z války, válečného aktu, občanské války, invaze, povstání, převratu, užití ozbrojené síly nebo uchvacení vlády ozbrojenou silou; nebo
- b) ze záměrného užití ozbrojené síly k zastavení, předejití nebo zmírnění zjevného nebo předpokládaného teroristického činu; nebo
- c) z jakéhokoli teroristického činu.

Pro účely této vyluky se pojmy válka a teroristický čin definují takto:

- a) válka znamená válku, ať vyhlášenou či nikoliv, nebo jakékoli válečné akce včetně užití ozbrojené síly jakýmkoliv svrchovaným státem k dosažení ekonomických, územních, národnostních, politických, rasových, náboženských nebo jiných cílů,
- b) teroristický čin (činy) znamená bezprostřední užití nebo hrozbu užití síly nebo násilí zaměřeného na způsobení škody, újmy, poškození nebo narušení, nebo spáchání činu nebezpečného životu nebo majetku, proti jakémukoliv jednotlivci, majetku či jakékoli vládě, s uvedením cílů sledujících zájmy hospodářské, etnické, národnostní, politické, rasové nebo náboženské, nebo bez uvedení těchto cílů, ať vyhlášených či nikoliv. Loupeže nebo jiné trestné činy, spáchané především pro osobní prospěch nebo činy vyplývající především z osobních vztahů mezi pachatelem (pachateli) a obětí (oběťmi) se nepovažují za teroristické činy.

Teroristický čin rovněž zahrnuje jakýkoliv čin, který je mezinárodně jako takový uznán nebo potvrzen



**AIG CZECH REPUBLIC pojišťovna, a.s.**

Pokud není v těchto smluvních ujednáních uvedeno jinak, pak ustanoveními těchto smluvních ujednání nejsou v žádném ohledu dotčena kterákoli jiná ustanovení *podmínek*, které jsou nedílnou součástí pojistné smlouvy.

**Ověření - vidimace**

Ověřuji, že tento opis složený z 5 listů  
doslovně souhlasí s listinou, z níž byl  
pořízen, složenou z 5 listů.  
Ve Zlíně dne 21-08-2006

**Monika Mikulková**

notářská tajemnice

JUDr. Evy Dufkové, notáře ve Zlíně





# POJISTNÉ PODMÍNKY PRO POJIŠTĚNÍ PROFESNÍ ODPOVĚDNOSTI

## ÚVODNÍ USTANOVENÍ

Vztah pojistitele, pojistníka a pojištěného v souvislosti s pojištěním profesní odpovědnosti se řídí (1) pojistnou smlouvou, (2) smluvními ujednáními k pojistné smlouvě a (3) těmito podmínkami. Dokumenty (2) a (3) tvoří nedílnou součást pojistné smlouvy. Pojistná smlouva nebo podmínky se mohou rovněž odvolávat na dotazník vyplněný pojistníkem a pojištěným(i).

## 2. POJISTNÉ NEBEZPEČÍ, POJISTNÁ UDÁLOST

- 2.1 Pojištění se sjednává pro případ právním předpisem stanovené odpovědnosti pojištěného za škodu, která vznikla poškozenému v důsledku vadného poskytnutí odborných služeb, včetně případů vadného poskytnutí odborných služeb třetí osobou (subdodavatelem) za pojištěného jeho jménem, pokud za tyto služby vznikla odpovědnost pojištěnému.
- 2.2 Pojistnou událostí se pro účely těchto podmínek rozumí uplatnění nároku vůči pojištěnému, pokud poškozený sdělil nárok pojištěnému poprvé v průběhu pojistné doby a pokud k vadnému poskytnutí odborných služeb, ze kterého nárok vyplývá, došlo v průběhu pojistné doby (tzv. „claims made basis“); pokud není v pojistné smlouvě dohodnuto jinak, nárok na pojistné plnění vzniká, pouze pokud byla pojistná událost pojistiteli nahlášena v průběhu pojistné doby.
- 2.3 V pojistné smlouvě je možné dohodnout, že se pojištění vztahuje i na nároky vyplývající z vadného poskytnutí odborných služeb, ke kterému došlo v dohodnutém období před uzavřením pojistné smlouvy (tzv. retroaktivní datum).
- 2.4 Pojistnou událostí není událost způsobená úmyslně pojištěným, pojistníkem nebo jinou osobou z podnětu některého z nich.
- 2.5 Vše nároků vyplývajících z jedné příčiny, resp. z jednoho vadného poskytnutí odborných služeb, je pro účely těchto podmínek považováno za jednu pojistnou událost bez ohledu na počet poškozených.

## 3. ROZSAH POJISTNÉHO PLNĚNÍ

- 3.1 Pojistitel poskytne v souladu s ustanoveními pojistné smlouvy a těchto podmínek pojistné plnění v rozsahu:
  - a) peněžité náhrady škody, za kterou pojištěný odpovídá ve výši, v jaké o ní rozhodl soud nebo v jaké došlo se souhlasem pojistitele k smíru či mimosoudnímu narovnání, a to až do výše limitu pojistného plnění; a / nebo
  - b) náhrady nákladů právního zastoupení, které vznikly pojištěnému v souvislosti s obranou proti uplatněnému nároku, a to i v případě, že tento nárok je neopodstatněný, neoprávněný nebo vedený s podvodným úmyslem; náklady právního zastoupení se započítávají do celkového pojistného plnění pro účely zjištění, zda byl dosažen limit pojistného plnění.
- 3.2 Pojistitel poskytne pojistné plnění v rozsahu podle článku 3.1 (a) poškozenému a pojistné plnění v rozsahu náhrady nákladů podle článku 3.1 (b) pojištěnému. Poškozený však nemá přímé právo na poskytnutí pojistného plnění proti pojistiteli.

## 4. VÝLUKY

- 4.1 Pojištění uzavřené podle těchto podmínek se nevztahuje na nároky:
  - 4.1.1 Nároky vznesené mateřskou / dceřinou společností pojištěného nebo jinou společností, která je součástí stejného koncernu jako pojištěný nebo osobou, které má na společnosti pojištěného majetkový podíl nebo se účastní na jeho řízení; tato výluka však nebude uplatněna, pokud nároky byly vůči výše uvedeným osobám vzneseny třetí stranou a vyplývají z odborných služeb, které poskytl pojištěný.
  - 4.1.2 Škody na zdraví nebo věcné škody
    - a) za škody na zdraví nebo věcné škody; tato výluka však nebude uplatněna, pokud ke škodě na zdraví nebo věcné škodě došlo v důsledku toho, že pojištěný při poskytování odborných služeb porušil zákonem stanovenou povinnost péče; a
    - b) za škody na zdraví nebo věcné škody v případě, že se pojištěný smluvně zavázal k vyššímu stupni péče než je pro odborné služby, které poskytuje, obvyklé.
  - 4.1.3 Smluvní odpovědnost
 uplatněné v důsledku odpovědnosti, kterou pojištěný smluvně převzal nad rámec stanovený právními předpisy; tato výluka však nebude uplatněna, pokud škoda nastala z důvodu vadného poskytnutí odborných služeb a odpovědnost by ve stejném nebo větším rozsahu nastala i v případě neexistence takové smlouvy.
  - 4.1.4 Nesprávný odhad nákladů
 uplatněné v souvislosti s nesprávným odhadem nákladů spojených s poskytnutím odborných služeb pojištěným;
  - 4.1.5 Náklady na opravy
 uplatněné v souvislosti s náklady vynaloženými na opravy, doplnění nebo opětovné provedení odborných služeb poskytovaných pojištěným;

- 4.1.6 Pokuty, penále a jiné sankce, zajištění
 vyplývající z pokut, penále nebo jiné peněžité sankce uložené pojištěnému nebo pojistníkovi, a dále vyplývající z ručení, zajištění, prohlášení nebo ujištění, které pojištěný poskytl třetí osobě;
- 4.1.7 Klamavá reklama
 za škody způsobené klamavou reklamou vztahující se k odborným službám pojištěného, nekalou soutěží nebo porušením předpisů na ochranu spotřebitele;
- 4.1.8 Trestný čin
 vyplývající z úmyslného trestného činu;
- 4.1.9 Akty státních a regulačních orgánů
 vyplývající z aktu státního nebo jiného regulačního orgánu, zájmové, profesní nebo jiné organizace nebo obchodní komory; tato výluka se však neuplatní na nároky vyplývající z vadného poskytnutí odborných služeb těmto institucím;
- 4.1.10 Úpadek
 vyplývající přímo nebo nepřímo z úpadku pojištěného;
- 4.1.11 Průmyslové vlastnictví
 vyplývající z porušení práv k předmětům průmyslového vlastnictví nebo práv k obchodnímu tajemství;
- 4.1.12 Společný podnik (joint venture), sdružení
 za škody, za které pojištěný odpovídá v souvislosti s poskytováním odborných služeb za třetí osobu, se kterou tvoří pojištěný společný podnik, jejím jménem nebo jako účastník sdružení; tato výluka se však neuplatní, pokud pojistitel předem souhlasil se zahrnutím takových nároků do pojištění a výslovně toto upřesnil v pojistné smlouvě;
- 4.1.13 Znečištění
  - a) vyplývající přímo nebo nepřímo ze skutečného, údajného nebo hrozícího úniku, znečištění nebo zamoření škodlivinami;
  - b) vyplývající přímo nebo nepřímo z ionizujícího záření nebo radioaktivního záření pocházejícího z jaderného paliva nebo jaderného odpadu vzniklého při spalování jaderného paliva;
  - c) vyplývající přímo nebo nepřímo z působení radioaktivních, jedovatých, výbušných nebo jinak nebezpečných vlastností jaderného materiálu, jaderného zařízení nebo jaderné součásti jakéhokoliv zařízení;
- 4.1.14 Nároky uplatněné podle práva USA nebo Kanady
 uplatněné:
  - a) na území USA nebo Kanady a jiného území, které jsou pod správou USA nebo Kanady nebo se řídí jejich právním řádem; nebo
  - b) za účelem výkonu rozhodnutí jakéhokoliv soudu USA nebo Kanady nebo soudu příslušného na území, které jsou pod správou USA nebo Kanady nebo se řídí jejich právním řádem;
- 4.1.15 Válka, občanské nepokoje a terorismus
 vyplývající přímo nebo nepřímo z války, ať byla vyhlášena nebo nikoli, občanské války, občanských nepokojů, sabotáže, nepřátelských aktů nebo terorismu.
- 4.2 Pokud bude v pojistné smlouvě dohodnuto, že se některá z výluk neuplatní, není tím dotčeno uplatnění ostatních výluk. V pojistné smlouvě mohou být rovněž dohodnuty další výlučky.
5. VLASTNÍ VRUB POJIŠTĚNÉHO
  - 5.1 Pojistitel poskytne pojistné plnění ve výši, v jaké škoda přesahuje vlastní vrub. Pro účely zjištění, zda bylo dosaženo limitu pojistného plnění, se však k poskytnutému pojistnému plnění vlastní vrub nepřičítá. Za žádnou pojistnou událost, při které by pojistné plnění nepřevýšilo částku vlastního vrubu, pojistné plnění nenáleží.
  - 5.2 Pokud není v pojistné smlouvě dohodnuto jinak, vlastní vrub se vztahuje na každou pojistnou událost.
  - 5.3 Vlastní vrub nese pojištěný a jedná se o riziko, které nesmí být pojištěno.
6. PRAVA A POVINNOSTI ÚČASTNÍKŮ POJIŠTĚNÍ
  - 6.1 Pojistník je povinen seznámit pojištěného s obsahem pojistné smlouvy.
  - 6.2 Pojistník a pojištěný jsou na základě zákonných norem povinni pravdivě a úplně odpovědět na všechny písemné dotazy pojistitele týkající se pojistné smlouvy. To platí i v případě, že jde o změnu pojistné smlouvy.
  - 6.3 Pojistník je povinen sdělit pojistiteli pokud možno předem, jinak bez zbytečného odkladu, všechny změny, které v průběhu pojistné doby nastanou ve skutečnostech, o kterých pojistitele informoval při sjednávání pojištění.
  - 6.4 Při porušení povinností pojistníka nebo pojištěného uvedených v odstavci 6.2 může pojistitel od pojistné smlouvy odstoupit podle zákonných norem, jestliže by při pravdivém a úplném zodpovězení dotazů pojistnou smlouvou neuzavřel.
  - 6.5 Porušil-li pojistník nebo pojištěný při sjednávání pojistné smlouvy nebo při její změně některou z povinností uvedených v zákonných normách, těchto podmínkách nebo v pojistné smlouvě a bylo-li v důsledku toho stanoveno nižší pojistné, může pojistitel přiměřeně snížit pojistné plnění.
  - 6.6 Pokud mělo porušení povinností uvedených v zákonných normách, těchto podmínkách nebo v pojistné smlouvě podstatný vliv na vznik pojistné události, její průběh nebo na zvětšení rozsahu jejích následků anebo na zjištění nebo určení výše pojistného plnění, může



*pojistitel* pojistné plnění sníží úměrně tomu, jaký vliv mělo toto porušení na rozsah jeho povinnosti plnit.

*Pojistitel* může plnění z *pojistné smlouvy* odmítnout, jestliže příčinou *pojistné události* byla skutečnost, o které se dozvěděl až po vzniku *pojistné události* a kterou nemohl zjistit při sjednávání pojištění nebo jeho změně v důsledku úmyslně nebo z nedbalosti nepravdivé nebo neúplně zodpovězených písemných dotazů, a jestliže by při znalosti této skutečnosti v době uzavření *pojistné smlouvy* tuto smlouvu neuzevřel, nebo ji uzavřel za jiných podmínek. Stejně oprávnění má *pojistitel* v případě, že *pojištěný* uvedl při uplatňování práva na plnění z *pojistné smlouvy* vědomě nepravdivé nebo hrubě zkreslené údaje týkající se rozsahu *pojistné události* nebo podstatné údaje týkající se této události zamlčel. Dnem doručení oznámení o odmítnutí pojistného plnění zanikne i pojištění.

6.8 *Pojistitel* poskytne pojistné plnění podle *pojistné smlouvy* pod podmínkou, že *pojištěný*:

- řádně dbal na to, aby *pojistná událost* nenastala;
- neporušoval zákonné povinnosti směřující k tomu, aby hrozící újma byla odvrácena nebo aby bylo zmenšeno nebezpečí, které by *pojistnou událost* mohlo způsobit;
- vyvinul veškeré úsilí, které lze na něm rozumně vyžadovat, aby zmenšil újmu, která mu v důsledku *pojistné události* vznikla nebo mohla vzniknout; a
- umožnil *pojistiteli* zkontrolovat a přezkoumávat *pojistné riziko* a poskytnul mu potřebnou součinnost a informace k ohodnocení *pojistných rizik*. Pokud se prokáže, že porušení výše uvedených podmínek mělo vliv na vznik *pojistné události*, rozsah nebo výši škody, může *pojistitel* pojistné plnění snížit úměrně tomu, jaký vliv mělo toto porušení na rozsah jeho povinnosti plnit.

6.9 *Pojistník* a *pojištěný* jsou v případě *pojistné události* povinni poskytovat *pojistiteli* součinnost, kterou lze na nich rozumně vyžadovat, zejména účasti při soudních nebo jiných řízeních, zajištěním a poskytnutím důkazů a jinou součinnost potřebnou při vyřešení nároku

## 7. POJISTNÉ PLNĚNÍ

7.1 *Pojistitel* poskytne pojistné plnění podle *pojistné smlouvy* za všechny škody a náklady právního zastoupení, které vznikly v souvislosti s *pojistnými událostmi*, které nastaly v průběhu *pojistné doby*, bez ohledu na počet poškozených maximálně však do výše limitu pojistného plnění uvedeného v *pojistné smlouvě*. *Pojistná smlouva* může stanovit limit pojistného plnění pro jednotlivé části pojistného plnění (sublimit). Část pojistného plnění, na kterou byl aplikován sublimit se pro účely zjištění, zda bylo dosaženo limitu pojistného plnění, počítá se všemi dalšími částmi pojistného plnění.

7.2 Výše pojistného plnění je ve smyslu článku 7.1 omezena limitem pojistného plnění, který byl dohodnut v *pojistné smlouvě* platné v okamžiku, kdy došlo k *pojistné události* bez ohledu na to, zda byla uzavřena nová *pojistná smlouva*, která na příslušnou *pojistnou smlouvu* navazuje.

7.3 Pojistné plnění je splatné do 15 dnů po skončení šetření nutného ke zjištění důvodu a rozsahu povinnosti *pojistitele* plnit. Pojistné plnění se poskytuje v české měně, pokud *pojistná smlouva* nestanoví jinak. Pro přepočet zahraniční měny na českou je rozhodující kurs „devizový střed“ vyhlášený Českou národní bankou ke dni *pojistné události*.

7.4 *Pojistitel* poskytne *pojištěným* přiměřenou zálohu na náklady právního zastoupení podle článku 3.1 (b) v průběhu jednání o nároku.

7.5 Pokud byla záloha vyplacena na základě nároku, který je z tohoto pojištění vyloučen, je *pojištěný* povinen neprodleně *pojistiteli* tuto zálohu vrátit.

## 8. UPLATNĚNÍ NÁROKU NA POJISTNÉ PLNĚNÍ

8.1 Nárok se považuje za poprvé uplatněný poškozeným vůči *pojištěnému* v okamžiku, kdy *pojištěný* obdržel písemné vyjádření poškozeného, ve kterém je *pojištěný* označen za odpovědného za následky *vadného poskytnutí odborných služeb* nebo je vyjádřen záměr tak učinit; nebo, pokud poškozený takové vyjádření neučiní:

- podání návrhu na zahájení civilního nebo správního řízení ve věci náhrady škody, včetně nemajetkové újmy, který proti *pojištěnému* podal poškozený;
- rozhodnutí o zahájení trestního stíhání, které bylo zahájeno pro trestný čin, kterého se měl dopustit *pojištěný* nebo jeho zaměstnanec

8.2 Oznámení škodné události musí *pojištěný* učinit bez zbytečného odkladu v průběhu *pojistné doby*

8.3 Pokud se *pojištěný* v průběhu *pojistné doby* dozví o skutečnostech, které mohou důvodně zakládat budoucí nárok vůči *pojištěnému* a tyto skutečnosti s dostatečnými detaily a podklady oznámí písemně *pojistiteli*, bude se nárok vznesený v souvislosti s těmito skutečnostmi považovat za uplatněný v době, kdy byly tyto skutečnosti *pojistiteli* oznámeny poprvé

8.4 *Pojištěný* je dále povinen:

- neprodleně předat *pojistiteli* všechny dokumenty dokládající, že byl vůči němu vznesen nárok, zahájení nebo průběh soudního nebo jiného řízení v souvislosti s nárokem, a další dokumenty potřebné pro šetření *pojistné události*;

b) na vyžádání *pojistitele* zajistit další podklady a důkazy, které souvisí s *pojistnou událostí*, a poskytnout *pojistiteli* náležitou součinnost.

8.5 V případě, že *pojistitel* odmítne obnovit pojištění nebo pojištění zanikne z jiného důvodu než pro neplacení pojistného, může *pojištěný* oznámit *pojistiteli*, že byl proti němu uplatněn nárok i v průběhu 60 dnů, které následují po zániku pojištění. To platí za předpokladu, že k *vadnému poskytnutí odborných služeb* došlo nejpozději k datu zániku pojištění.

8.6 Více nároků vyplývajících z jednoho *vadného poskytnutí odborné služby* bude považováno za jednu *pojistnou událost*. Pro určení data, kdy nastala *pojistná událost* a kdy byla nahlášena *pojistiteli*, jsou rozhodná data, kdy poškozený poprvé vůči *pojištěnému* uplatnil nárok a kdy byl tento nárok poprvé nhlášen *pojistiteli*.

8.7 *Pojištěný* není bez předchozího písemného souhlasu *pojistitele* oprávněn:

- učinil jakýkoli úkon, kterým byl uznával svoji odpovědnost či činil jakoukoli jinou otázkou v této souvislosti nespornou;
- uznat nebo smírně vyřešit jakýkoli nárok, včetně nároku na náhradu nákladů;
- nevyužít všech nástrojů, které má k obraně proti uplatněnému nároku, včetně dostupných opravných prostředků.

8.8 *Pojistník* a *pojištěný* jsou povinni vyvinout veškeré úsilí, které lze na nich rozumně vyžadovat, zejména účastnit se soudních nebo jiných řízení, zajistit a poskytnout důkazy a učinit další kroky potřebné pro úspěch v těchto řízeních.

8.9 *Pojištěný* je povinen *pojistiteli* umožnit nahlížet do účetních knih a evidence *pojištěného* kdykoli v průběhu šetření škodné události.

## 9. ZMĚNA RIZIKA

9.1 *Pojistník* nebo *pojištěný*, pokud je odlišný od *pojistníka*, je povinen bez zbytečného odkladu oznámit *pojistiteli* změnu v odborných službách, poskytovaných *pojištěným* nebo jiných skutečnostech, které znamenají změnu nebo zánik *pojistného rizika*.

9.2 Pokud se v *pojistné době* *pojistné riziko* podstatně zvýší, vzniká *pojistiteli* právo navrhnout změnu *pojistné smlouvy* nebo *pojistnou smlouvu* vypovědět v souladu s příslušnými ustanoveními *zákonných norem*.

## 10. POJISTNÉ

10.1 Pojistné je jednorázovým pojistným, jehož výše je stanovena v *pojistné smlouvě*

10.2 *Pojistník* je povinen zaplatit jednorázové pojistné předem za celou *pojistnou dobu*. V *pojistné smlouvě* však může být dohodnuto, že *pojistník* uhradí pojistné ve splátkách.

10.3 *Pojistitel* může započíst dlužné pojistné na výplatu pojistného plnění.

10.4 Je-li *pojistník* v prodlení s placením pojistného, je povinen zaplatit *pojistiteli* úrok z prodlení v *zákonně* výši.

10.5 Pokud není v *pojistné smlouvě* ujednáno jinak, pojištění se v případě prodlení s placením pojistného nepřerušuje

## 11. VZNIK A ZÁNİK POJIŠTĚNÍ

11.1 Pojištění vzniká dnem uvedeným v *pojistné smlouvě* a sjednává se s *pojistnou dobou* v délce trvání 12 měsíců, pokud není v *pojistné smlouvě* uvedeno jinak

11.2 Pojištění zaniká:

- uplynutím *pojistné doby*;
- písemnou dohodou *pojistitele* a *pojistníka*;
- výpovědí kterékoliv ze stran v případech stanovených *zákonnými normami*;
- odstoupením v případech stanovených *zákonnými normami* a dále bez udání důvodu v následujících případech:

(i) *pojistník* může v průběhu *pojistné doby* od *pojistné smlouvy* kdykoli odstoupit. Odstoupení je účinné třicátým dnem od doručení oznámení o odstoupení *pojistiteli*. *Pojistitel* v tomto případě vrátí *pojistníkovi* poměrnou část pojistného odpovídající době, která zbývá po účinnosti odstoupení do konce původně sjednané *pojistné doby* po odečtení administrativních nákladů na správu a zrušení *pojistné smlouvy* ve výši uvedené v *pojistné smlouvě*.

(ii) *pojistitel* může v průběhu *pojistné doby* od *pojistné smlouvy* kdykoli odstoupit. Odstoupení je účinné třicátým dnem od doručení oznámení o odstoupení *pojistníkovi*. *Pojistitel* v tomto případě vrátí *pojistníkovi* poměrnou část pojistného odpovídající době, která zbývá po účinnosti odstoupení do konce původně sjednané *pojistné doby*.

- prodlením s placením pojistného dle příslušných *zákonných norem*; a
- v dalších případech stanovených v *zákonných normách*

## 12. DORUČOVÁNÍ

12.1 Oznámení nebo sdělení podle *pojistné smlouvy* se doručují na adresu uvedenou v *pojistné smlouvě*.

12.2 Jakékoliv oznámení nebo sdělení, které má být doručeno podle *pojistné smlouvy* *pojistníkovi* nebo *pojištěnému*, se bude považovat za doručené okamžikem, kdy adresát toto oznámení nebo sdělení sku-





tečně převzatí nebo okamžikem, kdy jeho přijetí odmítl nebo jinak znemožnil (např. neoznámením změny v adrese)

### 13. SUBROGACE, POSTOUPENÍ PRÁV

- 13.1 Jestliže má *pojištěný* proti jinému právo na náhradu škody způsobené *pojistnou událostí* nebo jiné obdobné právo, přechází jeho právo výplatou pojistného plnění na *pojistitele*, a to do výše částek, které *pojistitel* z pojištění poskytl. *Pojištěný* je povinen učinit veškerá opatření za účelem zajištění práv *pojistitele* vůči jiným stranám. *Pojistitel* je oprávněn na třetí osobu postoupit práva, která na něj v souladu s tímto ustanovením přešla nebo jakákoliv další práva z *pojistné smlouvy*. *Pojistitel* však neuplatní právo na náhradu škody podle tohoto článku vůči zaměstnancům *pojištěného*, pokud škodu nepůsobily úmyslně nebo jednáním, které je úmyslným trestným činem.
- 13.2 Práva vyplývající z *pojistné smlouvy* nesmí být postoupena na další osobu bez písemného souhlasu *pojistitele*.

### 14. ROZHODNÉ PRÁVO

*Pojistná smlouva* se řídí českým právem

### 15. ŘEŠENÍ SPORŮ

Pokud mezi *pojistitelem* a *pojištěným* nebo *pojistníkem* dojde ke sporu ohledně existence nároku na pojistné plnění nebo jeho rozsahu nebo jakékoliv otázky týkající se *pojistné smlouvy*, bude takový spor nejprve řešen prostřednictvím mediátora, na kterém se strany společně dohodnou.

Pokud se strany nedohodnou podle postupu uvedeného v předchozím odstavci nebo spor nebude vyřešen, bude spor předložen k rozhodnutí příslušnému soudu v České republice

### 16. NÁROKY PROTI POJISTITELI

*Pojistitel* není povinen poskytnout pojistné plnění, pokud nebudou splněny všechny podmínky *pojistné smlouvy* a *podmínek*. *Pojistitel* není povinen poskytnout pojistné plnění za škodu, dokud nebude na základě pravomocného a vykonatelného soudního rozhodnutí nebo dohody o soudním smíru nebo mimosoudním narovnání, se kterými *pojistitel* souhlasil, určena výše pojistného plnění.

### 17. ODDĚLITELNOST USTANOVENÍ

- 17.1 Pokud se kterékoli ustanovení těchto *podmínek* nebo *pojistné smlouvy* stane nebo bude shledáno neplatným nebo nevymahatelným, nebude tím dotčena platnost a vymahatelnost ostatních ustanovení těchto *podmínek*, ledaže by taková neplatnost podstatným způsobem ovlivnila význam ostatních ustanovení tak, že by strana za obdobných podmínek *pojistnou smlouvu* neuzavřela.
- 17.2 *Pojistník* a *pojistitel* se v případě neplatnosti nebo nevymahatelnosti zavazují jednat v dobré víře tak, aby toto ustanovení nahradil jiným s obdobným účinkem.

### 18. OSTATNÍ UJEDNÁNÍ

- 18.1 Pojištění se sjednává jako pojištění škodové.
- 18.2 Veškeré změny uzavřené *pojistné smlouvy* lze činit pouze písemně dodatky podepsanými oběma smluvními stranami. Není-li v *pojistné smlouvě* nebo v těchto *podmínkách* stanoveno jinak, musí být všechny úkony v souvislosti s *pojistnou smlouvou* činěny písemně na adresu smluvní strany uvedenou v *pojistné smlouvě*.
- 18.3 Nadpisy odstavců a článků jsou pouze orientační a jejich účelem není jakkoliv ovlivňovat význam či obsah ustanovení, která uvozují.
- 18.4 V *pojistné smlouvě* je možné se od těchto *podmínek* odchýlit a taková ujednání bude mít přednost před ustanoveními těchto *podmínek*. Pokud však odchylka směřuje k omezení některé z výluk učiněných v těchto *podmínkách*, bude mít taková odchylka přednost pouze v případě, že výslovně stanová, že se příslušná výluka nepoužije.

### 19. DEFINICE

Pokud z textu nevyplývá něco jiného, mají následující pojmy psané v textu *kurzívou* dále uvedené významy:

**Limit pojistného plnění** je částka uvedená v *pojistné smlouvě*, která je horní hranicí pojistného plnění;

**Náklady právního zastoupení** jsou přiměřené a nezbytné náklady, které *pojištěnému* vznikly v důsledku obrany proti nároku a s jejichž vynaložením písemně souhlasil *pojistitel*; tento souhlas však nesmí *pojistitel* bezdůvodně odmítnout; **náklady právního zastoupení** zahrnují platy nebo odměny *pojištěných*;

**Nárok** znamená:

- písemný nárok třetí osoby na náhradu škody proti *pojištěnému* v penězích, za kterou *pojištěný* právně odpovídá důsledku *vadného poskytnutí odborných služeb*;
- civilní nebo správní řízení vedené třetí osobou proti *pojištěnému* ve věci náhrady škody;
- trestní stíhání a trestní řízení vedené pro trestný čin, kterého se měl *pojištěný* dopustit.

**Odborné služby** jsou odborné služby včetně poradenství, které *pojištěný* poskytuje třetím osobám a které jsou uvedeny v *pojistné smlouvě*;

**Podmínky** jsou tyto pojistné podmínky pro pojištění profesní odpovědnosti;

**Pojistitel** je AIG CZECH REPUBLIC pojišťovna, a.s., zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B vložka 7340; IČ: 26477696; V Celnici 1031/4, 110 00 Praha 1, Česká republika;

**Pojistná doba** je doba určená v *pojistné smlouvě*, na kterou bylo pojištění sjednáno,

**Pojistná smlouva** je smlouva uzavřená mezi *pojistitelem* a *pojistníkem* podle těchto *podmínek*;

**Pojistná událost** je náhodilá událost, splňující znaky popsané v těchto *podmínkách*, se kterou je spojen vznik povinnosti *pojistitele* poskytnout pojistné plnění;

**Pojistné riziko** je míra pravděpodobnosti vzniku *pojistné události* vyvolané pojistným nebezpečím;

**Pojištěný** je osoba uvedená v *pojistné smlouvě*, na jejíž odpovědnost za škodu se toto pojištění vztahuje. Pro vyloučení pochybností se uvádí, že pojem *pojištěný* může zahrnovat i *pojistníka*, je-li v *pojistné smlouvě* uveden jako *pojištěný*;

**Pojistník** je osoba, která uzavřela *pojistnou smlouvu* s *pojistitelem* a která je povinna platit pojistné;

**Poškozený** je fyzická nebo právnická osoba, kromě *pojištěného* nebo *pojistníka*, která uplatňuje vůči *pojištěnému* nebo *pojistníkovi* nárok;

**Škoda** je majetková újma,

- za kterou *pojištěný* právně odpovídá a kterou je na základě soudního rozhodnutí nebo dohody o soudním smíru nebo mimosoudním vyrovnání povinen nahradit *poškozenému*; škoda na základě doložky o mimosoudním vyrovnání či soudním smíru je však považována za škodu jen pokud *pojistitel* předem vyslovil písemný souhlas s rozhodčí doložkou nebo smlouvou, respektive s mimosoudním narovnáním či soudním smírem;
- soudem přiznané náklady na právní zastoupení *poškozeného* v souvislosti s *nárokem*, který není z tohoto pojištění vyloučen;

**Škoda na zdraví** je smrt, zranění nebo nemoc nebo smrt, která nastala v důsledku takového zranění nebo nemoci; **škoda na zdraví** rovněž zahrnuje duševní újmu, psychické útrapy a šok;

**Škodliviny** jsou pevné, kapalné, plynné nebo tepelné dráždivé nebo znečišťující látky, včetně dýmu, páry, sazí, kouře, kyselých nebo zásaditých látek, toxických chemikálií a odpadních látek; odpadní látky jsou zejména látky, které mají být recyklovány, uvedeny do původního stavu nebo obnoveny;

**Škodná událost** je skutečnost, ze které vznikla škoda a která by mohla být důvodem vzniku práva na pojistné plnění;

**Vadné poskytnutí odborných služeb** je nedbalostní jednání *pojištěného* při poskytování *odborných služeb*, včetně chyby a omylu za předpokladu, že se takového jednání dopustil *pojištěný* neúmyslně v souvislosti s poskytováním *odborných služeb*;

**Věcná škoda** je škoda způsobená fyzickým poškozením, zničením nebo ztrátou hmotného majetku;

**Vlastní vrub** je částka uvedená v *pojistné smlouvě*, kterou se *pojištěný* podílí na vzniklé škodě a *nákladech právního zastoupení* a která se odečítá od pojistného plnění, jak je uvedeno v těchto *podmínkách*;

**Zákonné normy** je zákon č. 40/1964 Sb. občanský zákoník, zákon č. 37/2004 Sb., o pojistné smlouvě a další právní předpisy vztahující se k pojištění.

**Zaměstnanec** je

- osoba, která pracuje pro *pojištěného* na základě jakéhokoliv pracovního právního vztahu nebo jiné smlouvy, pokud je taková smlouva jejím hlavním zdrojem příjmu; a
- osoba, která u *pojištěného* vykonává odbornou praxi, stáž nebo obdobnou činnost



**Personalizační profil PKI appletu UKP a customizace middleware** ke smlouvě „Smlouva o poskytnutí služby „Řešení PKI pro čipovou kartu““ č. objednatele INO/40/05/001121/2006, č. zhotovitele 246/06

Personalizační profil definuje vlastnosti (počet, velikost, ochrana, ...) objektů PKI karty. Na 64kB kartě s tímto personalizačním profilem zůstane ještě asi 22kB volného místa pro další applety.

Obsah personalizačního profilu bude po podpisu smlouvy definován objednatelem. Zhotovitel poskytně objednateli potřebnou konzultační součinnost.

**Typ:** JavaCard 64k

**Mapování:** *CryptoPlus2*, v5

**Bezpečnostní politiky:**

Root certifikát: **ANO**

Personalizovaný root certifikát: **<bude upřesněno>**

Kontrola platnosti klientského certifikátu: **NE**

Modifikace device klíče a certifikátu: **Zakázána**

Vytváření objektů a mazání uživatelských objektů: **PIN**

Použití privátního klíče: **PIN**

Čtení veřejných informací: **FREE**

Zajištění integrity-modifikace: **3DES Usc (uložen v SW)**

Import privátního klíče: **ANO**

Expirace karty: **ANO, 4 roky**

**PIN:** konstantní „1111“, max. 3 neúspěšné pokusy

**PUK:** konstantní „44444444“, max. 5 neúspěšných pokusů

**Alokovaný prostor:**

RSA klíče 1024 bitů: **2**

RSA device klíč 1536 bitů: **1**

RSA klíče 2048 bitů: **2**

Certifikáty CA: **2 certifikáty 5KB**

Device certifikát: **1 certifikát / 1KB**

Klientské certifikáty: **4 certifikáty / 8KB**

Počet tajemství PKCS#11: **4**

Chráněné hodnoty tajemství PKCS#11: **3KB**

Dodatečné atributy PKCS#11: **1KB**

**AID:** A0 00 00 00 28 80 10 XX YY (XX YY – <bude upřesněno>)

**Logické číslo:** V souladu s normou ČSN ISO/IEC 7812

**Typ** – typ HW čipové karty, je navržena karta s 64KB EEPROM a operačním systémem JavaCard, HW generátor RSA

**Mapování** – definuje typ a verzi použitého mapování paměti souborového systému PKI appletu. Navrhovaná verze 5 nabízí nejvíce možností (rozšířená podpora ukládání PKCS#11 atributů objektů).

**Bezpečnostní politiky** – politiky, které budou aplikovány v rámci prvotní inicializace profilu *CryptoPlus*

- na kartě bude vyhrazen prostor pro kořenové certifikáty

- ukládání kořenových certifikátů v rámci personalizace bude upřesněno
- Nebude omezení na import klientských certifikátů dle certifikátů CA, které jsou na kartě uloženy
- Operace vytváření, mazání a modifikace dalších objektů budou chráněny PIN
- Operace s privátním klíčem budou chráněny PIN
- Veřejné informace (veřejné klíče, certifikáty, veřejné datové objekty) je možné číst bez nutnosti zadání PIN
- Zápis údajů na kartu bude dodatečně chráněn 3DES U<sub>sr</sub> klíčem (je zakódován do klientských knihoven CSP, PKCS#11)
- Na kartě bude povolen import privátních klíčů (např. z PKCS#12 souborů, při archivaci klíčů v rámci MS CA 2003, ..), export není možný
- Karta bude mít nastavenou expiraci na 4 roky, po konci platnosti karty na ni nebude možné nahrát nový certifikát, všechny ostatní funkce zůstanou zachovány
- PIN bude konstantní s hodnotou „1111“, maximální počet následujících neúspěšných pokusů bude nastaven na 3.
- PUK bude konstantní s hodnotou „44444444“, maximální počet následujících neúspěšných pokusů bude nastaven na 5.
- **Alokovaný prostor** – popisuje rozložení paměti:
  - na kartě bude alokovan prostor pro 4 páry (soukromý + veřejný) RSA klíčů (2x 1024 bitů, 1x 1536 bitů, 2x 2048 bitů),
  - na kartě bude prostor pro uložení dvou certifikátů CA; komprimovaná délka obou certifikátů nesmí překročit 5KB
  - na kartě bude prostor pro uložení 1 (device) certifikátu karty; komprimovaná délka obou certifikátů nepřekročí 1KB
  - na kartě bude prostor pro uložení 4 uživatelských certifikátů; komprimovaná délka všech certifikátů nesmí přesáhnout 8KB
  - na kartě bude prostor pro vytvoření čtyř obecných datových (ne PKI) objektů
  - chráněné hodnoty tajemství (hodnotu je možné přečíst až po zadání PIN) mohou mít max. délku 3KB
  - dodatečné atributy objektů PKCS#11 (např. ID klíčů a certifikátů, atd.), mohou mít max. délku 1KB

**AID** – je interní identifikátor aplikace. Jeho hodnota je přidělena Zhotovitelem tak, aby byly karty akceptovány v rámci dodávaných komponent middleware. Přesná podoba bude upřesněna.

**Logické číslo** – definuje číselnou řadu dodávaných karet. Formát bude v souladu s normou ČSN ISO/IEC 7812 a bude upřesněn.

### **Customizace CryptoPlus ProID middleware**

Prostřednictvím customizace je ovlivněna funkčnost a bezpečnostní vlastnosti použitého software, customizací se software jednoznačně identifikuje s grafickými prvky projektu.

Customizace CryptoPlus ProID middleware bude po podpisu smlouvy definována objednatelem. Zhotovitel poskytne objednateli potřebnou konzultační podporu.

Customizace se vztahuje na:

- kryptografické knihovny
- aplikaci „*Správce karty*“

## Customizace kryptografických knihoven

Kryptografické knihovny jsou programové moduly, které rozšiřují operační systém resp. aplikace o funkce podporované čipovou kartou.

### Bezpečnostní politiky

Kryptografické knihovny jsou implementovány v souladu s bezpečnostními politikami na kartě, nicméně je možné specifikovat dodatečné bezpečnostní politiky aplikované SW knihovnami:

- Délka PIN, který je SW knihovnami akceptován. Standardně je v rozsahu 4 až 8 číslic.
- Vynucení zadání PIN při každé operaci elektronického podpisu s hash algoritmy MD2, MD5, SHA-1 a RIPEMD160 (tj. mimo SSL autentizaci).
- Podpora šifrovaného ověření PIN (není možné v případě, že se používají některé PINPad čtečky)
- Povolení importu pouze těch klientských certifikátů, které vydaly důvěryhodné certifikační autority. Důvěryhodné CA z pohledu čipové karty jsou ty, které mají na kartě bezpečně uložen svůj certifikát (vázáno na bezp. politiku karty uložení certifikátů CA).
- Povolení kontroly časové platnosti karty. SW knihovna nedovolí import certifikátu, jenž začíná platit později, než skončila doba platnosti karty (vázáno na bezp. politiku uložení časové platnosti karty).
- Je možné realizovat plug-in zajišťující ověření nestandardních přístupových podmínek (např. s podporou administrativních 3DES klíčů uložených na administrativních kartách, HSM, ..)

### Název knihovny

Změna standardního názvu kryptografické knihovny dle šablony:

*<Název> CryptoPlus <typ knihovny> v<verze>, kde*

*<Název> představuje název nebo zkratku customizace *CryptoPlus*, popř. název nebo zkratku firmy (organizace), pro kterou je knihovna customizována*  
*<typ knihovny> představuje typ interface (např. CSP nebo Cryptoki)*  
*<verze> představuje číslo verze knihovny*

**Příklad:** Knihovny pro UKP, verze knihoven 1.0.

CSP pro systémy Microsoft Windows:

UKP *CryptoPlus* CSP v1.0

PKCS#11 pro Netscape

UKP *CryptoPlus* Cryptoki v1.0

### Jméno karty

Při pojmenování karty je vhodné dodržet formát

*<Název> CryptoPlus, kde*

<Název> představuje název nebo zkratku customizace *CryptoPlus*, popř. název nebo zkratku firmy (organizace), pro kterou je karta customizována

### **Uživatelské rozhraní**

Kryptografické knihovny komunikují s uživatelem vždy, když potřebují použít čipovou kartu. Před dotazem na PIN je zobrazeno dialogové okno.

Design okna se může kompletně změnit, podmínkou ovšem je, aby zde byl prostor pro zobrazení:

- jména aplikace, která žádá o čipovou kartu
- ikonky aplikace
- jména aktuálního okna aplikace
- typ žádané operace (2 řádky)

PKCS#11 disponuje funkcí pro zadání PIN, implementace *CryptoPlus ProID* však dovoluje tzv. automatické přihlášení k PKCS#11 – PIN dialog se automaticky zobrazí pokud požadovaná operace vyžaduje PIN. Automatické přihlášení k PKCS#11 je možné úplně zakázat.

### **Customizace Správce karty**

*Správce karty* umožňuje správu čipové karty, tj. zobrazení její struktury, mazání a import certifikátů, správu RSA klíčů, správu PIN, atp.

Její název se řídí formátem:

<Název> *CryptoPlus*, kde

<Název> představuje název nebo zkratku customizace *CryptoPlus*, popř. název nebo zkratku firmy (organizace), pro kterou je utilita customizována.

Správce karty se vyznačuje tím, že je v něm zabudován internetový prohlížeč. S využitím této technologie lze snadno uživateli prezentovat mnoho zajímavých informací, dát mu k dispozici odkazy na různé webové servery (server společnosti, server s technickou podporou, atp.). Je možné dodat materiály (ať už ve formě HTML nebo v podobě textů, které budou zpracovány grafikem objednatele), které budou aplikací zobrazeny po startu nebo na vyžádání.

## **Příloha č. 7**

**Plná moc** ke smlouvě „Smlouva o poskytnutí služby „Řešení PKI pro čipovou kartu““ č.  
objednatele INO/40/05/001121/2006, č. zhotovitele 246/06





Příloha č. 7

**PLNÁ MOC**

Obchodní společnost: **MONET+, a. s.**, se sídlem Zlín, Štípa, Za Dvorem 505, PSČ 763 14, IČ: 26217783, zapsaná v OR vedeném Krajským soudem v Brně, oddíl B, vložka 3351 (dále jen „Společnost“)

zmocňuje: **Mgr. Jiřího Beneše**, nar. 16.5.1965, bytem NIVY II./4251, PSČ: 760 01 Zlín, obchodního ředitele Společnosti (dále jen „Zmocněnec“),

aby za Společnost jako uchazeče činil v zadávacím řízení na veřejnou zakázku „Realizace Servisního Kartového Centra“, evidenční č. VZ 50023676, vyhlášenou Zadavatelem, veškeré úkony vůči Hl. m. Praha (dále jen „Zadavatel“) nebo třetím osobám v souvislosti s podáním nabídky Společnosti v předmětném zadávacím řízení, zejm. k podpisu nabídky Společnosti a jakýchkoli prohlášení Společnosti, které budou součástí nabídky Společnosti, jakož i k jednání, uzavírání a podpisu smluv se Zadavatelem nebo třetími osobami.

Ve Zlíně, dne: 23. října 2006.

  
**MONET+, a.s.**

Ing. Břetislav Endrys, předseda představenstva

  
**MONET+, a.s.**

Ing. Miroslav Janda, místopředseda představenstva

Přijímám zmocnění.

  
**Mgr. Jiří Beneš**

obchodní ředitel Monet+, a. s.

Číslo O 958/2006  
Ověřuji, že Ing. Břetislav Endrys,  
r.č. 6312129, DIČ: 655, bytem Zlín,  
číslo účtu I. 3541  
jehož totožnost byla prokázána platným  
úředním průkazem, tuto listinu přede  
mnou vlastní rukou podepsal.

Ve Zlíně dne 23. 10. 2006

Notář JUDr. Eva Duřková

Ing. Eva Zinráková  
pověřená notářem



Číslo O 958/2006  
Ověřuji, že Ing. Miroslav Janda,  
r.č. 512666021, bytem Zlín,  
Mladcová, Strahov 450  
jehož totožnost byla prokázána platným  
úředním průkazem, tuto listinu přede  
mnou vlastní rukou podepsal.

Ve Zlíně dne 23. 10. 2006

Notář JUDr. Eva Duřková

Ing. Eva Zinráková  
pověřená notářem



**MONEY<sup>+</sup>, a.s.** <sup>®</sup>

Za Dvorem 585, Věs 14 Zlín - Šumperk  
ICO: 28217783, DIČ: CZ28217783  
TEL: +420 57 311 111, fax: +420 57 311 112