



## Řízení letového provozu České republiky

### Kupní smlouva

**„Dodávka zaměstnaneckých ID karet pro zajištění provozní potřeby ŘLP a pro výměnu ID karet  
v roce 2019“**

uzavřená podle ust. § 2079 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších  
předpisů (dále jen „**občanský zákoník**“)

(dále jen „**smlouva**“)

#### 1. Smluvní strany

##### **Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)**

se sídlem: Navigační 787, 252 61 Jeneč

zastoupený: Ing. Miloslavou Mezerovou, výkonnou ředitelkou Útvaru finančně správního

IČO: 49710371

DIČ: CZ699004742

bankovní spojení: ČSOB Praha 5, č. účtu: 88153/0300

SWIFT kód: CEKOCZPP

zapsaný v obchodním rejstříku vedeném u Městského soudu v Praze, v oddíle A, vložce 10771

(dále jen „**kupující**“)

a

##### **První certifikační autorita, a.s.**

se sídlem: Podvinný Mlýn 2178/6, 190 00 Praha 9

zastoupená: Ing. Petrem Budišem, Ph.D., MBA, předsedou představenstva a

Ing. Romanem Kučerou, členem představenstva

IČO: 26439395

DIČ: CZ26439395

bankovní spojení: [REDACTED]

zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, v oddíle B, vložce 7136

(dále jen „**prodávající**“)

(kupující a prodávající rovněž „**smluvní strany**“)

## 2. Předmět smlouvy

- 2.1 Předmětem této smlouvy je závazek prodávajícího, že kupujícímu odevzdá věc, která je předmětem koupě specifikovaným v čl. 3 této smlouvy, a umožní kupujícímu nabýt vlastnické právo k předmětu koupě, a závazek kupujícího, že věc převezme a zaplatí prodávajícímu kupní cenu sjednanou v čl. 4 této smlouvy.

## 3. Předmět koupě

- 3.1 Prodávající se zavazuje dodat kupujícímu zaměstnanecké ID karty v počtu ■■■ ■■ dle vzoru vyvinutého na základě specifických požadavků kupujícího. Povinná technická specifikace je uvedena v Příloze č. 1 - „Technická specifikace zaměstnanecké ID karty“, která tvoří nedílnou součást této smlouvy (dále jen „**předmět koupě**“). Součástí dodávky zaměstnaneckých ID karet musí být i provedení aktivace a personalizace vestavěných kryptografických kontaktních čipů, a to tak, aby zaměstnanecké ID karty bylo možné provozovat ve spolupráci se systémy ŘLP ČR, s. p., vč. systému ICARA. Personalizace bude provedena tak, aby bylo možné zaměstnanecké ID karty využívat v systémech ŘLP minimálně po dobu 10 let od data jejich dodání kupujícímu.
- 3.2 Smluvní strany berou ve smyslu § 2095 občanského zákoníku na vědomí a výslovně souhlasí s tím, že prodávající odevzdává předmět koupě kupujícímu jako nový a bez jakýchkoliv vad či opotřebení.
- 3.3 Smluvní strany se dohodly, že vlastnické právo k předmětu koupě se převádí touto smlouvou převzetím předmětu koupě kupujícím.

## 4. Kupní cena

- 4.1 Kupní cena za předmět koupě (dále jen „**kupní cena**“) je stanovena dohodou smluvních stran dle zákona č. 526/1990 Sb., o cenách ve znění pozdějších předpisů a činí:

Řádek	Položka	Cena v Kč celkem
1.	Zaměstnanecká ID karta	1.504.000,00
2.	<b>Cena celkem</b>	<b>1.504.000,00</b>

(slovy: jedenmilionpětsetčtyřtisíc korun českých)

- 4.2 Kupní cena zahrnuje veškeré náklady prodávajícího související s dodávkou předmětu koupě do místa plnění.
- 4.3 Ke kupní ceně bude účtována příslušná sazba DPH v souladu se zákonem 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „**zákon o DPH**“).
- 4.4 Kupní cena uvedená v odst. 4.1 této smlouvy je sjednána smluvními stranami jako cena pevná. Změny ceny mohou být provedeny výhradně písemným dodatkem k této smlouvě, podepsaným oběma smluvními stranami.
- 4.5 Kupní cena je splatná ve lhůtě třiceti (30) kalendářních dnů ode dne, kdy byla kupujícímu doručena faktura - daňový doklad prodávajícího (dále jen „**faktura**“) obsahující (i) náležitosti daňového dokladu podle platného obecně závazného právního předpisu, a (ii) odkaz na číslo této smlouvy kupujícího. Faktura musí být zaslána na adresu kupujícího uvedenou v záhlaví této smlouvy.
- 4.6 Právo prodávajícího vystavit fakturu vzniká ke dni odevzdání předmětu koupě kupujícímu na základě předávacího protokolu o řádném předání a převzetí předmětu koupě.

- 4.7 Kupující má právo fakturu prodávajícímu před uplynutím lhůty splatnosti vrátit, aniž by došlo k prodlení s jeho úhradou, (i) obsahuje-li nesprávné údaje, (ii) chybí-li na faktuře odkaz na číslo této smlouvy kupujícího, (iii) není-li připojena kopie předávacího protokolu o řádném předání a převzetí předmětu koupě. Nová lhůta splatnosti v délce třiceti (30) kalendářních dnů počne plynout ode dne doručení opravené faktury kupujícímu.
- 4.8 Smluvní strany se dohodly a souhlasí, že úhradou faktury kupujícím se rozumí odeslání částky v příslušné faktuře požadované ve prospěch bankovního účtu prodávajícího.

## 5. Místo a čas plnění

- 5.1 Smluvní strany si sjednaly, že prodávající odevzdá kupujícímu a kupující od prodávajícího převezme předmět koupě nejpozději do T0 + 2 (dva) měsíce v sídle kupujícího uvedeném v záhlaví této smlouvy, kde T0 je den uveřejnění smlouvy v registru smluv a jedním měsícem se rozumí 30 po sobě jdoucích dní.
- 5.2 Přejímajícím za kupujícího bude zaměstnanec skladu v sídle kupujícího.
- 5.3 Prodávající se zavazuje písemně vyzvat kupujícího nejméně tři (3) pracovní dny předem k převzetí předmětu koupě prostřednictvím kontaktního emailu: [rlp\\_sklad@ans.cz](mailto:rlp_sklad@ans.cz).

## 6. Předání a převzetí předmětu koupě

- 6.1 Prodávající splní svůj závazek předáním a převzetím předmětu koupě kupujícím, což bude potvrzeno předávacím protokolem o řádném předání a převzetí předmětu koupě, který podepíší obě smluvní strany.
- 6.2 Prodávající je povinen předmět koupě zabalit nebo opatřit obalem pro přepravu, a to tak, aby nedošlo k jeho poškození.
- 6.3 Případné vady předmětu koupě zjištěné kupujícím při předání je prodávající povinen odstranit ihned po ohlášení kupujícím.
- 6.4 Předávací protokol o řádném předání a převzetí předmětu koupě bude obsahovat výčet případných vad předmětu koupě nebo prohlášení, že předmět koupě je bez vad, a bude podepsán oběma smluvními stranami.

## 7. Vlastnické právo a nebezpečí škody

- 7.1 Vlastnické právo k předmětu koupě dodanému podle této smlouvy přechází z prodávajícího na kupujícího bezprostředně po podpisu předávacího protokolu o řádném předání a převzetí předmětu koupě dle odst. 6.1 této smlouvy oběma smluvními stranami.
- 7.2 Prodávající prohlašuje a odpovídá kupujícímu za právní bezvadnost předmětu koupě a za skutečnost, že uzavřením smlouvy není porušeno žádné právo či povinnost prodávajícího nebo oprávněné zájmy jiných osob.
- 7.3 V případě, že jakákoliv jiná osoba uplatní nárok proti kupujícímu z titulu porušení práv duševního vlastnictví v souvislosti s touto smlouvou, zavazuje se prodávající poskytnout kupujícímu účinnou pomoc a uhradit mu veškeré náklady, které v souvislosti se sporem mezi kupujícím a jinou osobou kupujícímu vzniknou. Dále se prodávající zavazuje nahradit kupujícímu veškeré vzniklé škody, které mu vzniknou v důsledku uplatnění autorských nároků vůči kupujícímu v souvislosti s touto smlouvou a to v plné výši bez jakéhokoliv omezení.
- 7.4 Nebezpečí škody přechází na kupujícího spolu s vlastnickým právem.

## 8. Záruka a odpovědnost za vady

- 8.1 Prodávající poskytne na předmět koupě podle této smlouvy záruku v délce dvacet čtyři (24) měsíců od protokolárního předání předmětu koupě kupujícímu. Prodávající odpovídá za to, že předmět koupě bude po záruční dobu způsobilý ke smlouvenému účelu, jinak k účelu obvyklému a zachová si po tuto dobu smlouvené vlastnosti. Tyto vlastnosti jsou uvedeny v příloze č. 1 této smlouvy.
- 8.2 Kupující má právo oznámit prodávajícímu zjištěné vady předmětu koupě. Oznámení vady předmětu koupě je možné učinit e-mailem nebo telefonem. Telefonní oznámení musí být následně potvrzeno písemně e-mailem.
- 8.3 Smluvní strany si sjednaly a souhlasí, že kupující má v případě výskytu vady předmětu koupě v záruční době právo dle své volby požadovat odstranění vady dodáním nové věci bez vady nebo dodáním chybějící věci, na odstranění vady opravou věci, na přiměřenou slevu z kupní ceny a právo od této smlouvy odstoupit.
- 8.4 Kupující sdělí prodávajícímu, jaké právo zvolil při oznámení vady nebo bez zbytečného odkladu po oznámení vady. Provedenou volbu nemůže kupující změnit bez souhlasu prodávajícího; to neplatí, žádal-li kupující opravu vady, která se ukáže jako neopravitelná. Neodstraní-li prodávající vady dle požadavku kupujícího v přiměřené lhůtě či oznámí-li kupujícímu, že vady neodstraní, může kupující požadovat místo odstranění vady přiměřenou slevu z kupní ceny, nebo může od této smlouvy odstoupit.
- 8.5 Záruční doba podle této smlouvy bude přerušena a příslušně prodloužena o dobu potřebnou k odstranění vady či o dobu, kterou si vyžádá poskytnutí bezvadného plnění. Rozhodujícím datem je datum oznámení vady prodávajícímu a datum předání bezvadného předmětu koupě.
- 8.6 Vady zjištěné kupujícím během záruční doby prodávající odstraní bezplatně.
- 8.7 V případě, že prodávající nebude plnit řádně a včas záruční podmínky sjednané v této smlouvě, je kupující oprávněn sám odstranit vadu předmětu koupě nebo sjednat její odstranění třetí osobou. Náklady spojené s odstraněním vady nese prodávající.
- 8.8 Pokud není v této smlouvě uvedeno jinak, řídí se odpovědnost za vady ustanoveními občanského zákoníku.
- 8.9 Odpovědnost za právní vady předmětu koupě nese prodávající a tato odpovědnost není omezena záruční dobou sjednanou v této smlouvě.

## 9. Smluvní pokuty

- 9.1 Smluvní strany sjednávají pro případ porušení smluvních povinností smluvní pokutu.
- 9.2 V případě, že prodávající nedodrží termín plnění sjednaný v článku 5 této smlouvy, je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 0,05 % z celkové ceny uvedené v článku 4 této smlouvy za každý započatý den prodlení.
- 9.3 Odchylně od § 2050 občanského zákoníku se smluvní strany dohodly, že sjednání jakékoli smluvní pokuty se nedotýká práva na náhradu škody vzniklé z porušení povinností, ke kterému se smluvní pokuta vztahuje, a nárok na náhradu škody může být uplatněn nezávisle na smluvní pokutě a v plné výši.
- 9.4 Smluvní pokuta uplatněná dle této smlouvy je splatná do třiceti (30) kalendářních dnů ode dne doručení písemného oznámení o jejím uplatnění stranou oprávněnou straně povinné. Ujednání o smluvních pokutách zůstávají případným odstoupením od této smlouvy nedotčena a trvají i po skončení účinnosti této smlouvy.
- 9.5 Uplatněním smluvní pokuty podle této smlouvy není dotčeno právo kupujícího na náhradu škody.



## 10. Ostatní ujednání

10.1 Prodávající je povinen předmět koupě zabalit tak, aby při běžných podmínkách přepravy, manipulace a skladování byl řádně chráněn před poškozením. Prodávající je odpovědný za škodu způsobenou vadným balením.

10.2 Prodávající prohlašuje, že předmět koupě bude dodán v souladu s předpisy, které se na předmět koupě vztahují.

10.3 Prodávající je povinen při realizaci této smlouvy respektovat podmínky kupujícího ohledně režimu vstupu a vjezdu vozidel do objektů a na pozemky kupujícího.

10.4 Prodávající prohlašuje, že realizací této smlouvy nejsou dotčena žádná práva jiných osob a prodávající má právo dodat kupujícímu předmět koupě a převést na kupujícího veškerá práva s tím spojená s ohledem na autorská práva. Veškerá odpovědnost z tohoto vyplývající jde k tíži prodávajícího, který odpovídá za škodu způsobenou porušením tohoto ustanovení.

### 10.5 Uveřejňování

Prodávající bere na vědomí, že kupující je povinen uveřejnit tuto smlouvu ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Prodávající bere dále na vědomí, že kupující je povinen poskytnout informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. Při uveřejnění této smlouvy v registru smluv budou v jejím textu znečitelněny zejména tyto údaje: bankovní spojení smluvních stran, podpisy na smlouvě, a dále obchodní tajemství ve smyslu § 504 občanského zákoníku specifikované v odst. 10.6 této smlouvy.

### 10.6 Obchodní tajemství

Podle § 504 občanského zákoníku je obchodním tajemstvím informace o počtu kusů obsažená v odst. 3.1 a 4.1 této smlouvy a jednotková cena uvedená v odst. 4.1 této smlouvy, a proto nebudou výše uvedené informace uveřejněny, ani poskytnuty dle odst. 10.5 této smlouvy.

### 10.7 Bezpečnost v civilním letectví

Prodávající podpisem smlouvy bere na vědomí, že není oprávněn sdělovat či jakkoliv šířit informace, kterými by mohla být narušena bezpečnost v civilním letectví, a to z důvodu požadavků na zachování bezpečnosti v civilním letectví, které vyplývají z příslušných právních předpisů (zejména Letecký předpis L 17), a které ukládají poskytovatelům letových provozních služeb přijmout taková adekvátní opatření, na základě kterých bude zajištěna ochrana civilního letectví před protiprávními činy. Prodávající nesmí zejména jakkoliv reprodukovat a dále šířit informace, o nichž se dozvěděl v souvislosti s plněním této smlouvy.

### 10.8 Ochrana osobních údajů

Kupující i prodávající respektují pravidla o ochraně osobních údajů dle nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), tj. nařízení GDPR, a dalších obecně závazných právních předpisů upravujících ochranu osobních údajů. Bližší informace o ochraně osobních údajů kupujícího jsou k dispozici na webových stránkách

<http://www.rlp.cz/spolecnost/osobniudaje/Stranky/default.aspx>

## 11. Vyšší moc (vis maior)

- 11.1 Smluvní strany se osvobozují od odpovědnosti za částečné nebo úplné nesplnění smluvních závazků, jestliže se tak prokazatelně stalo v důsledku vyšší moci. Za vyšší moc se pokládají okolnosti, které vznikly po uzavření této smlouvy v důsledku smluvními stranami nepředvídaných a neodvratitelných událostí, mimořádné povahy a mají bezprostřední vliv na plnění předmětu této smlouvy. Nastanou-li výše uvedené okolnosti, jsou obě smluvní strany povinny se neprodleně o těchto okolnostech vzájemně informovat.
- 11.2 Lhůty pro plnění povinností podle této smlouvy se prodlužují o dobu, po kterou prokazatelně trvá okolnost vylučující odpovědnost.
- 11.3 Jestliže důsledky vyplývající ze zásahu vyšší moci prokazatelně trvají déle než tři (3) po sobě jdoucí kalendářní měsíce, může kterákoliv ze smluvních stran od této smlouvy odstoupit s tím, že se nároky smluvních stran vyrovnají tak, aby žádné ze smluvních stran nevzniklo bezdůvodné obohacení.

## 12. Odstoupení od smlouvy

- 12.1 Kupující je oprávněn odstoupit od této smlouvy v případě, že prodávající nebude realizovat předmět koupě v souladu s touto smlouvou a/nebo bude zanedbávat plnění svých závazků tak závažným způsobem, že tato skutečnost výrazně ovlivní kvalitu předmětu koupě nebo termín předání předmětu koupě. Kupující za podstatné porušení této smlouvy s možností okamžitého odstoupení považuje:
- 12.1.1. prodlení s termínem předání předmětu koupě delší než 15 dní,
  - 12.1.2. prodávající bude v úpadku ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.
- 12.2 Prodávající je oprávněn odstoupit od této smlouvy v případě, že kupující bude v prodlení se zaplacením faktury delším než 30 dní.
- 12.3 V případě odstoupení kterékoliv smluvní strany od této smlouvy, končí platnost a účinnost této smlouvy dnem doručení písemného oznámení o odstoupení od této smlouvy druhé smluvní straně.

## 13. Náhrada majetkové a nemajetkové újmy

- 13.1 Pro náhradu majetkové újmy (škody) a nemajetkové újmy platí příslušná ustanovení občanského zákoníku. Majetková újma se nahrazuje v penězích, nedohodnou-li se smluvní strany jinak. Smluvní strany prohlašují, že dojde-li porušením povinností prodávajícího ke vzniku újmy na pověsti nebo obchodní firmě kupujícího či k jiné nemajetkové újmě, uhradí prodávající kupujícímu přiměřené zadostiučinění.

## 14. Závěrečná ustanovení

- 14.1 Tuto smlouvu lze měnit nebo doplňovat pouze výslovným oboustranně potvrzeným smluvním ujednáním, a to ve formě dodatku k této smlouvě, podepsaným oprávněnými zástupci obou smluvních stran.
- 14.2 Tato smlouva vstupuje v platnost dnem podpisu obou smluvních stran a účinnosti nabývá dnem uveřejnění v registru smluv.
- 14.3 Obě smluvní strany prohlašují, že jednotlivé články této smlouvy jsou dostatečné z hlediska náležitosti pro vznik smluvního vztahu, a že bylo využito smluvní volnosti stran a tato smlouva se uzavírá určitě, vážně a srozumitelně. Smluvní strany se dohodly, že jejich závazkový vztah se řídí ustanoveními občanského zákoníku.

14.4 Veškerá práva a povinnosti vyplývající z této smlouvy přecházejí, pokud to povaha těchto práv a povinností nevyklučuje, na právní nástupce smluvních stran.

14.5 Smlouva je vyhotovena v českém jazyce ve čtyřech stejnopisech, z nichž každá smluvní strana obdrží dva výtisky.

14.6 Nedílnou součástí této smlouvy je následující příloha.

Příloha č. 1 - „Technická specifikace zaměstnanecké ID karty“.

V Jenči dne .....17-09-2018

Ři

V Praze dne 6. 9.



## **Technická specifikace zaměstnanecké ID karty**

### **1) Základní specifikace**

ID karta standardní velikosti, obsahující kontaktní čip Starcos3.5, bezkontaktní rádiový čip HITAG1 a druhý bezkontaktní rádiový čip MIFARE DESFire EV1 8K.

Rozměry karty jsou dle ISO/IEC 7810, tedy  $5.40 \times 8.57 \times 0.076 \pm 0.0076$  cm. Všechny čipy jsou umístěny v těle karty tak, že je možné realizovat potisk lícové strany karty.

### **2) Specifikace kontaktního čipu a SW pro jeho administraci**

Kontaktní čip je realizován v typovém provedení Starcos3.5 a je umístěn do středu rubové strany karty dle standardu pro kontaktní kryptografické čipy. Čipová karta Starcos3.5 je vývojově novou řadou čipových karet a zahrnuje řadu nových funkcí a možností pro uživatele.

#### Personalizace

Personalizaci kontaktního čipu a vývoj SW pro jeho administraci zajišťuje První certifikační autorita, a.s. (dále jen „I.CA“). Součástí personalizace je také nahrání mezilehlých a kořenových certifikátů I.CA.

#### Technologická specifikace čipu Starcos3.5

- Paměťová kapacita čipu je využívána dynamicky, což umožňuje na čip uložit variabilní počet klíčů, certifikátů a ostatních dat. Toto pravidlo se nevztahuje na kvalifikované certifikáty. Kvalifikované certifikáty lze na čip umístit pouze dva, z toho jeden platný pro realizaci kvalifikovaného elektronického podpisu. Toto je zásadní změna v porovnání se stávajícími čipy Starcos3.5.
- Čip je využíván i pro bezpečné uložení kořenového certifikátu Certifikační autority. Díky uloženému certifikátu Certifikační autority je možné ho používat i v neznámém prostředí. Je možné zvolit podporované (důvěryhodné) Certifikační autority, jejichž klientské certifikáty může klient využívat. Jiné klientské certifikáty pak není možné na čip umístit, čímž se významně omezuje možnost jeho použití k nepovoleným operacím.
- Čipová karta má životnost několik let, během života karty si může majitel na čip nechat vydat několik certifikátů.
- Bezpečnostně citlivé operace je možné vždy realizovat pouze po zadání PIN, jehož délka je 6 – 8 míst. Čip je dále možné v případě zapomenutí PIN odblokovat pomocí PUK. Čip není po personalizaci vybaven PIN a PUK a klient je při prvním použití karty požádán o zvolení PIN a PUK.
- Čip je kvalifikovaným prostředkem pro vytváření elektronických podpisů a pečetí podle nařízení eIDAS, konkrétně je certifikován jako Qualified Signature Creation Device (QSigCD).



#### Základní technické parametry

- Velikost paměti: 80 kB
- Velikost privátního klíče generovaného na čipu: 1024 a 2048
- Kryptografické funkce: AES až 256bit, RSA až 4096 bits, elliptic curves až 521bit
- Podpora Hashes: SHA1, SHA-2 až SHA-512
- Podporované standardy: ISO 7815-4/-8/-9, ISO 14443-1/-2/-3/-4
- Podporované protokoly: ISO 7816-3 T=0 a T=1
- Podporované rozhraní: MS CSP, PKCS 11
- Standard PKCS 12
- Privátní klíč se generuje přímo v čipu a nikdy ho neopustí
- Počet úložišť pro privátní klíče a certifikáty je variabilní. Možnost vytvoření nového úložiště a uložení dat na kontaktní čip je omezena pouze volnou kapacitou čipu. Standardně se na čip vejde 8 certifikátů s privátními klíči.

#### Kompatibilita se standardy

- ISO/IEC, DIN, EMV

#### Další funkčnosti čipu

- Prostor pro citlivá data chráněný PINem
- Nativní práce s volným prostorem
- Tvorba žádosti o obnovu certifikátu v rámci aplikace
- PIN management (individuální PIN pro zabezpečená datová úložiště)
- Blokace čipu při zadání chybného PIN
- Podpora pro Secure PIN entry
- Nativní podpora pro TWINS.

#### Podpora pro

- OS: Windows 2003, Windows Vista, Windows 7, 8 či 10
- MS CAPI (existence Cryptographic Services Provider pro Microsoft) PC/SC rozhraní
- CryptoOKI (modul PKCS11 pro aplikace typu Firefox).

#### Výhody čipové karty Starcos3.5

Čipová karta s kontaktním čipem Starcos3.5 je dodávána s obslužnou aplikací SecureStore I.CA, která je vždy upravena s ohledem na specifické požadavky uživatele tak, aby byla zajištěna jeho komfortní práce s čipovou kartou. Jedná se o SW pro správu certifikátů, klíčů, přihlašovacích údajů a ostatních údajů na pracovní stanici.

#### SW SecureStore I.CA

SW SecureStore I.CA umožňuje použití karty v aplikacích a poskytuje nástroj pro management karty. SW je tvořen několika moduly:

- SecureStore CSP (Crypto Service Provider) – komponenta umožňující použití karty v prostředí MS Explorer, MS Outlook a dalších aplikacích na platformě Windows, které využívají standardní rozhraní CryptoAPI.
- SecureStore PKCS11 – komponenta umožňující použití karty v aplikacích typu Mozilla Firefox na platformě Windows, které využívají rozhraní CryptoOKI.
- I.CA NewCert je aplikace pro tvorbu žádosti o všechny typy certifikátů.
- Aplikace SecureStore – Windows aplikace umožňující správu kontaktního čipu.

Aplikace SecureStore je samostatně běžícím programem na platformě MS Windows s následujícími základními funkcemi:

- generování páru klíčů o velikosti 1024 nebo 2048 bit současně s vytvořením příslušné žádosti o certifikát vybraného typu (komerční, kvalifikovaný). Pro pár klíčů je vždy možné zvolit, zda se jedná o pár určený pro šifrování (pár se při tvorbě zálohuje) nebo pár určený pro elektronický podpis (pár se nezálohuje).
- import vydaného certifikátu na kontaktní čip - vydaný certifikát ve formátu DER uloží do příslušného úložiště k páru klíčů
- práce s certifikáty uloženými na čipu a správa úložišť - včetně mazání a importu certifikátu
- označení úložiště používaného pro Windows SmartCard Logon
- PIN management - změna PIN - pomocí starého PINu lze nastavit nový, odblokování PIN - pomocí zadání PUK lze nastavit nový PIN
- registrace certifikátu do Windows - provede instalaci certifikátu do úložišť Windows tak, aby byl dostupný pomocí služeb pracujících s certifikáty v prostředí Windows
- sledování využití prostoru čipu
- využití volného prostoru čipu pro ukládání libovolných souborů. Úložiště pro volný prostor je možné zvolit ve dvou variantách:
  - nezabezpečené, které je volně přístupné
  - zabezpečené, které je přístupné pouze po zadání PINu k tomuto úložišti. Toto úložiště je vhodné např. pro správu hesel.

• SW SecureStore zajišťuje dodržení zpětné kompatibility, tj. umožňuje paralelně pracovat s kontaktním čipem Starcos3.0 i s kontaktním čipem Starcos3.5.

### 3) Specifikace bezkontaktních čipů

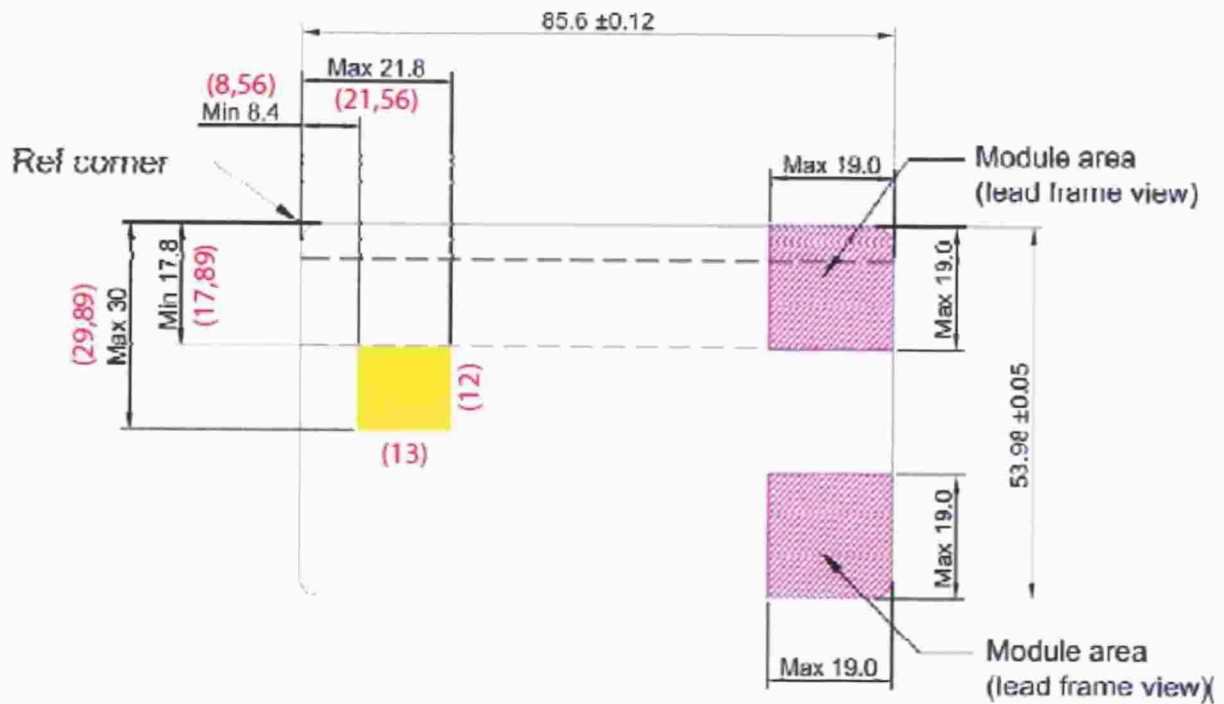
Bezkontaktní čipy jsou realizovány v provedení HITAG1 / MIFARE DESFire EV1 8K a jsou umístěny do těla karty - pozičně do volného prostoru tak, aby byla zajištěna maximální možná míra eliminace případného negativního ovlivňování práce bezkontaktních čipů stíněním kovových částí ostatních komponent ID karty a aby tím bylo zajištěno jejich bezproblémové využití.

Základní technické parametry bezkontaktních čipů:

- Operační frekvence: MIFARE DESFire EV1 13.56 MHz, - HITAG1 125 kHz
- Maximální čtecí vzdálenost: MIFARE DESFire EV1 2.54 cm - HITAG1 5.59 cm
- Pracovní teplota: -31°C až +50 °C
- Velikost paměti: HITAG 1: 2048 bitů, MIFARE DESFire EV1: až 28 aplikací a až 32 souborů/ 1 aplikace
- MIFARE DESFire EV1 je plně v souladu s ISO 14443A 1-4, a splňuje úroveň bezpečnosti karty (Common Criteria) EAL 4+

### 4) Mechanické uspořádání komponent na kartě:

Rozměry karty jsou dle ISO/IEC 7810, tedy 5.40 x 8.57 x 0.076 ± 0.0076 cm. Umístění jednotlivých čipů na kartě je uvedeno na následujícím schématu:



Mechanicky je karta provedena tak, že bezkontaktní čipy jsou zalisovány dovnitř těla karty, kontaktní čip má vyvedeny kontakty na rubové straně a lícová strana karty je celá bílá.