SMLOUVA
o úpravě stávajícího systému čipových karet a souvisejících podpůrných systémů včetně poskytování podpory a údržby

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník"), a zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, mezi:

Českou národní bankou

Na Příkopě 28
115 03 Praha 1
zastoupenou: Ing. Milanem Zirnsákem, ředitelem sekce informatiky
a
Ing. Zdeňkem Viriusem, ředitelem sekce správní
IČO: 48136450
DIČ: CZ48136450

(dále jen „objednatel" nebo také „ČNB")

a

T-SOFT a.s.

zapsanou v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 15233,
se sídlem:
Za Brumlovkou 1559/5
140 00 Praha 4 - Michle
Česká republika
zastoupenou: Ing. Marošem Jančovičem, předsedou představenstva
a
Ing. Michalem Vaněčkem, Ph.D., MBA, místopředsedou představenstva
IČO: 40766314
DIČ: CZ40766314
č. účtu: 1010251000 / 2700

(dále jen „zhotovitel")

Preambule

Objednatel provozuje ve svém standardním systémovém prostředí systém čipových karet, které slouží mimo jiné k autentizaci uživatelů při jejich přihlašování do operačních systémů, uchovávání různých typů certifikátů či informací, jako jsou například uživatelská hesla apod. Vzhledem k tomu, že došlo k vyčerpání možnosti čerpat podporu na stávající systém a některé jeho komponenty již nemají podporu jejich výrobce, nebo mohou být provozovány na nepodporovaném operačním systému (dále také jako „OS"), je nutné jej upravit, upgradovat, obměnit či doplnit pro provoz na podporovaných verzích OS a uzavřít novou smlouvu o jeho

[redacted]

podpoře a v neposlední řadě i o dodávkách HW a SW pro zajištění jeho budoucího rozvoje či jeho kapacitního rozšíření.

Článek I

Předmět smlouvy

1. Předmětem této smlouvy je povinnost zhotovitele provést dílo, konkrétně:

   a) Upravit, upgradovat, obměnit nebo doplnit v současné době objednatelem užívané komponenty (HW a SW) systému čipových karet a související komponenty systémového prostředí objednatele (dále též „SCK“) tak, aby po provedení uvedených modifikacích SCK objednatele byl tento:

      - způsobilý pro provozování bez konfliktů na výrobcem podporovaných OS, současně ČNB užívaných (viz příloha č. 2), a dalších výrobcem podporovaných programových prostředcích (SW), využívaných nebo využívajících SCK;
      - způsobilý zajistit potřeby autentizace a další funkce pro 1750 uživatelů;
      - pokryt v uvedeném rozsahu 1750 uživatelů SCK servisní podporou (jak pro HW, tak pro klientský SW i SW pro správu);
      - provozován výhradně s čipovými kartami splňujícími certifikaci Common Criteria na úroveň EAL4+ nebo vyšší; **výčet karet, které již nesplňují požadavky a musejí být v rámci Řešení vyměněny, je obsažen v příloze č. 3 této smlouvy.**

   (dále též „Řešení“).

   Podrobné požadavky na Řešení stanoví příloha č. 4 této smlouvy „Technické podmínky předmětu plnění“. Technické a programové prostředky, které zhotovitel dodá v rámci implementace Řešení, jsou uvedeny v příloze č. 1 této smlouvy.

   b) V případě potřeby upravit, upgradovat, obměnit nebo doplnit další komponenty systémového prostředí objednatele související s SCK nad rámec písm. a) v podobě nezbytných souvisejících technických a programových prostředků tak, aby bylo zajištěno naplnění požadavků na Řešení podle písm. a) a byl zachován současný rozsah funkcí SCK, i pokud by podrobnější vymezení takové úpravy nebo doplnění nebylo obsaženo v příloze č. 4 této smlouvy „Technické podmínky předmětu plnění“, ale bylo by vynuceno vlastnostmi zhotovitelem zvoleného řešení; plnění podle tohoto písmene je považováno za součást Řešení.

2. Součástí díla podle odst. 1 je dále:

   a) vypracování realizační studie za využití šablony dle přílohy č. 8 této smlouvy;

   b) provedení školení zaměstnanců objednatele v souladu s přílohou č. 9 této smlouvy;

   c) vytvoření dedikovaného testovacího prostředí na bázi Řešení, shodné nebo obdobné konfigurace jako SCK provozované objednatelem (viz příloha č. 3), pro nejvýše 10 současně napojených jmenovitých uživatelů objednatele na serveru/serverech zajištěném objednatelem pro testovací provoz;

   d) dodání uživatelské dokumentace výrobce/výrobců technických prostředků (HW) a dokumentace výrobce/výrobců programových prostředků (SW), které budou zhotovitelem dodány v rámci Řešení;

e) vypracování dokumentace k SCK po realizaci Řešení (dále jen „realizační dokumentace“) v elektronické podobě ve formátu MS Word 2010 nebo vyšším.

3. Zhotovitel se dále zavazuje dodávat objednateli na základě jeho objednávek další technické a programové prostředky dle čl. VII této smlouvy.
4. Zhotovitel se rovněž zavazuje poskytovat objednateli provozní podporu a budoucí rozvoj SCK podle čl. VI této smlouvy.
5. Dodané technické prostředky (HW) podle této smlouvy budou nové a nepoužité (maximálně ty, u nichž to připadá v úvahu, z továrny zahořelé z výroby nebo zapnuté pro ověření funkčnosti v rámci kompletace prostředků zhotovitelem před dodáním).
6. Řešení musí splňovat funkční a technické požadavky uvedené v příloze č. 4 „Technické podmínky předmětu plnění“ této smlouvy. Provedení úprav, upgrade, obměn a doplnění podle odst. 1 (dále též „implementace“) musí být realizováno v souladu s návrhem technického řešení dle přílohy č. 6 této smlouvy a schválenou realizační studií podle odst. 2 písm. a).
7. Zhotovitel bere na vědomí, že k technickým ani programovým prostředkům (HW ani SW) SCK nebude zhotoviteli poskytován vzdálený přístup.
8. Zhotovitel bere rovněž na vědomí, **že nesmí nad míru obvyklou**, odpovídající stavu technologie a poznání v čase a místě provádění díla, **zatěžovat ani technické (HW) ani programové (SW) prostředky** (popsané v přílohách č. 2 a 3) **a ani lidské zdroje objednatele**; to nevylučuje možnost zhotovitele dodat, pro potřeby jeho řešení, objednateli další technické nebo programové prostředky (HW nebo SW) za předpokladu jejich uvedení v příloze č. 1.
9. Zhotovitel bere dále na vědomí, že veškeré v přílohách (zejména č. 2, 3 a 4) uvedené verze programových prostředků (SW) užívaných objednatelem jsou orientační a mohou být během provádění díla aktualizovány na vyšší verze, resp. nahrazeny za přímé nástupce daných programových prostředků.
10. Bude-li v rámci plnění objednateli jakýmkoliv způsobem poskytnut jakýkoliv technický prostředek (HW) v podobě paměťového média (viz též příloha č. 1), bere zhotovitel na vědomí, že **od prvního okamžiku použití tohoto technického prostředku (HW) k uložení dat objednatele nebude již možné tento technický prostředek od objednatele získat zpět**, a to ani v rámci oprav nebo poskytování podpory.
11. Objednatel se zavazuje za poskytnutá plnění uhradit ceny dle čl. IV této smlouvy.

Článek II

Průběh plnění

1. Plnění této smlouvy bude realizováno zhotovitelem v následujících etapách:

   1. etapa: Vytvoření realizační studie

   První etapa zahrnuje vypracování realizační studie za využití šablony dle přílohy č. 8 této smlouvy a její akceptaci postupem dle přílohy č. 11 této smlouvy. Realizační studie detailně zmapuje skutečný stav stávajícího SCK, prověří realizovatelnost Řešení a jeho implementaci v prostředí objednatele a obsáhne veškeré informace nezbytné pro implementaci Řešení v souladu s touto smlouvou.

2. etapa: Implementace Řešení v prostředí objednatele

Druhá etapa zahrnuje:

a) převzetí podpory stávajících technických a programových prostředků SCK (které již ČNB v rámci SCK vlastní / oprávněně užívá) dle čl. VI této smlouvy;

b) dodávku technických a programových prostředků uvedených v příloze č. 1 včetně dokumentace podle čl. I odst. 2 písm. d);

c) úpravu, upgrade, obměnu a doplnění SCK a dalších komponent systémového prostředí objednatele souvisejících s SCK dle čl. I odst. 1, **zejména** instalaci technických a programových prostředků uvedených v příloze č. 1, zprovoznění režimu vysoké dostupnosti (příloha č. 4, požadavek „Režim vysoké dostupnosti"), zprovoznění a zajištění funkce získání certifikátů pro přihlášení na stávajících **i nově dodávaných (vč. obměňovaných)** hybridních i kontaktních čipových kartách (dále společně „čipové katy") a funkce vydávání kvalifikovaných certifikátů pro realizaci kvalifikovaných podpisů na nově dodávaných čipových kartách a tokenech (příloha č. 4, požadavky „Základní funkce" a „Kapacita a prostor pro data") a migraci dat (příloha č. 4, požadavek „Migrace dat");

d) školení správy SCK po implementaci Řešení v souladu s přílohou č. 9 této smlouvy;

e) vytvoření testovacího prostředí a testovací provoz SCK s implementovaným Řešením vč. akceptace dle přílohy č. 11 této smlouvy;

f) ověřovací provoz SCK s implementovaným Řešením v provozním prostředí objednatele vč. akceptace dle přílohy č. 11 této smlouvy.

Pro vytvoření testovacího a provozního prostředí SCK poskytne objednatel fyzické a virtuální servery označené jako zařízení dedikovaná pro testovací a provozní prostředí SCK v příloze č. 2.

Maximální přípustné doby provozních odstávek při implementaci Řešení jsou uvedeny v příloze č. 4, v požadavku „Provozní odstávky".

3. etapa: Školení provozu SCK s implementovaným Řešením a realizační dokumentace

Třetí etapa zahrnuje:

a) vypracování realizační dokumentace podle čl. I odst. 2 písm. e) o obsahu dle přílohy č. 10 této smlouvy a její akceptaci postupem dle přílohy č. 11 této smlouvy;

b) školení provozu SCK v souladu s přílohou č. 9 této smlouvy.

Článek III

Místo plnění, lhůty, předání a převzetí díla

1. Místem plnění budou prostory výpočetního střediska v objektu objednatele na adrese: Na Příkopě 28, 115 03 Praha 1 (lokalita „Senovážná") a Strojírenská 175, Praha 5 (lokalita „Zličín").
2. Plnění bude prováděno v pracovní dny v době od 8.00 hod. do 17.00 hod., nedohodnou-li se smluvní strany v konkrétním případě jinak nebo nestanoví-li jinak tato smlouva.
3. Smluvní strany vzájemně dohodly následující lhůty:

   a) zhotovitel předá objednateli realizační studii k akceptaci **do 10 týdnů** od uzavření smlouvy;

b) zhotovitel umožní objednateli zahájení testovacího provozu SCK s implementovaným Řešením nejpozději **do 18 týdnů** od uzavření smlouvy a zahájení ověřovacího provozu SCK s implementovaným Řešením nejpozději **do 28 týdnů** od uzavření smlouvy;

c) zhotovitel předá objednateli realizační dokumentaci k akceptaci **do 32 týdnů** od uzavření smlouvy.

4. Zhotovitel předá objednateli dílo nejpozději **do 35 týdnů** ode dne uzavření této smlouvy.

5. Lhůty podle odst. 3 a 4 je oprávněna (nikoliv povinna) kterákoliv z pověřených osob objednatele podle čl. V odst. 2 písm. a) na písemnou a odůvodněnou žádost zhotovitele přiměřeně okolnostem prodloužit, a to po zvážení všech objektivních okolností zhotovitelem v jeho žádosti uvedených anebo objednateli známých (včetně např. zdržení v dodavatelsko-odběratelském řetězci, nenastalo-li z důvodů na straně zhotovitele, nebo okolnosti přičitatelné objednateli), majících vliv na možnosti zhotovitele plnit v předmětných lhůtách. Zhotovitel je povinen na žádost objednatele kteroukoliv jím tvrzenou skutečnost (okolnost) doložit.

6. Jsou-li akceptovány všechny části díla podle přílohy č. 11 této smlouvy a provedeny všechny další součásti díla včetně školení podle přílohy č. 9 této smlouvy, sepíší smluvní strany protokol o předání a převzetí díla.

7. Zhotovitel garantuje, že:

a) SCK s implementovaným Řešením je schopen rutinního provozu ve standardním systémovém prostředí objednatele (viz přílohy č. 2 a 3 této smlouvy), a to i za pravidelného nasazování aktualizací (update / upgrade / patch / hotfix) komponent systémového prostředí objednatele i jen souvisejících s SCK [čl. I odst. 1 písm. b)],

b) poskytl veškeré potřebné licence pro správný a bezproblémový provoz SCK s implementovaným Řešením a poskytnuté licence odpovídají licenčním ujednáním dle čl. IX,

c) dodaný SCK s implementovaným Řešením je funkční dle předané realizační dokumentace.

Článek IV

Cena plnění a platební podmínky

1. Ceny plnění uvedené v odst. 2 až 6 tohoto článku byly stanoveny dohodou smluvních stran a zahrnují veškeré náklady zhotovitele (včetně náhradních dílů, práce, dopravného apod.) spojené s plněním podle této smlouvy.

2. Cena díla dle čl. I odst. 1 a 2 činí celkem 2 345 154,- Kč bez DPH, z toho cena za školení činí 28 000,- Kč bez DPH. Podrobnější rozpis ceny je obsažen v příloze č. 7 této smlouvy.

3. Cena za budoucí rozvoj podle čl. VI odst. 6 písm. a) a b) bude stanovena dohodou stran na základě cenové nabídky zhotovitele, a to podle předpokládaného rozsahu pracnosti a hodinové sazby podle přílohy č. 7. V případě, že výsledkem plnění bude autorské dílo, je v ceně takového plnění zahrnuta odměna za licenci.

4. Cena za budoucí rozvoj podle čl. VI odst. 6 písm. c) a d) bude stanovena jako součin počtu skutečně odpracovaných hodin a hodinové sazby podle přílohy č. 7.

5. Paušální cena za provozní podporu podle čl. VI odst. 3 až 5 této smlouvy činí čtvrtletně 187 707,- Kč bez DPH. Tato cena zahrnuje podporu pro 1750 uživatelů využívajících

funkcí čipových karet bez ohledu na množství čipových karet, které využívají, a prostředků, kde je nainstalován SW pro obsluhu těchto čipových karet. V případě dalších dodávek technických a programových prostředků podle čl. VII může být paušální cena za provozní podporu na základě dohody smluvních stran zvýšena nejvýše o 15 % z ceny dodávky. Zvýšení ceny podpory bude provedeno dodatkem ke smlouvě.

6. Ceny jednotlivých komponent v případě dalších dodávek technických a programových prostředků podle čl. VII jsou stanoveny v příloze č. 7.
7. K cenám bude účtována DPH v sazbě platné v den uskutečnění příslušného zdanitelného plnění.
8. Daňový doklad na cenu podle odst. 2 tohoto článku je zhotovitel oprávněn vystavit nejdříve v den podpisu protokolu o předání a převzetí díla.
9. Cena podle odst. 3 tohoto článku bude hrazena na základě daňového dokladu vystaveného nejdříve v den převzetí plnění.
10. Cena podle odst. 4 tohoto článku bude hrazena na základě daňového dokladu vystaveného nejdříve ke dni uskutečnění zdanitelného plnění, kterým je poslední den měsíce, ve kterém bylo příslušné plnění poskytováno. Přílohou daňového dokladu bude objednatelem odsouhlasený výkaz práce.
11. Paušální cena podle odst. 5 tohoto článku bude hrazena čtvrtletně na základě daňového dokladu vystaveného vždy nejdříve k prvnímu dni, v němž je v daném kalendářním čtvrtletí provozní podpora poskytována. V případě, že provozní podpora bude zahájena jiným, než prvním dnem kalendářního čtvrtletí, nebo ukončena jiným, než posledním dnem kalendářního čtvrtletí, je hrazena pouze alikvotní část paušální ceny podle odst. 5 tohoto článku.
12. Cena dalších dodávek technických a programových prostředků dle odst. 6 tohoto článku bude hrazena na základě daňového dokladu vystaveného nejdříve ke dni převzetí plnění.
13. Doklady k úhradě (fakturu) zašle zhotovitel elektronicky jako přílohu e-mailové zprávy na adresu faktury@cnb.cz ve formátu ISDOC. Pokud není možné vytvořit doklad ve formátu ISDOC, je možné zasílat jej ve formátu PDF. V jedné e-mailové zprávě smí být pouze jeden doklad k úhradě. Mimo vlastní doklad k úhradě může být přílohou e-mailové zprávy jedna až sedm příloh k dokladu ve formátech PDF, DOC, DOCX, XLS, XLSX. Přijaty budou i doklady k úhradě v jiném formátu, který bude v souladu s evropským standardem elektronické faktury. Nebude-li možné zaslat doklad k úhradě elektronicky, zašle jej zhotovitel v analogové formě na adresu:

    Česká národní banka
    sekce rozpočtu a účetnictví
    odbor účetnictví
    Na Příkopě 28
    115 03 Praha 1

14. Doklad k úhradě bude obsahovat údaje podle § 435 občanského zákoníku a bankovní účet, na který má být placeno, a který je uveden v záhlaví této smlouvy nebo který byl později aktualizován zhotovitelem (dále jen „určený účet“). Daňový doklad bude nadto obsahovat náležitosti stanovené v zákoně o dani z přidané hodnoty. Nezbytnou náležitostí každého dokladu je také číslo této smlouvy (ve formátu ISDOC v poli ID ve skupině Contract References). Pokud doklad bude postrádat některou ze stanovených náležitostí nebo bude obsahovat chybné údaje, je objednatel oprávněn jej vrátit zhotoviteli, a to až do lhůty splatnosti. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného dokladu.

15. V případě, že bude v dokladu k úhradě uveden jiný než určený účet, je pověřený pracovník zhotovitele povinen na základě výzvy objednatele sdělit na e-mailovou adresu, ze které byla výzva odeslána, zda má být zaplaceno na bankovní účet uvedený v dokladu, nebo na určený účet. V tomto případě se doklad k úhradě nevrací s tím, že lhůta splatnosti začíná běžet až dnem doručení sdělení zhotovitele podle předchozí věty.
16. Splatnost dokladů činí 14 dnů ode dne jejich doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu zhotovitele.
17. Zhotovitel je oprávněn navrhnout změnu cen podle odst. 3, 4 a 5 v návaznosti na vývoj indexu cen tržních služeb, stejné období předchozího roku = 100, konkrétně index J62 sloupec „Průměr od počátku roku“, a to průměr za předchozí kalendářní rok, který vyhlašuje Český statistický úřad. Ceny mohou být zvýšeny maximálně o částku odpovídající předmětné roční inflaci. Úprava cen (y) bude provedena formou dodatku ke smlouvě. První úpravu cen může zhotovitel navrhnout po uplynutí jednoho roku od zahájení poskytování provozní podpory.
18. Smluvní strany se ve smyslu občanského zákoníku dohodly, že objednatel je oprávněn započíst jakoukoli svou peněžitou pohledávku za zhotovitelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce zhotovitele za objednatelem, ať splatné či nesplatné.

Článek V

Další povinnosti smluvních stran, pověřené osoby

1. Objednatel se zavazuje vytvořit zhotoviteli k instalaci potřebné podmínky, zejména:
   a) umožnit zhotoviteli vykládku a úschovu technických prostředků v prostorách objednatele určených k instalaci v termínu, o kterém bude zhotovitelem zpraven nejméně 3 pracovní dny předem;
   b) převzít technické prostředky do úschovy a zajistit jejich bezpečné uskladnění do zahájení jejich instalace;
   c) zajistit provozní odstávky aplikací dotčených migrací dat s tím, že v rámci geografického clusteru je v pracovní době možná odstávka vždy jen jednoho serveru clusteru. Odstávky celého clusteru je možné provádět jen během víkendu. Takovou odstávku je nutné avizovat nejméně 7 pracovních dnů předem. Maximální přípustné doby provozních odstávek jsou uvedeny v příloze č. 4 této smlouvy v požadavku „Provozní odstávky“;
   d) zajistit potřebné rekonfigurace technických a programových prostředků a systémů dotčených přechodem na dodávané prostředky za podmínky, že neohrozí stávající provoz;
   e) přidělit IP adresy pro dodávané prostředky;
   f) zajistit přístup odborných pracovníků zhotovitele na příslušná pracoviště objednatele.
2. Pověřenými osobami pro:
   a) plný rozsah činností dle této smlouvy jsou:
      - za objednatele: [redacted]

- za zhotovitele: 

b) řešení problémů v rámci provozní podpory (právo zadávat požadavky):

- za objednatele: 

- za zhotovitele:

3. Zhotovitel je povinen vést deník o instalaci, tj. průběžně zaznamenávat provedené změny v celém průběhu implementace Řešení a zajišťovat zápisy z jednání a protokoly o zpřístupnění či poskytnutí funkčních celků implementovaného Řešení. Informace z deníku o instalaci musí zhotovitel přenést do realizační dokumentace.
4. Zhotovitel poskytne objednateli asistenci při vytváření instalačních balíčků, instalaci a případných úpravách veškerých dodaných programových prostředků (SW) na všech aplikačních serverech a klientských stanicích (platformy Linux, Windows a Igel; blíže viz příloha č. 2, a to nejpozději před zahájením testovacího provozu (vytvoření balíčků) a dále v jeho průběhu a též telefonicky po dobu 2 týdnů od jeho ukončení (instalace a případné úpravy).
5. Zhotovitel v rámci testovacího provozu, na základě údajů při něm získaných, uzpůsobí v realizační studii obsažený návrh plánu ostrého přechodu a předá jej objednateli.
6. Zhotovitel v rámci ověřovacího provozu, na základě údajů při něm získaných, vytvoří a předá objednateli návrh optimalizace SCK s implementovaným Řešením. Objednatel může zhotoviteli tuto povinnost prominout, jeví-li se fungování SCK s implementovaným Řešením jako optimální.
7. Zhotovitel prohlašuje, že jím dodané technické i programové prostředky pochází od certifikovaného / autorizovaného distributora a poskytovatele technické podpory v rámci evropského hospodářského prostoru a jsou určeny pro prodej na jednotném evropském trhu. Výjimkou jsou takové prostředky, u nichž je sám výrobcem. Zhotovitel je po dobu účinnosti této smlouvy povinen na požádání objednateli tuto skutečnost doložit, a to do 5 pracovních dnů ode dne doručení požadavku objednatele.
8. Zhotovitel je povinen zajistit, aby jeho pracovníci, kteří se budou podílet na plnění této smlouvy, splňovali kvalifikační kritéria, která objednatel požadoval v kvalifikačních požadavcích zadávacího řízení na předmět této smlouvy (bod 8.3.2 zadávací dokumentace). Zhotovitel je po dobu účinnosti této smlouvy povinen na požádání kvalifikaci jednotlivých osob objednateli doložit, a to do 5 pracovních dnů ode dne doručení požadavku objednatele.
9. V případě poskytování služeb prostřednictvím poddodavatele platí všechna relevantní ustanovení tohoto článku také pro poddodavatele a jeho pracovníky, kteří se budou na plnění smlouvy podílet. V případě, že zhotovitel splnil některý z požadavků stanovených objednatelem v zadávací dokumentaci zadávacího řízení na předmět této

smlouvy prostřednictvím poddodavatele, je povinen v případě změny tohoto poddodavatele na požádání objednatele prokázat, že nový poddodavatel tento požadavek splňuje, a to do 5 pracovních dnů ode dne doručení požadavku objednatele.

10. Zhotovitel je povinen prokázat, že dodávané čipové karty a USB tokeny jsou provozovatelné v režimu QSCD a jsou současně uvedeny na seznamu kvalifikovaných prostředků - **https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds** a je zajištěno dodávání kvalifikovaných certifikátů pro realizaci kvalifikovaných elektronických podpisů. To vše musí čipové karty a USB tokeny splňovat po dobu 5 let ode dne podpisu protokolu o předání a převzetí díla.
11. Objednatel si vyhrazuje právo ověřit si skutečnosti dle odst. 7 až 10 tohoto článku. Objednatel si dále vyhrazuje právo prověřovat schopnost zhotovitele dostát lhůtám definovaným v čl. VI odst. 3.
12. V případě, že se na dodávaných čipových kartách, tokenech nebo USB nebo bluetooth čtečkách (dále společně „čtečky“) v rámci jakýchkoliv po sobě jdoucích 12 měsíců projeví táž závada více než 50krát, má objednatel právo požadovat nahrazení příslušného dodávaného technického prostředku jiným jeho bezvadným typem splňujícím technické požadavky podle přílohy č. 4, a to za shodnou cenu.

Článek VI

Provozní podpora a budoucí rozvoj

1. Zhotovitel poskytuje objednateli pro **stávající i nově dodané technické a programové prostředky SCK** provozní podporu, a to ode dne následujícího po podpisu akceptačního protokolu realizační studie podle přílohy č. 11 této smlouvy.
2. Poskytování provozní podpory v sobě zahrnuje odstraňování závad, provozní údržbu a aktualizace SCK.
3. Podmínky pro odstraňování závad **stávajících i nově dodaných technických a programových prostředků SCK** a klasifikace závad (kritické/nekritické) jsou následující:

   a) Pokud uskutečnění servisního zásahu bude vyžadovat provozní odstávku, musí zhotovitel dodržet maximálně stanovené časy odstávek dle přílohy č. 4 této smlouvy, část „Provozní odstávky“.

   b) **Odstraňování kritických závad technických a programových prostředků**:

   Za kritickou závadu se považuje taková závada, kdy na úrovni operačního systému serveru v rámci SCK běžícího v libovolné lokalitě:

   - není možné přihlášení do managementu SCK ani v jedné z lokalit a není to způsobeno závadou na komunikační trase zajišťované objednatelem;
   - není možné generovat klíčový pár a žádost o certifikát na čipových kartách nebo USB tokenech a je to způsobeno některou komponentou SCK;
   - není možné realizovat přihlášení prostřednictvím certifikátu na čipové kartě nebo USB tokenu a není to způsobeno závadou na komunikační trase zajišťované objednatelem.

   Mezi kritické závady dále patří také zásadní výkonnostní problémy, např. latence při přihlášení delší než 2 min.

Řešení kritické závady musí být zahájeno nejpozději do 2 hodin v pracovních dnech od 8:00 do 18:00 hodin a závada musí být odstraněna do 24 hodin od nahlášení závady.

c) **Odstraňování nekritických závad technických a programových prostředků**:

Za nekritickou závadu se považuje taková závada technických a programových prostředků, která neohrožuje vlastní provoz těchto prostředků, zejména:

- ostatní závady na managementu SCK a SW na klientech;
- nefunkčnost managementu SCK v jedné z lokalit;
- ztráta interoperability mezi jednotlivými částmi SCK (např. omezení funkčnosti používaných technických prostředků ve vztahu k programovým prostředkům a jimi navzájem);
- nefunkčnost některých technických prostředků v rámci SCK.

Řešení nekritické závady musí být zahájeno nejpozději následující pracovní den po jejím ohlášení zhotoviteli a dokončeno do 10 pracovních dnů od jejího nahlášení. Dohodou smluvních stran může být lhůta pro odstranění závady prodloužena v případě, kdy zhotovitel prokáže objektivní důvody, které mu brání v odstranění závady. Práce na odstranění závady v místě plnění je zhotovitel oprávněn provádět pouze v pracovních dnech od 8:00 do 18:00 hodin, nedohodnou-li se pověřené osoby smluvních stran jinak.

d) Pokud závadu zjistí zhotovitel, oznámí ji neprodleně objednateli a další postup při jejím odstraňování se řídí ustanoveními tohoto článku s tím, že stanovené lhůty běží od oznámení závady objednateli.

e) Zhotovitel je srozuměn s tím, že veškerá komunikace při hlášení a řešení závad bude mezi objednatelem a pracovníky zhotovitele probíhat v českém jazyce. Při eskalaci řešení problémů k výrobci technických a programových prostředků je akceptována i komunikace v anglickém jazyce.

f) Odstranění závady zahrnuje jak **výměnu nebo opravu** vadného **technického nebo programového prostředku,** tak **zprovoznění** nového nebo opraveného prostředku včetně jeho **úplné konfigurace**. Pokud nebude možné na vadném technickém prostředku prokazatelně bezpečně smazat data objednatele, bude oprava provedena výměnou s tím, že vadný technický prostředek se zhotoviteli nevrací.

g) Za závadu se nepovažuje technologická nefunkčnost konkrétního jednotlivého technického prostředku (čipové karty, čtečky atd.) po uplynutí 24 měsíců od jeho převzetí objednatelem.

4. Provozní údržba zahrnuje 1x za pololetí:

a) provedení kontroly správné funkce SCK;

b) analýzu a kontrolu logů SCK;

c) doporučení nezbytných úprav pro dosažení správné funkce SCK a jejich realizace.

5. Aktualizace zahrnují:

a) informování objednatele o aktualizacích/opravách/nových verzích SCK;

b) informování objednatele o ukončení podpory konkrétních verzí všech komponent SCK v předstihu alespoň 60 pracovních dnů;

c) poskytnutí aktualizací/oprav/nových verzí všech programových prostředků SCK včetně případné implementace;

d) aktualizace realizační dokumentace SCK, pokud na ni měla aktualizace/oprava/nová verze vliv.

6. Budoucí rozvoj v sobě zahrnuje:

a) vypracování písemných analýz a návrhů řešení nových uživatelských požadavků objednatele na úpravy SCK;

b) úpravy SCK, příp. včetně úprav realizační dokumentace, na základě a podle požadavku objednatele;

c) řešení provozních situací a problémů, které nespadají do provozní podpory;

d) konzultace na žádost objednatele související s SCK.

Činnosti podle písm. a) a b) poskytuje zhotovitel ve lhůtách dle dohody pověřených osob smluvních stran. Nedohodnou-li se, určí přiměřenou lhůtu objednatel e-mailem.

Činnosti podle písm. c) jsou poskytovány ve lhůtách podle odst. 3 písm. b) a c) v závislosti na závažnosti provozní situace nebo problému, pověřená osoba objednatele může lhůtu na žádost zhotovitele prodloužit.

Konzultace podle písm. d) poskytuje zhotovitel ve lhůtě dohodnuté pověřenými osobami. Nedohodnou-li se, určí termín objednatel e-mailem s tím, že bude stanoven nejméně 7 pracovních dnů od doručení e-mailu objednatele.

7. Služby poskytované zhotovitelem musí vyhovovat technickým specifikacím a požadavkům výrobce příslušného technického prostředku.

8. Požadavky na odstranění závad a na ostatní služby podle této smlouvy budou hlášeny na tel.: **+420 222 268 747** s následným písemným potvrzením e-mailem na e-mailovou adresu **pověřené osoby zhotovitele** nebo požadavek pověřená osoba objednatele nahlásí e-mailem na e-mailovou adresu zhotovitele: **hotlinecnb@tsoft.cz**. Přijetí požadavku je zhotovitel povinen potvrdit e-mailem na adresu pověřených osob objednatele uvedených v čl. V odst. 2 písm. b), a to nejpozději do 2 hodin od přijetí požadavku.

9. Kategorii závady podle odst. 3 písm. b) a c), resp. provozní situace nebo problému u činnosti podle odst. 6 písm. c), v případě pochybností určí objednatel; jeho rozhodnutí ve věci je konečné.

10. O každém provedeném servisním zásahu nebo údržbě vyhotoví pracovník zhotovitele zápis o provedení práce, který stvrdí svým podpisem přejímající pracovník objednatele.

Článek VII

Další dodávky technických a programových prostředků

1. Zhotovitel se zavazuje dodat další kompatibilní technické a programové prostředky, specifikované v příloze č. 1 této smlouvy, v následujících dodacích lhůtách:

a) hybridní čipové karty do 2 měsíců od doručení objednávky; minimální objednávka ze strany objednatele je 200 ks,

b) kontaktní čipové karty do 1 měsíce od doručení objednávky; minimální objednávka ze strany objednatele je 5 ks,

c) USB tokeny do 1 měsíce od doručení objednávky; minimální objednávka ze strany objednatele je 5 ks,

d) USB čtečky čipových karet do 1 měsíce od doručení objednávky; minimální objednávka ze strany objednatele je 20 ks,

e) bluetooth čtečky čipových karet do 1 měsíce od doručení objednávky; minimální objednávka ze strany objednatele je 1 ks,

f) klientské programové prostředky / licence (SW) do 1 měsíce od doručení objednávky; minimální objednávka ze strany objednatele jsou programové prostředky / licence (SW) pro 100 uživatelů,

g) programové prostředky / licence (SW) pro centrální správu čipových karet do 1 měsíce od doručení objednávky; minimální objednávka ze strany objednatele jsou programové prostředky / licence (SW) pro centrální správu 100 uživatelů.

2. Objednávky budou předkládány prostřednictvím elektronické pošty na e-maily pověřených osob zhotovitele uvedené v čl. V odst. 2 písm. a).

3. Převzetí dodávky objednatel potvrdí poté, co ověří její funkčnost a kompatibilitu. Potvrzení o převzetí plnění vystaví kterákoliv z pověřených osob objednatele dle čl. V odst. 2 písm. a) a následující pracovní den je prostřednictvím elektronické pošty zašle na e-maily pověřených osob zhotovitele uvedené v čl. V odst. 2 písm. a). Objednatel ověří funkčnost a kompatibilitu do 10 pracovních dnů od podpisu dodacího listu objednatelem. Objednatel je oprávněn akceptovat plnění bez výhrad také tím, že do 12 dnů od podpisu dodacího listu objednatelem neodešle potvrzení o převzetí plnění nebo oznámení o tom, že plnění má vady.

4. Provozní podpora dle čl. VI se vztahuje i na HW a SW dodaný dle tohoto článku.

Článek VIII

Smluvní pokuty, úrok z prodlení

1. V případě prodlení zhotovitele má objednatel právo požadovat smluvní pokutu:

   a) ve výši 2 000 Kč za každý den prodlení ve lhůtě dle čl. III odst. 3 písm. a) této smlouvy;

   b) ve výši 10 000 Kč za každý den prodlení v jakékoliv ze lhůt dle čl. III odst. 3 písm. b) této smlouvy;

   c) ve výši 10 000 Kč za každý den prodlení ve lhůtě dle čl. III odst. 4 této smlouvy.

2. V případě prodlení zhotovitele má objednatel právo požadovat smluvní pokutu:

   a) ve výši 20 000 Kč za každou hodinu prodlení ve lhůtě pro zahájení řešení kritické závady dle čl. VI odst. 3 písm. b) této smlouvy;

   b) ve výši 20 000 Kč za každou hodinu prodlení ve lhůtě pro odstranění kritické závady dle čl. VI odst. 3 písm. b) této smlouvy;

   d) ve výši 1 000 Kč za každý pracovní den prodlení ve lhůtě pro zahájení řešení nebo ve lhůtě pro odstranění nekritické závady dle čl. VI odst. 3 písm. c) této smlouvy;

   e) ve výši 2 000 Kč za každou hodinu prodlení ve lhůtě pro potvrzení přijetí požadavku na servisní zásah dle čl. VI odst. 8 této smlouvy v případě ohlášení kritické vady.

3. V případě, že se po dobu 12 měsíců ode dne předání díla prokáže, že nebyly splněny některé z požadavků uvedených v příloze č. 4 této smlouvy „Technické podmínky

předmětu plnění“, má objednatel právo požadovat smluvní pokutu ve výši 30 000 Kč za každý případ nedodržení takového požadavku. Tím nejsou dotčena práva na odstoupení od smlouvy ani na náhradu vzniklé škody.

4. V případě prodlení zhotovitele ve lhůtě pro prokázání skutečností požadovaných objednatelem podle čl. V odst. 7 až 9 této smlouvy je objednatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
5. V případě porušení povinnosti podle čl. V odst. 10 této smlouvy je objednatel oprávněn požadovat smluvní pokutu ve výši 200 000 Kč za každý rok do konce pětiletého období podle citovaného ustanovení.
6. V případě prodlení zhotovitele ve lhůtě k odstranění závady uvedené v akceptačním protokolu podle části 3) písm. b) přílohy č. 11 této smlouvy má objednatel právo požadovat smluvní pokutu:
   a) ve výši 20 000 Kč za každou hodinu prodlení, byla-li závada v akceptačním protokolu kategorizována jako kritická;
   b) ve výši 1 000 Kč za každý pracovní den prodlení, byla-li závada v akceptačním protokolu kategorizována jako nekritická nebo kategorizována nebyla.
7. V případě prodlení s uhrazením daňového dokladu zaplatí objednatel zhotoviteli úrok z prodlení podle předpisů občanského práva.
8. Smluvní pokutou není dotčen nárok na náhradu škody.

Článek IX

Vlastnictví, nebezpečí škody na věci a licenční ujednání

1. Vlastnictví k technickým prostředkům (HW) dle této smlouvy přechází na objednatele dnem předání a převzetí díla, resp. dalšího plnění. Právo užívání programových prostředků (SW) nabývá objednatel ode dne, kdy zhotovitel poskytl objednateli k těmto prostředkům přístup.
2. Dnem převzetí nových technických prostředků (HW) objednatelem do úschovy přechází nebezpečí škody na těchto prostředcích na objednatele.
3. Zhotovitel poskytuje objednateli nevýhradní, nepřevoditelnou a místně neomezenou licenci na dobu trvání majetkových práv, umožňující užívat poskytnuté programové prostředky (SW), dodané dle této smlouvy, pro vnitřní potřebu objednatele a pro potřeby dalších externích subjektů, avšak pouze v rámci IS, které provozuje objednatel. Počet uživatelů je omezen ustanoveními této smlouvy [čl. I odst. 1 písm. a) a čl. VII odst. 1 písm. f) a g)].
4. Licence podle odst. 3 je poskytována též pro dokumentaci podle čl. I odst. 2 písm. d).
5. Licence se vztahuje i na veškeré poskytnuté aktualizace poskytnutých programových prostředků (tj. update / upgrade / patch / hotfix atd.), na programové prostředky poskytnuté dle čl. VII a autorská díla vytvořená v rámci budoucího rozvoje dle čl. VI.
6. Zhotovitel poskytuje objednateli nevýhradní, nepřevoditelnou a místně neomezenou licenci na dobu trvání majetkových práv k tomu, aby objednatel sám nebo prostřednictvím třetí osoby mohl užívat realizační dokumentaci podle čl. I odst. 2 písm. e) v souvislosti s poskytováním provozní podpory nebo budoucího rozvoje SCK. Realizační dokumentaci nebo její části může dále objednatel sám nebo prostřednictvím třetí osoby měnit, upravovat,

zpracovávat, spojovat s jiným (autorským) dílem / prvky či zařazovat do jiného (autorského) díla souborného.

7. Objednatel není povinen licence využít.
8. Zhotovitel prohlašuje, že práva, která touto smlouvou poskytuje, mu náleží bez jakéhokoliv omezení, a odpovídá za škodu, která by objednateli vznikla, pokud by toto prohlášení bylo nepravdivé.

Článek X

Mlčenlivost, bezpečnostní požadavky objednatele

1. Zhotovitel se zavazuje zajistit, že jeho pracovníci a pracovníci jeho poddodavatelů, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se u objednatele seznámí a které nejsou veřejně známy. Povinnost mlčenlivosti není časově omezena.
2. Zhotovitel se zavazuje v plném rozsahu dodržovat bezpečnostní požadavky objednatele, které jsou uvedeny v příloze č. 5 této smlouvy.

Článek XI

Odstoupení od smlouvy, výpověď

1. Smlouva se v částech týkajících se podpory a dalších dodávek technických a programových prostředků uzavírá na dobu neurčitou. Kterákoliv smluvní strana je oprávněna smlouvu vypovědět. Smlouvu nelze vypovědět v prvních 4 letech jejího trvání ode dne předání a převzetí díla. Výpovědní doba smlouvy činí 1 rok a začíná běžet prvním dnem v měsíci následujícím po měsíci, v němž došla výpověď druhé smluvní straně.
2. V případě, že některá ze smluvních stran podstatně poruší smluvní povinnost vyplývající pro ni z této smlouvy, je druhá smluvní strana oprávněna od smlouvy odstoupit. Objednatel je oprávněn odstoupit i od části smlouvy.
3. Za podstatné porušení smluvní povinnosti se považuje zejména:

- ze strany zhotovitele:

a) nesplnění kteréhokoli požadavku / požadované funkce uvedených v příloze č. 4 této smlouvy,

b) prodlení zhotovitele ve kterékoli lhůtě dle čl. III odst. 3 písm. a) až c) a odst. 4 delší než 5 týdnů,

c) případ, kdy zhotovitel nebude schopen v rámci implementace dodržet maximálně stanovené časy odstávek uvedené v příloze č. 4 této smlouvy, v požadavku „Provozní odstávky“,

d) opakované porušení kterékoliv povinnosti zhotovitele dle čl. V odst. 3 a 4,

e) porušení kterékoliv povinnosti zhotovitele dle čl. V odst. 5 až 10 a 12,

f) opakované prodlení se zahájením prací na odstraňování kritické závady v rámci provozní podpory delším než 2 hodiny od nahlášení podle čl. VI této smlouvy,

g) opakované prodlení s odstraněním nekritické závady v rámci provozní podpory programových prostředků;

- ze strany objednatele:

  a) prodlení s úhradou kteréhokoliv daňového dokladu k úhradě delším než 30 dnů,

  b) neposkytnutí součinnosti předpokládané touto smlouvou ani na opakovanou písemnou výzvu zhotovitele.

4. Smluvní strany se dále dohodly, že objednatel je oprávněn odstoupit od smlouvy kdykoliv v průběhu insolvenčního řízení zahájeného na majetek zhotovitele.
5. Smluvní strany si v souladu s ustanovením § 1992 občanského zákoníku sjednávají, že objednatel je oprávněn zrušit tuto smlouvu zaplacením odstupného ve výši 50 000 Kč na účet zhotovitele, a to kdykoliv před akceptací realizační studie podle přílohy č. 11 této smlouvy. Zrušení smlouvy je účinné zaplacením sjednaného odstupného na bankovní účet zhotovitele, č. ú.: 1010251000 / 2700. Zaplacením odstupného zanikají všechna práva a povinnosti obou smluvních stran vyplývající ze zrušené smlouvy s výjimkou závazku mlčenlivosti zhotovitele.
6. V případě odstoupení od smlouvy objednatelem se zhotovitel zavazuje na své náklady uvést SCK a všechny další komponenty systémového prostředí objednatele související s SCK, případně další jím nedopatřením či záměrně ovlivněné komponenty systémového prostředí objednatele, do původního stavu a zajistit odvoz technických a programových prostředků, a to nejpozději do 30 dnů ode dne doručení oznámení o odstoupení od smlouvy.
7. Odstoupení od smlouvy je účinné dnem doručení oznámení o odstoupení od smlouvy druhé smluvní straně.

Článek XII

Uveřejnění smlouvy a skutečně uhrazené ceny za plnění smlouvy

1. Zhotovitel si je vědom zákonné povinnosti objednatele uveřejnit na svém profilu tuto smlouvu včetně všech jejích případných změn a dodatků a výši skutečně uhrazené ceny za plnění této smlouvy.
2. Profilem objednatele je elektronický nástroj, prostřednictvím kterého objednatel, jako veřejný zadavatel dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ“), uveřejňuje informace a dokumenty ke svým veřejným zakázkám způsobem, který umožňuje neomezený a přímý dálkový přístup, přičemž profilem objednatele v době uzavření této smlouvy je https://ezak.cnb.cz/.
3. Povinnost uveřejňování dle tohoto článku je objednateli uložena § 219 ZZVZ.
4. Uveřejňování bude prováděno dle ZZVZ a příslušného prováděcího předpisu k ZZVZ.

Článek XIII

Závěrečná ustanovení

1. Smlouva nabývá platnosti a účinnosti dnem podpisu oprávněnými zástupci obou smluvních stran.
2. Smlouva může být měněna a doplňována pouze formou písemných vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran, není-li ve smlouvě uvedeno jinak. Za písemnou formu nebude pro účel uvedený v tomto odstavci považována

výměna e-mailových či jiných elektronických zpráv, není-li ve smlouvě uvedeno jinak.

3. Zhotovitel prohlašuje, že po dobu účinnosti této smlouvy bude mít sjednáno pojištění pro případ vzniku odpovědnosti za škodu způsobenou třetí osobě v souvislosti s plněním této smlouvy, a to s pojistným plněním ve výši nejméně 5 000 000 Kč (slovy: pět milionů korun českých) s tím, že jeho spoluúčast nepřevyšuje 5 %. Zhotovitel se zavazuje, že pojištění v uvedené výši a rozsahu zůstane účinné po celou dobu účinnosti této smlouvy a do 5 pracovních dnů od výzvy objednatele je zhotovitel povinen toto objednateli prokázat.
4. Použije-li zhotovitel při své činnosti poddodavatele, nahradí škodu jím způsobenou stejně, jakoby ji způsobil sám.
5. Smlouva je sepsána v českém jazyce. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě bude probíhat v českém nebo slovenském jazyce, nebude-li smluvními stranami v konkrétním případě dohodnuto jinak nebo nestanoví-li tato smlouva jinak.
6. Závazkové vztahy touto smlouvou založené se řídí českým právním řádem, zejména zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
7. Smluvní strany se dohodly, že případný spor, který vznikne z této smlouvy nebo v souvislosti s ní, bude rozhodován výlučně podle českého práva obecnými soudy v České republice.
8. Smlouva je vyhotovena ve třech stejnopisech, z nichž objednatel obdrží dvě a zhotovitel jedno vyhotovení.
9. Odpověď strany této smlouvy podle § 1740 odst. 3 občanského zákoníku s dodatkem nebo odchylkou není přijetím nabídky, ani když podstatně nemění podmínky nabídky.
10. Uplatnění domněnky doby dojití dle § 573 občanského zákoníku se vylučuje.

Přílohy:
- č. 1 Specifikace dodávaných technických a programových prostředků
- č. 2 Seznam zařízení a operačních systémů objednatele
- č. 3 Terminologie a popis stávajícího řešení SCK a souvisejících komponent systémového prostředí objednatele
- č. 4 Technické podmínky předmětu plnění
- č. 5 Bezpečnostní požadavky ČNB
- č. 6 Návrh technického řešení
- č. 7 Specifikace cen včetně podrobného rozpisu ceny plnění
- č. 8 Vzor realizační studie
- č. 9 Rozsah, obsah a lhůty školení
- č. 10 Obsah realizační dokumentace
- č. 11 Ověřování funkčnosti a akceptace

V Praze dne: 24.8. 2021

Za objednatele:

[redacted]

Ing. Milan Zirnsák
ředitel sekce informatiky

[redacted]

Ing. Zdeněk Virius
ředitel sekce správní

[redacted]

ČNB ČESKÁ NÁRODNÍ BANKA
Na Příkopě 28, 115 03 Praha 1
48

V Praze dne: 20.8. 2021

Za zhotovitele:

[redacted]

Ing. Maroš Jančovič
předseda představenstva

[redacted]

Ing. Michal Vaněček, Ph.D., MBA
místopředseda představenstva

T-SOFT a.s.
Za Brumlovkou 1559/5
140 00 Praha 4
Tel.: 222 268 738
IČ: 40766314
DIČ: CZ40766314

Příloha č. 1

Specifikace dodávaných technických prostředků a programových prostředků

Soupis dodávaných technických prostředků a programových prostředků

U nabízených technických a programových prostředků uvádí Part Number někdy výrobce, jindy distributor, proto pro jednoduché ověření uvádíme také přímý odkaz na technickou specifikaci (Product Brief) produktů u výrobců.
Verze programových produktů jsou uváděny majoritním číslem, konkrétní úplná verze bude uvedena v prováděcím projektu. Vždy bude vybíráno z verzí, které jsou v době nasazení podporovány výrobcem a zároveň splňují požadavky zadavatele na kompatibilitu jeho stávajících technických a programových prostředků, specifikovaných v přílohách č. 2 a č. 3 Smlouvy.

Položka	Product Brief /Part Number	Výrobce	Stručný popis
Hybridní (duální) čipová karta SafeNet IDPrime MD940	https://cpl.thalesgroup.com/resources/access-management/idprime-940-product-brief 10-43061-003	GEMALTO - part of the THALES Group	Hybridní (duální) čipová karta na platformě IDPrime MD940, kde jsou implementovány 2 bezkontaktní čipy odpovídající technické specifikaci v příloze 2 a 3 ZD.
Kontaktní čipová karta SafeNet IDPrime MD940	https://cpl.thalesgroup.com/resources/access-management/idprime-940-product-brief O1132421	GEMALTO - part of the THALES Group	Kontaktní čipová karta QSCD.
USB token SafeNet e-token 5110 CC	https://cpl.thalesgroup.com/access-management/authenticators/pki-usb-authentication/etoken-5110-usb-token 909-000115-001	GEMALTO - part of the THALES Group	USB token QSCD.
USB čtečka čipových karet OMNIKEY 3121USB	https://www.hidglobal.com/products/readers/omnikey/3121 R31210320-01	HID Global	Robustní čtečka standardní velikosti vhodná pro denní kancelářské použití.
Bluetooth bezdrátová čtečka čipových karet AirID2	https://certgate.com/en/products/airid/ 100305	Certgate GmbH	Čtečka je ideální pro mobilní používání, velikost čtečky jen minimálně přesahuje formát standardní čipové karty.

Klientské programové prostředky (licence): SafeNet Authentication Client (SAC) Version 10	https://cpl.thalesgroup.com/resources/access-management/safenet-authentication-client-product-brief 10-43-108	GEMALTO - part of the THALES Group	Klientský software (middleware) pro podporu čipových karet. Kompatibilní se všemi typy karet, které zadavatel uvádí v příloze č. 2 ZD.
Programové prostředky / klientské licence (SW) pro centrální správu čipových karet: CMS MYID, MICROSOFT PKI, LIC, ONLY CLIENT LIC	https://www.intercede.com/myid-enterprise/ 926-000008-001-004	INTERCEDE	Licence pro klienta, jehož karta je spravována v nabízeném systému SCK (CMS) MyID.
Programové prostředky / serverové licence (SW) pro centrální správu čipových karet: CMS MYID ENTERPISE, MICROSOFT PKI, CD + SERVER LIC Version 11	https://www.intercede.com/myid-enterprise/ 925-000007-001-000	INTERCEDE	Rozšíření licence stávajícího serveru systému SCK (CMS) MyID ENTERPRISE o druhý server pro zajištění HA režimu.

Specifikace jednotlivých technických prostředků a programových prostředků

Hybridní (duální) čipové karty dle článku VII odstavec 1.a Smlouvy

Hardware	Čipová karta MD940 s až dvěma bezkontaktními čipy
Volné místo na certifikáty a další data	73 kB
Kontejnery na klíčové páry	20 (z toho 2 v CC části)
Podporované operační systémy	Windows Server 2016, 2012, Windows Server 2008/R2, Windows 7, Windows 8, Windows 8.1, Windows 10, Mac OS, Linux
Middleware:	SafeNet Authentication Client (SAC)
Počet zápisů / přepisů v paměti	500.000
Podporované symetrické algoritmy v hardware	3DES, AES 128/192/256
Podporované asymetrické algoritmy v hardware	RSA až 4096 bit, podpora RSA OAEP, ECDSA P-256, P-384, P-521

Podporované hash funkce	SHA1, SHA2 (256-512)
Podporované crypto API	PKCS#11, MS CryptoAPI, CNG, PC/SC, X.509v.3 Global Platform 2.2.1
Bezkontaktní čipy	Možno implementovat až 2 čipy podle potřeby. Aktuálně připravena konfigurace pro ČNB: Hybrid Card (HID ICLASS PROX COMP EMBED 16K, CONF., F-GLOSS, B-GLOSS, NO#, NO SLOT, LAM - 2132CGGNNN), white, PVC laminated with laserable overlay, chip serial number laser engraved on card body
Certifikace FIPS 140-2	úroveň 3
Certifikace apletu	EAL+ Protection Profile dle EN 419211 1-6
Certifikace čipu karty	EAL6+
Karta uvedena na evropském seznamu QSCD zařízení (eIDAS)	Ano
CSIRT tým výrobce karty a obslužného software	Ano
Prohlášení o shodě	Ano
Vyhovuje standardům RoHS	Ano
Podpora českých kvalifikovaných poskytovatelů služeb vytvářejících důvěru	PostSignum České pošty
Podporované jazyky obslužného software	Čeština, Angličtina, Francouzština, Němčina
Uživatel může kdykoliv změnit PIN	Ano
Nastavení PIN před prvním použitím	Ano
Uživatel může pojmenovat vlastní zařízení	Ano

Nastavitelná komplexnost 4 hesel - PIN, PUK, qPIN, qPUK	Ano

Kontaktní čipové karty dle článku VII odstavec 1.b Smlouvy

Hardware	Čipová karta IDPrime MD940
Volné místo na certifikáty a další data	73 kB
Kontejnery na klíčové páry	20 (z toho 2 v CC části)
Podporované operační systémy	Windows Server 2016, 2012, Windows Server 2008/R2, Windows 7, Windows 8, Windows 8.1, Windows 10, Mac OS, Linux
Middleware:	SafeNet Authentication Client (SAC)
Počet zápisů / přepisů v paměti	500.000
Podporované symetrické algoritmy v hardware	3DES, AES 128/192/256
Podporované asymetrické algoritmy v hardware	RSA až 4096 bit, podpora RSA OAEP, ECDSA P-256, P-384, P-521
Podporované hash funkce	SHA1, SHA2 (256-512)
Podporované crypto API	PKCS#11, MS CryptoAPI, CNG, PC/SC, X.509v.3 Global Platform 2.2.1
Certifikace FIPS 140-2	úroveň 3
Certifikace apletu	EAL+ Protection Profile dle EN 419211 1-6
Certifikace čipu karty	EAL6+
Karta uvedena na evropském seznamu QSCD zařízení (eIDAS)	Ano
CSIRT tým výrobce karty a obslužného software	Ano
Prohlášení o shodě	Ano
Vyhovuje standardům RoHS	Ano
Podpora českých kvalifikovaných poskytovatelů služeb vytvářejících důvěru	PostSignum České pošty
Podporované jazyky obslužného software	Čeština, Angličtina, Francouzština, Němčina
Uživatel může kdykoliv změnit PIN	Ano

Nastavení PIN před prvním použitím	Ano
Uživatel může pojmenovat vlastní zařízení	Ano
Nastavitelná komplexnost 4 hesel - PIN, PUK, qPIN, qPUK	Ano

Tokeny USB dle článku VII odstavec 1.c Smlouvy

Hardware	USB Token 5110 CC (sesterský typ karty MD940)
Volné místo na certifikáty a další data	73 kB
Kontejnery na klíčové páry	20 (z toho 2 v CC části)
Podporované operační systémy	Windows Server 2016, 2012, Windows Server 2008/R2, Windows 7, Windows 8, Windows 8.1, Windows 10, Mac OS, Linux
Middleware:	SafeNet Authentication Client (SAC)
Počet zápisů / přepisů v paměti	500.000
Podporované symetrické algoritmy v hardware	3DES, AES 128/192/256
Podporované asymetrické algoritmy v hardware	RSA až 4096 bit, podpora RSA OAEP, ECDSA P-256, P-384, P-521
Podporované hash funkce	SHA1, SHA2 (256-512)
Podporované crypto API	PKCS#11, MS CryptoAPI, CNG, PC/SC, X.509v.3 Global Platform 2.2.1
Certifikace FIPS 140-2	úroveň 3
Certifikace apletu	EAL+ Protection Profile dle EN 419211 1-6
Certifikace čipu karty	EAL6+
Karta uvedena na evropském seznamu QSCD zařízení (eIDAS)	Ano
CSIRT tým výrobce karty a obslužného software (uveďte odkaz)	Ano

Prohlášení o shodě	Ano
Vyhovuje standardům RoHS	Ano
Podpora českých kvalifikovaných poskytovatelů služeb vytvářejících důvěru	PostSignum České pošty
Podporované jazyky obslužného software	Čeština, Angličtina, Francouzština, Němčina
Uživatel může kdykoliv změnit PIN	Ano
Nastavení PIN před prvním použitím	Ano
Uživatel může pojmenovat vlastní zařízení	Ano
Nastavitelná komplexnost 4 hesel - PIN, PUK, qPIN, qPUK	Ano
Provozní podmínky:	teplota 0°C-70°C, vlhkost 0% - 100% (bez kondenzace)
Odolnost proti vodě:	certifikace IP X7 – IEC 60529
Rozhraní:	USB type A; USB 1.1 a 2.0 (full speed and high speed)
Velikost:	16,4 x 8,5 x 40,2 mm
Hmotnost:	5 g

USB čtečky čipových karet dle článku VII odstavec 1.d Smlouvy

Hardware	Stolní čtečka OMNIKEY 3121 USB
Připojení	USB 2.0
Interface čipové karty	Kontaktní interface (ISO7816-1/2/3/4) pro ID-1 karty (formát kreditní karty) , protokol T=1. T=0, PPS, up to 500Kbs
Podporované platformy	Windows 2000/XP/7/8/10, Windows server 2003/8/16, MacOS, LINUX
Další vlastnosti	Robustní konstrukce, možnost fixního umístění čtečky na pracovní stůl pomocí přiloženého stojánku.
Rozměry	80 x 67 x 28 mm

Hmotnost	110g

Bluetooth čtečky čipových karet dle článku VII odstavec 1.e Smlouvy

Hardware	Bezdrátová čtečka AirID 2, Business, wireless smartcard reader
Připojení	Bluetooth LE v. 4.2, USB
Interface čipové karty	Kontaktní interface (ISO7816-1/2/3/4) pro ID-1 karty (formát kreditní karty) , protokol T=1. T=0
Podporované platformy	Windows10, MacOS, iOS, Android, LINUX
Další vlastnosti	Bluetooth připojení chráněno navíc šifrováním (AES 256) Displej 132x32 pixelů, nabíjení přes USB
Rozměry	90 x 60 x 10 mm
Hmotnost	46 g

Klientské programové prostředky/licence (SW) dle článku VII odstavec 1.f Smlouvy

Software	Midleware SafeNet Authentication Client verze 10.x (aktuálně 10.8)
Podporované operační systémy (32 i 64 bit verze, pokud není výslovně uvedeno jinak)	Windows Server 2008 R2 SP1 Windows Server 2008 SP2 Windows Server 2012 and 2012 R2 (64-bit) Windows Server 2016 (64-bit) Windows 7 SP1 Windows 8, Windows 8.1 Windows 10 MAC OS X Linux Distributions: Ubuntu, CentOS, Red Hat 8, SUSE Linux enterprise desktop 15

	Fedora 30 Debian
Podporované API	PKCS#11 V2.20, MS CryptoAPI and CNG (CSP, KSP), Mac Keychain (TokenD), PC/SC
Podporované CA	Microsoft, Entrust, VeriSign
Podporované browsery	Firefox Internet Explorer Microsoft Edge (does not support certificate enrollment) Chrome (does not support certificate enrollment)
Klíčové vlastnosti	Inicializace tokenů Změna administrátorského (pokud je podporováno) a uživatelského PINu Odblokování zamknutých tokenů (Unlocking) Připojení/Odpojení eTokenu Virtual (softwarový token) Prohlížení, mazání, import a export certifikátů (ne privátních klíčů!) Konfigurace bezpečnostní politiky tokenu (vč. PIN quality) Logování Další klientská nastavení tokenu a management
Kompatibilita	Plná zpětná kompatibilita se všemi typy karet, které zadavatel uvádí v příloze č. 2 ZD.

Programové prostředky / licence klientů (SW) pro centrální správu čipových karet dle článku VII odstavec 1.g Smlouvy

Předmětem nabídky je navýšení licencí uživatelů, jejichž čipové karty jsou spravovány systémem SCK (CMS). Specifikaci určuje použitý server systému CMS (MyID).

Programové prostředky / licence serveru (SW) pro centrální správu čipových karet (SCK) pro zajištění HA režimu stávajícího serveru CMS MyID

Pro specifikaci parametrů systému CMS MyID ENTERPRISE jsme využili možnosti v ZD ponechat anglickou terminologii.

Software CMS	**MyID ENTERPRISE**
Credential management features	
Credential request and approval	✓
Face-to-face and multi-step credential issuance	✓
Card updates	✓
Batch issuing smart cards	✓
Card activation, including terms & conditions	✓
Card replacement and reprovision	✓
Administrator secure key recovery	✓
Client applications	
MyID Desktop	✓
Self-Service App	✓
Self-Service Kiosk	✓
Identity Agent	✓
Mobile SDKs and frameworks	On request
Integration	
Server operating system	Windows Server
Database platform	SQL Server SQL Azure
Certificate authorities	Microsoft Windows CA Entrust CA

	PrimeKey EJBCA Symantec (Digicert) MPKI UniCERT CA
Directories	Active Directory LDAP v3.0
Hardware Security Modules (HSMs)	nCipher nShield SafeNet Network HSM
Physical Access Control System (PACS) integration	On request
Smart Card bureau integration	On request
Product APIs	
System health check	✓
Lifecycle API	✓
Credential Web Service	✓
Device Management API	✓
SCEP API	✓
Reporting Web Service API	✓
SNMP Monitoring	✓
Certificate Authority Connector API	On request
Credential stores/devices	
Smart cards and USB tokens	✓
iOS and Android devices	✓
Microsoft Virtual Smart Cards	✓
Intel Authenticate	✓
Soft certificates (.pfx files)	✓
Cryptas Virtual Smart Cards	✓
Windows Hello for Business	✓
Peripherals	
Smart card printers	✓
Document scanners (WIA)	✓

Web cams	✓
Document printing (PIN letters)	✓
Platform capabilities	
Audit record creation and reporting	✓
Management Information reports	✓
Role-based access control to workflows	✓
Operator scope control to limit access to user records	✓
Secure authentication to MyID clients	✓
Cryptographic key management	✓
User and audit archival	✓

thalescpl.com

THALES

SafeNet IDPrime 940

Plug & Play Smart Cards

As cybercriminals get smarter and more determined than ever, more and more businesses and government agencies are coming to the realization that single-factor authentication solutions using simple usernames and passwords are not enough. Thales, the world leader in digital security, offers an extensive portfolio of identity and access management including a wide range of multi-factor authentication methods.

SafeNet IDPrime smart cards are designed for PKI-based applications, and come with a SafeNet minidriver that offers perfect integration with native support for Microsoft® environments (through Windows 10), without any additional middleware.

Compatible with Any Environment

In addition to its seamless integration into Windows ecosystems, the SafeNet IDPrime 940 is a contact interface smart card and is compatible with any environment through support by the SafeNet Authentication Client.

Strong Security

SafeNet IDPrime 940 Smart Cards are secured with both RSA up to 4096 and Elliptic curves algorithms, and address a range of use cases that require PKI security, including secure access, email encryption, secure data storage, digital signatures and secure online transactions for end users.

SafeNet IDPrime 940 is CC EAL5+ / PP Java Card certified for the Java platform and CC EAL5+ / PP QSCD certified for the combination of Java platform and PKI applet. SafeNet IDPrime 940 is qualified by the French ANSSI and is qualified according to the eIDAS regulations for both the eSignature and the eSeal applications.

Optional Onboard Applets

SafeNet IDPrime cards are multi-application smart cards, meaning they can have optional onboard applets for various functions. An MPCOS applet can be added to provide both e-purse and data management services.

Benefits

- Perfect integration in Windows environment—Certified and distributed by Microsoft, the SafeNet minidriver ensures immediate integration with all Microsoft environments, plus Plug & Play service up to Windows 10.
- Secure Flash mask chip—400 KB.
- Compatible with any environment—SafeNet IDPrime 940 is fully supported by the SafeNet Authentication Client.
- Compliant with eIDAS regulations—SafeNet IDPrime 940 is is fully qualified according the eIDAS regulations for both eSignature and eSeal applications, and is qualified by the French ANSSI. Its Java platform is also CC EAL5+ / PP Java Card certified.
- Multi-application smart cards—SafeNet IDPrime smart cards can have optional onboard applets for MPCOS e-purse.
- Enhanced cryptographic support—SafeNet IDPrime 940 offers PKI services with both RSA up to 4096 and elliptic curves up to 521 bits.

Product characteristics	
Memory	• SafeNet IDPrime 940 is based on a 400KB Flash memory chip. SafeNet IDPrime 940 comes as standard with 20 key containers. The memory available for certificates and other applets and data in this standard configuration is 73 KB.
Standards	• BaseCSP minidriver (SafeNet minidriver) • Global Platform 2.2.1 • Java Card 3.0.4 • ISO 7816
Operating systems	• Windows, MAC, Linux
Cryptographic algorithms	• Hash: SHA-1, SHA-256, SHA-384, SHA-512. • RSA: up to RSA 4096 bits • RSA OAEP & RSA PSS • P-256 bits ECDSA, ECDH. P-384 & P-521bits ECDSA, ECDH are available via a custom configuration • On-card asymmetric key pair generation (RSA up to 4096 bits & Elliptic curves up to 521 bits) • Symmetric: AES—For secure messaging and 3DES for Microsoft Challenge/Response only
Communication protocols	• T=0, T=1, PPS, with baud rate up to 446 Kbps at at 3.57 MZ (TA1=97h)
Other features	• Onboard PIN Policy • Multi-PIN support • SafeNet IDPrime family of cards can be customized (card body and programming) to fit customers' needs.
Thales applets (optional)	
MPCOS	• E-purse & secure data management application
Chip characteristics	
Technology	• Embedded crypto engine for symmetric and asymmetric cryptography
Lifetime	• Minimum 500,000 write/erase cycles • Data retention for minimum 25 years
Certification	• CC EAL6+
Security	
	• SafeNet IDPrime smart cards include multiple hardware and software countermeasures against various attacks: side channel attacks, invasive attacks, advanced fault attacks and other types of attacks. • The SafeNet IDPrime 940 is both CC EAL5+ / PP Java Card certified for the Java platform and CC EAL5+ / PP QSCD certified for the combination of Java platform plus PKI applet, is eIDAS qualified for both eSignature and eSeal, and qualified by the French ANSSI.

> thalescpl.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com

cpl.thalesgroup.com

THALES

SafeNet eToken 5110

To protect identities and critical business applications in today's digital business environment, organizations need to ensure access to online and network resources is always secure, while maintaining compliance with security and privacy regulations. SafeNet eToken 5110 offers two-factor authentication for secure remote and network access, as well as certificate-based support for advanced security applications, including digital signature and pre-boot authentication.

Two-Factor Authentication you can Trust

SafeNet eToken 5110 is a portable two-factor USB authenticator with advanced smart card technology. Certificate-based technology generates and stores credentials-such as private keys, passwords, and digital certificates inside the protected environment of the smart card chip. To authenticate, users must supply both their personal SafeNet eToken authenticator and password, providing a critical second level of security beyond simple passwords to protect valuable digital business resources.

Future-Proofed and Scalable with Centralized Management Control

SafeNet eToken 5110 is based on the advanced Thales IDCore platform, and integrates seamlessly with third-party applications through SafeNet Authentication development tools, supports SafeNet PKI and password management applications and software development tools, and allows customization of applications and extension of functionality through on-board Java applets. SafeNet eToken 5110 is also supported by SafeNet Authentication Client for full local admin and support for advanced token management, events and deployment.

Benefits

- Improves productivity by allowing employees and partners to securely access corporate resources
- Enables advanced certificate-based applications, such as digital signature and pre-boot authentication
- Portable USB token: no special reader needed
- Simple and easy to use – no training or technical know-how needed
- Expand security applications through on-board Java applets
- Enhance marketing and branding initiatives with private labeling and color options.

Supported Applications

- Secure remote access to VPNs and Web portals and Cloud Services
- Secure network logon
- Digital signing
- Pre-boot authentication

Technical Specifications

Supported operating systems	Windows Server 2008/R2, Windows Server 2012 and 2012 R2, Windows 7, Mac OS, Linux, Windows 8, Windows 10		
API & standards support	PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE, MS minidriver, CNG		
Memory size	80K		
Dimensions	5110– 16.4mm*8.5mm*40.2mm		
ISO specification support	Support for ISO 7816-1 to 4 specifications		
Operating temperature	0º C to 70º C (32º F to 158º F)		
Storage temperature	-40º C to 85º C (-40º F to 185º F)		
Humidity rating	0-100% without condensation		
Water resistance certification	IP X7 – IEC 60529		
USB connector	USB type A; supports USB 1.1 and 2.0 (full speed and high speed)		
Casing	Hard molded plastic, tamper evident		
Memory data retention	At least 10 years		
Memory cell rewrites	At least 500,000		
	SafeNet eToken 5110 FIPS	**SafeNet eToken 5110 CC**	**SafeNet eToken 5110**
On-board security algorithms	• Symmetric: AES, 3DES (Triple DES) 128/192/256 bit • Hash: SHA-256 • RSA: 2048-bit, • Elliptic curves: P-256, P-384, ECDH	• Symmetric: 3DES (ECB, CBC), AES (128, 192, 256 bits) • Hash: SHA-1, SHA-256, SHA-384, SHA-512 • RSA: up to RSA 4096 bits • RSA OAEP & RSA PSS • P-256 bits ECDSA, ECDH. • P-384 & P-521bits • ECDSA, ECDH are available via a custom configuration • On-card asymmetric key pair generation (RSA up to 4096 bits & Elliptic curves up to 521 bits) • Symmetric: AES—For secure messaging and 3DES for Microsoft Challenge/Response only	• Symmetric: 3DES (Triple DES), AES 128/192/256 bit • Hash: SHA1, SHA256 • RSA 1024-bit / 2048-bit • Elliptic curves: P-256, P-384, ECDH
Security certifications	FIPS 140-2 level 3	CC EAL5+ / PP QSCD, eIDAS qualified for both eSignature and eSeal, and qualified by the French ANSSI	FIPS 140-2 level 3(SC chip and OS)
Smart Card Platform	Thales IDCore 30 (rev B) and eToken applet	IDPrime MD 940	Thales IDCore 30 and eToken applet

> cpl.thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: apacsales.cpl@thalesgroup.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com

EXTENDED ACCESS TECHNOLOGIES

OMNIKEY® 3121 USB Desktop Reader

USB SMART CARD READER

- **Easy to install** – Eliminates the need to install drivers; uses native supported CCID drivers within the operating system.
- **Readily Compliant** – Meets all relevant industry standards for smooth integration in PC environment
- **Convenient and Reliable** – Multiple-base mounting options, robust housing, long USB cable
- **Suits Any Application** – Compatible with virtually any smart card and major PC operating system

The OMNIKEY® 3121 is a high-performance, USB smart card reader for desktop use that features multiple-base mounting options and a robust housing. Compliant with all industry standards, this reader is compatible with virtually any contact smart card, operating system and a variety of applications. The OMNIKEY 3121 is easy to install and wellsuited for all contact smart card operations, including single sign-on, online banking or digital signature applications.

FEATURES:

- Meets major standards, including ISO 7816, USB CCID, PC / SC, and HBCI (Home Banking Computer Interface) Specification
- Supports power management to support low energy schemes
- UPC barcode for easier logistics
- Bulk or single packaging option available
- Interchangeable standing base options available for both vertical and horizontal configurations
- USB CCID support makes integration into an existing system the easiest ever by connecting host and smart card reader without the need for additional drivers
- All major operating systems supported
- Meets GSA FIPS 201 requirements
- Supports high-speed data transmission

SPECIFICATIONS

	SMART CARD INTERFACE
Card Size	ID-1 (Full size)
Standards	ISO 7816
Supported Card Types	Class A: 5V @ 60 mA; Class B: 3 V @ 60 mA; Class C: 1.8V @35 mA ATR response time up to 1.6 s
Protocols	Asynchronous: T=0; T=1 Synchronous: S=8 (I^2C) ; S=9 (3-wire); S=10 (2-wire)
Insertion Cycles	100,000
Smart Card Interface Speed	420 kbps
Smart Card Clock Frequency	up to 12 MHz
Smart Card detection	Movement detection with auto power-off; Automatic detection of smart card type; Short circuit and thermal protection
8-Pin Handling	C4 / C8 supported
	HOST INTERFACE
USB Interface	USB 2.0 Full Speed Device (12 MBps) USB 3.0 extended operability, tested with hubs/controllers
Connector / Cable	USB Type A connector; 59.1" (150 cm) cable
Operating Systems	Windows 10/8.1/8/7/Vista/Server 2012/Server 2008R2 Windows CE (5/6/7) depending on hardware Linux Debian 6.0+ / Ubuntu 11.04+/ Fedora 15+; Open SUSE 11.4+ Mac OS X; AndroidTM
Driver	CCID native driver from operating system
Supported APIs	PC/SC - API
	HUMAN INTERFACE
Status indicator	Dual-color LED (green & red)
	HOUSING
Housing	Two-tone grey, ABS plastics
Dimensions	3.15" x 2.64" x 1.1" (80 x 67 x 28 mm)
Weight	Reader only 3.88 oz (110g); Standard standing base 1.09 oz (31g)
	OPERATING CONDITIONS
Operating Temperature	32-131 F (0-55°C)
Operating Humidity	10-90% rH
Storage Temperature	-4 - 176 F (-20 - 80°C)
Meantime Between Failure (MTBF)	500.000 hours
	COMPLIANCE AND REGULATORY
Compliance / Certification	EMVCo Level 1 USB 2.0; TAA; GSA Fips 201 approved list
Regional certifications	CE, FCC, UL, VCCI, KCC, MIC, RCM (C-Tick)
Environmental	WEEE, RoHS, Reach
	OPERATING CONDITIONS
Warranty	Two-year manufacturer`s warranty
	OPTIONS
Part Numbers	R31210320-01 (Standard); R31210349-1 (TAA, ROM); R31210399 (TAA, Flash)

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 55 9171 1108

For more information, click here

2021-02-22-omnikey-3121-usb-desktop-reader-ds-en PLT-00318

Part of ASSA ABLOY

611 Center Ride Drive
Austin TX, 78753 USA

Declaration of Conformity (DoC)

We, HID Global Corporation located at 611 Center Ride Drive, Austin TX, 78753 USA, declare under our sole responsibility that the product(s) described in the tables are in conformity with the *essential requirements* and *other relevant reqirements* of the following Directives:

Electromagnetic Compatibility (EMC) Directive: 2004/108/EC
Low voltage (LVD) Directive: 2006/95/EC
RoHS Recast (RoHS2) Directive: 2011/65/EU

and applicable parts of

Product / Device Information:

Product Type:	Logical Access Reader
Trade Name(s):	OMNIKEY Smart Card Reader
Further Description: *(only where required)*	OMNIKEY Reader
Model Number(s):	3121

The following harmonized standards and/or other normative documents were applied in full to show conformity to the Directives:

Product Specifications	Standard(s) Applied in Full
Safety	EN 60950-1:2006/ A11:2009 +A1:2010 +A12:2011
EMC	EN 55024:2010, EN 50130-4:2011
Spectrum	EN 55022:2010 +AC:2011 (Class A)
RoHS2	EN 50581:2012

Supplementary Information:

Testing Organization Involved:	TÜV Austria 1230 Vienna, Austria

Technical/Compliance File Held by:	HID Global Corporation (Compliance Engineering Department) 10385 Westmoor Drive, Suite 300, Westminster, CO 80021 USA
Place and Date of Issuance:	Westminster, CO USA on October 8, 2009

Signature of Authorized Person: Robert A Cresswell

May 31, 2016

Robert Cresswell: Manager – Global Product Compliance

Date of Signature:

Phone/303-404-6700
Fax/ 303.404.6840
Web/ www.hidcorp.com

AirID 2 BUSINESS

AirID 2 Business is a wireless, flexible smartcard reader and FIDO security key (authenticator) in one compact and lightweight device.

As a smartcard reader, the AirID 2 connects exchangeable smartcards in ID1 format (credit cards) via Bluetooth, NFC and USB to smartphones, tablets, laptops or stationary systems.

As FIDO Authenticator, FIDO U2F and FIDO2 authentications can additionally and simultaneously be performed via Bluetooth or USB.

Smartcard and FIDO can be used simultaneously, even on different devices.

fido ALLIANCE MEMBER SINCE 2014

Bluetooth

WORLD'S LEADING COMPANIES AND AUTHORITIES TRUST WIRELESS SECURITY THROUGH AirID

Prevent account hijacking and Man-in-the-Middle Attacks

Every computer is vulnerable to attacks from the outside. Malware, Trojans and malicious software can spy out passwords, digital keys and other access data. The AirID 2 Business stores these keys and data either on the smartcard used or securely on an integrated chip - separate from the computer - and so the keys cannot be stolen.

Average costs of 3.5 million € for one breach of data privacy and security

In the globally recognized report by the Ponemon Institute*, 524 companies with data privacy breaches were investigated in 2020. The average damage per case was estimated at USD 3.86 million (= €3.5 million). These costs arise from technical investigations, mandatory information to customers & the public, lost business and expenses in the follow-up of the incident. In another study by FireEye**, 75% of respondents said they would no longer use services from companies with data breaches.

WHY AIRID 2 BUSINESS?

- Independent through Bluetooth connections
- Only one device for smartcard and FIDO login
- Flexible due to ID1 smart card slot
- Future-proof through Bluetooth version 5
- Integrated distance logout for smartcard
- Easy operation & long battery life
- Compact & light at 46 grams

Do you use your own individual smartcards? The AirID 2 supports e.g. CAC, CardOS, JAVA, PIV, StarCOS, TCOS cards and is compatible with virtually any smartcard.

AirID 2 Business with FIDO2 is supported by Microsoft, OKTA, PING Identity and many others

Protect your computer, accesses, network and data instantly and without much effort. The AirID 2 with FIDO2 is supported by virtually all leading manufacturers and can be configured and rolled out in minutes.

GO PASSWORDLESS with Smartcards & FIDO2

With AirID 2 you have the choice. Simply use your smartcards as before and at the same time you have the option to react flexibly to new challenges with FIDO security keys.

This way you can also reduce your IT costs in the area of IT help desk and password reset. According to research by the GARTNER Group, about 30-50% of IT help desk costs are related to password problems and their resolution.

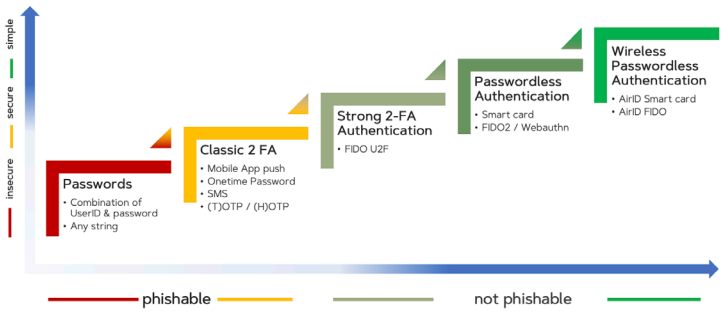


Illustration of the different authentication methods in terms of security and usability (c) certgate

Future-proof due to integrated FIDO Standard

FIDO (Fast IDentification Online) is a worldwide Alliance (www.fidoalliance.com) which is supported by practically all leading IT manufacturers and service providers. certgate has been a member of the FIDO Alliance for years. With AirID FIDO you already have the new worldwide standard in your pocket with FIDO2. Due to the automatic update capability, you can be sure that the AirID 2 Business will grow with your future requirements.

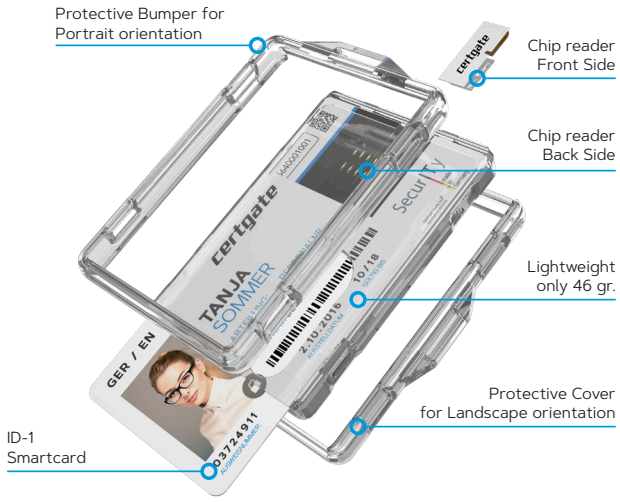
* https://www.ibm.com/account/reg/us-en/signup?formid=urx-46542
** https://www2.fireeye.com/rs/848-DID-242/images/rpt-beyond-bottomline.pdf

TECHNICAL SPECIFICATION

- **Smartcard Reader Support:**
  - Contact interface (ISO7816) for ID-1 cards (credit card format)
  - Supported smart card protocol: T=1, T=0 Voltage: 3V
  - Chip reader for card back- & front side
  - Compatible with portrait & landscape cards
- **FIDO Authenticator Support:**
  - Storage for upto 200 FIDO keys
  - „Driverless" FIDO support on Win10
  - FIDO U2F* & FIDO2 via Bluetooth LE
  - FIDO U2F & FIDO2 via USB*
- **Secure Bluetooth Low Energy Connection**
  - Secure Pairing for secure, encrypted Bluetooth LE™ connections
  - Additional AES256 encrypted communication for smart card functions
  - Protected against Man-in-the-Middle Attacks
- **Platform Support**
  - Smart card: Windows10 (min V1909), macOS (min. 10.15.7) , Linux (on request), iOS (min. V13), Android (min. V9)
  - FIDO: Windows10 (BLE & USB*), macOS (USB*, BLE in Vorbereitung)
- **Future-Proof by Firmware-Updates**
  - Fully updateable & expandable
  - Automated software updates through Online software distribution service
  - Secure, encrypted updates
- **Display and LED-indicator**
  - Low Power Display for Infos & Menu
  - Multi-color LEDs for battery charge status, power supply and activity
- **Easy to use:**
  - Simple menu via JOG-Dial
  - Individual settings
  - AirID Night Mode for optimised battery live
- **Power Supply**
  - Rechargable battery
  - Battery charge shown in display
  - LED indicator while charging

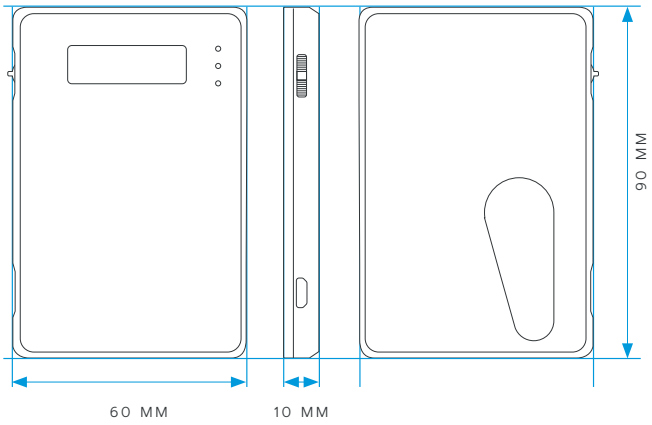
* by firmware version V2.2, est. availability July 2021

NOTE: Some functions and features are only available on selected platforms and interfaces. For example, FIDO via BLE is currently only supported by Windows10. Future platforms and interfaces are under development and will be made available automatically via the AirID update service. Your AirID is future-proof and will grow with you.



DIMENSIONS & WEIGHT

Packaging: W94 x H44 x L107 mm / 140 gr. incl. accessory (46 gr. only AirID)



SOFTWARE, DOWNLOADS & FAQ

In our Online Service & Support area we always provide the most actual documentation and software for an easy and fast installation.

www.AirID.com/support

PATENTED AIRID TECHNOLOGY

With the patented wireless technology of the AirID (Patent No.: DE102013112943A1), you are at the cutting edge of state of the art and therefore well equipped for modern requirements for your IT.

SecurITy made in Germany

certgate GmbH
Kaiserswerther Straße 45
40477 Düsseldorf
Germany

Phone: + 49 (0) 911 93 523-0
E-Mail: info@certgate.com
Web: www.AirID.com

AirID 2 GOVERNMENT

AirID 2 Mini Government is a wireless, flexible smartcard reader and FIDO security key (authenticator) in a compact and lightweight form factor.

A special firmware version allows authorities to communicate securely up to classification VS-NfD when used as a smartcard reader and SecurePIM.

As FIDO Authenticator, FIDO U2F and FIDO2 authentications can additionally and simultaneously be performed via Bluetooth or USB.

The AirID2 is approved by the German Federal Office for Information Security (BSI) as a smartcard reader for VS-NfD environments when used with TCOS & SecurePIM.

AirID

fido ALLIANCE MEMBER SINCE 2014

VS-NfD
Im Einsatz mit Secure PIM

Bluetooth

LEADING AUTHORITIES TRUST WIRELESS SECURITY THROUGH AirID

Prevent account hijacking and Man-in-the-Middle Attacks

Every computer is vulnerable to attacks from the outside. Malware, Trojans and malicious software can spy out passwords, digital keys and other access data. The AirID 2 Government stores these keys and data either on the smartcard used or securely on an integrated chip - separate from the computer - and so the keys cannot be stolen.

Average costs of 3.5 million € for one breach of data privacy and security

In the globally recognized report by the Ponemon Institute**, 524 companies with data privacy breaches were investigated in 2020. The average damage per case was estimated at USD 3.86 million (= €3.5 million). These costs arise from technical investigations, mandatory information to customers & the public, lost business and expenses in the follow-up of the incident. In another study by FireEye***, 75% of respondents said they would no longer use services from companies with data breaches.

WHY AIRID 2 GOVERNMENT?

- Independent through Bluetooth connections
- Only one device for smartcard and FIDO login
- Approved by BSI for classified information*
- Future-proof through Bluetooth version 5
- Integrated distance logout for smartcard
- Easy operation & long battery life
- Compact & light at 46 grams

Do you use your own individual smartcards? The AirID 2 supports e.g. CAC, CardOS, JAVA, PIV, StarCOS, TCOS cards and is compatible with virtually any smartcard.

* When used with SecurePIM and TCOS smart card
** https://www.ibm.com/account/reg/us-en/signup?formid=urx-46542
*** https://www2.fireeye.com/rs/848-DID-242/images/rpt-beyond-bottomline.pdf

AirID 2 Government with FIDO2 is supported by Microsoft, OKTA, PING Identity and many others

Protect your computer, accesses, network and data instantly and without much effort. The AirID 2 with FIDO2 is supported by virtually all leading manufacturers and can be configured and rolled out in minutes.

GO PASSWORDLESS with Smartcards & FIDO2

With AirID 2 you have the choice. Simply use your smartcards as before and at the same time you have the option to react flexibly to new challenges with FIDO security keys.

This way you can also reduce your IT costs in the area of IT help desk and password reset. According to research by the GARTNER Group, about 30-50% of IT help desk costs are related to password problems and their resolution.

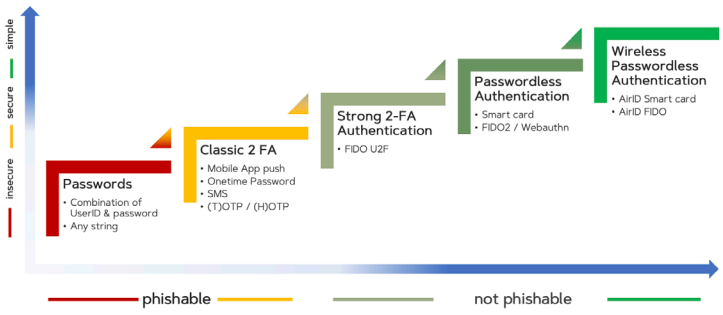


Illustration of the different authentication methods in terms of security and usability (c) certgate

Future-proof due to integrated FIDO Standard

FIDO (Fast IDentification Online) is a worldwide Alliance (www.fidoalliance.com) which is supported by practically all leading IT manufacturers and service providers. certgate has been a member of the FIDO Alliance for years. With AirID FIDO you already have the new worldwide standard in your pocket with FIDO2. Due to the automatic update capability, you can be sure that the AirID 2 Business will grow with your future requirements.

TECHNICAL SPECIFICATION

- **Smartcard Reader Support:**
  - Contact interface (ISO7816) for ID-1 cards (credit card format)
  - Supported smart card protocol: T=1, T=0 Voltage: 3V
  - Chip reader for card back- & front side
  - Compatible with portrait & landscape cards
- **FIDO Authenticator Support:**
  - Storage for upto 200 FIDO keys
  - „Driverless" FIDO support on Win10
  - FIDO U2F* & FIDO2 via Bluetooth LE
  - FIDO U2F & FIDO2 via USB*
- **Secure Bluetooth Low Energy Connection**
  - Secure Pairing for secure, encrypted Bluetooth LE™ connections
  - Additional AES256 encrypted communication for smart card functions
  - Protected against Man-in-the-Middle Attacks
- **Platform Support**
  - Smart card: Windows10 (min V1909), macOS (min. 10.15.7) , Linux (on request), iOS (min. V13), Android (min. V9)
  - FIDO: Windows10 (BLE & USB*), macOS (USB*, BLE in Vorbereitung)
- **Future-Proof by Firmware-Updates**
  - Fully updateable & expandable
  - Automated software updates through Online software distribution service
  - Secure, encrypted updates
- **Display and LED-indicator**
  - Low Power Display for Infos & Menu
  - Multi-color LEDs for battery charge status, power supply and activity
- **Easy to use:**
  - Simple menu via JOG-Dial
  - Individual settings
  - AirID Night Mode for optimised battery live
- **Power Supply**
  - Rechargable battery
  - Battery charge shown in display
  - LED indicator while charging

* by firmware version V2.2-GOV, est. availability July 2021

NOTE: Some functions and features are only available on selected platforms and interfaces. For example, FIDO via BLE is currently only supported by Windows10. Future platforms and interfaces are under development and will be made available automatically via the AirID update service. Your AirID is future-proof and will grow with you.

OPTIONAL: INCL. TCOS SMART CARD

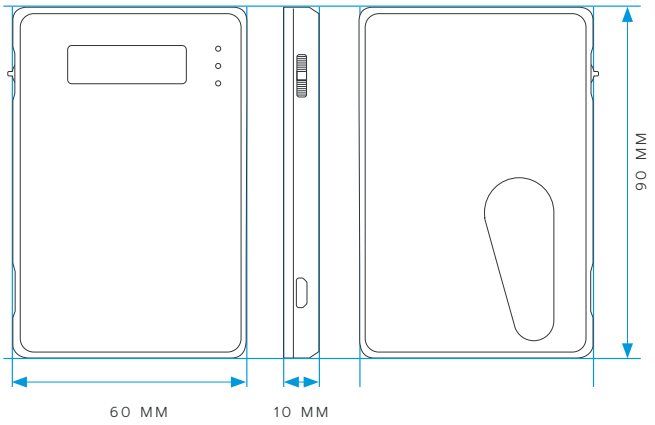
TCOS 3.0 Signature Card V2.0

- Smartcard OS: TCOS 3.0 Signature Card V2.0 Release 1, instruction set according to ISO 7816, CC EAL 4+
- Chip: Infineon SLE78CLX1440P, CC EAL5+ certified
- Cryptography: ECDSA with 256 Bit, Decryption: According to CEN-14890, Part 2 based on Elliptic Curves (NIST P-256), ECDH with 256 Bit, NIST P-256 (for Windows-LogOn), PACE according to TR-03110
- Random generator: hardware-based, P2 classification (SOF „high") acc. to AIS-31

TCOS smartcard must be specified when ordering AirID 2, otherwise delivery will be provided without smartcard.

DIMENSIONS & WEIGHT

Packaging: W94 x H44 x L107 mm / 140 gr. incl. accessory (46 gr. only AirID)



SOFTWARE, DOWNLOADS & FAQ

In our Online Service & Support area we always provide the most actual documentation and software for an easy and fast installation.

www.AirID.com/support

PATENTED AIRID TECHNOLOGY

With the patented wireless technology of the AirID (Patent No.: DE102013112943A1), you are at the cutting edge of state of the art and therefore well equipped for modern requirements for your IT.

SecurITy made in Germany

certgate GmbH
Kaiserswerther Straße 45
40477 Düsseldorf
Germany

Phone: + 49 (0) 911 93 523-0
E-Mail: info@certgate.com
Web: www.AirID.com

thalescpl.com

THALES

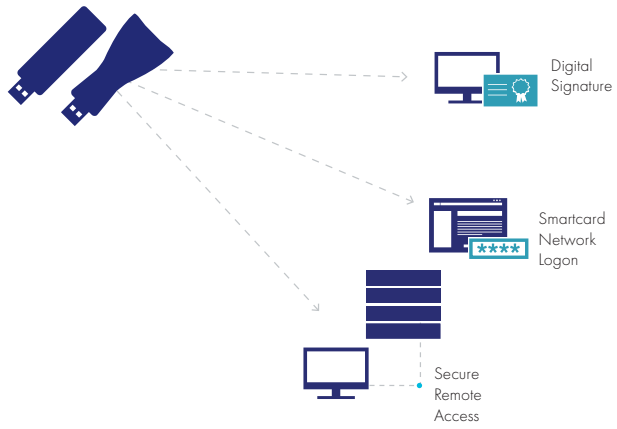
SafeNet Authentication Client

The Power to Easily Manage Thales's PKI-based Authentication

SafeNet Authentication Client is a unified middleware client that manages Thales's extensive SafeNet portfolio of Identity and Access Management Solutions, including certificate-based authenticators such as eToken, IDPrime smart cards, USB and software-based devices. Offering full backward compatibility and incorporating features from previous middleware versions, SafeNet Authentication Client ensures complete support for all currently deployed eToken devices, as well as IDPrime smart cards.

SafeNet Authentication Client links applications to Thales's PKI authenticators, providing full local administration and support for multiple advanced security applications such as digital signing, pre-boot authentication and disk encryption. With SafeNet Authentication Client, private keys can be generated and stored on-board highly secure smart card-based authenticators allowing users to securely carry all their digital credentials wherever they go.

Leverage your PKI Solution for multiple



Use Cases

Benefits

- Transparently operates with any standard certificate-based security application
- Consolidated & simplified management tools allow users to manage their own cards/tokens and certificates
- Supports secure access, data encryption and digital signing—all with a single authenticator

- Streamlines security operations by allowing organizations to deploy multiple security applications on a single platform
- Allows organizations to use certificate-enabled security capabilities from any client or server thanks to multi-platform support

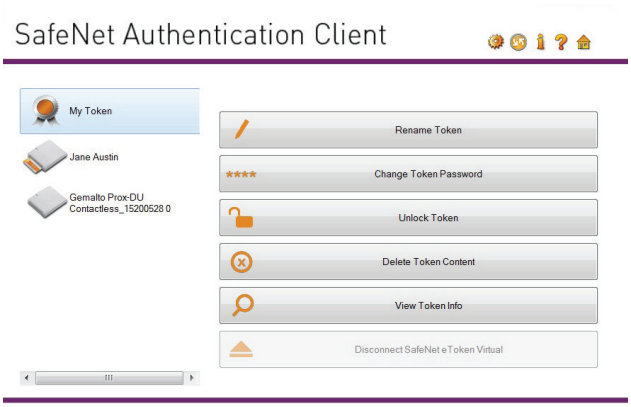
Features

- Strong two-factor authentication for network and data protection
- Support for Common Criteria and FIPS certified devices
- Full support for SN IDPrime smart cards, including Multi-slots support and PIN Quality modifications
- Support for PIN Pad Readers
- Support for See What You Sign (SWYS) PIN Pad readers with IDPrime MD smart cards
- Enables local administration and usage of devices
- Support for full client customization, including security configuration, policies and user interface
- Seamless integration with any certificate-enabled application based on industry standard APIs
- Enables enhanced password management applications for protecting PCs and securing on-site local network access, using SafeNet Network Logon or Thales IDGo Credential Provider
- Support for Virtual Keyboard enables you to enter passwords without using a physical keyboard, providing protection against kernel level keyloggers
- Common look and feel across all platforms

A Unified Solution for All Users

SafeNet Authentication Client is available for Windows, Mac, and Linux, so your organization can take full advantage of SafeNet's solutions ranging from identity and access management, certificate-based security, strong authentication, encryption and digital signing, from virtually any device.

SAC management tools reduce helpdesk costs by allowing users to maintain their own cards/tokens and certificates



Technical Specifications

Supported operating systems

- Windows Server 2008 R2 SP1 (32-bit, 64-bit)
- Windows Server 2008 SP2 (32-bit, 64-bit)
- Windows Server 2012 and 2012 R2 (64-bit)
- Windows Server 2016 (64-bit)
- Windows 7 SP1 (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit)
- Windows 10 (32-bit, 64-bit)
- MAC OS X 10.13.1 and 10.14
- Linux Distributions: Ubuntu 18.04.2 LTS and 19.04, CentOS 7.6 (and 6.10), Red Hat 8 (and 7.6), SUSE Linux enterprise desktop 15, Fedora 30, Debian

Supported APIs

- PKCS#11 V2.20, MS CryptoAPI and CNG (CSP, KSP), Mac Keychain (TokenD), PC/SC

Supported cryptographic algorithms

- 3DES, SHA-256, RSA up to 2048-bit, Elliptic Curve Cryptography (ECC)

Supported CAs

- Microsoft, Entrust, VeriSign

Supported Browsers

- Firefox
- Internet Explorer
- Microsoft Edge (does not support certificate enrollment)
- Chrome (does not support certificate enrollment)

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

* For a full list of backward compatible supported authenticators, please refer to the latest customer release notes.

> thalescpl.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com

MyID | Enterprise

MyID Enterprise is a flexible software solution for large organisations and governments that enables the deployment and management of PKI based digital identities to a wide range of secure devices.

MyID Enterprise delivers the integration, flexibility and scalability necessary for governments and large enterprises to run two-factor authentication and national identity schemes for thousands of employees through to millions of citizens.

Now featuring strong authentication for mobile, the new MyID Enterprise authenticator app turns end users' mobile devices into crypto-protected keys, enabling passwordless multi-factor authentication for end users into cloud resources, corporate systems and networks through touch ID, facial biometric or a PIN.

MyID Enterprise is for

- Large enterprises who want to protect their networks, systems and cloud-based resources with the most secure method of employee authentication
- Governments who wish to deploy PKI-based digital identities to citizens
- Governments who wish to digitally transform their citizen service delivery by embracing mobile
- Organisations wishing to deploy user credentials to a wide range of devices including smart cards, USB tokens, virtual smart cards and mobile devices
- Organisations who want an easy to use solution for IT to issue and lifecycle manage user credentials, from thousands to millions of end users
- Organisations who need a system flexible enough to adapt to existing business processes and integrate with existing infrastructure
- Organisations who want to deliver passwordless two-factor authentication for end users, across the technology they want to use

Software that simplifies issuing and managing credentials at scale

1.

Use MyID Enterprise to

- Issue cryptographically protected digital identities to individuals using public key infrastructure (PKI) to smart cards, USB tokens, smartphones and virtual smart card enabled technology
- Configure certificate and device issuance policies, ensuring the right people receive the right digital identities
- Issue credentials via face-to-face, centrally or via self-service
- Provide high levels of user service, with simple process-driven features for help desks to issue replacement devices upon loss, or re-enable locked devices
- Maintain full auditability and reporting – allowing visibility of who issued which digital identities to which users and on what device, helping with external audits and compliance with identity management guidelines
- Enable strong authentication for end users via their mobile device without the need for additional hardware or server software

Benefits of MyID Enterprise

Step up to the highest levels of security

Replace passwords with strong two-factor authentication, providing the most effective protection against the number one cause of data breach - weak or compromised user credentials

Simple to use

Shaped around ease of use both for operators and end users, MyID Enterprise guides users through processes, reducing day to day operational costs and ensuring high levels of user adoption

Integration flexibility

MyID Enterprise is developed to work with what you already have and support your existing business processes, minimising impact on your existing environment and speeding up deployment

Software enriched by >20 years' experience

Benefit from more than 20 years of software development, shaped by the governments and large enterprises who trust MyID Enterprise to help them issue and manage digital identities to their millions of citizens and employees for simple, secure access to the information they need

Technology Independent

Issue and lifecycle manage credentials across the devices you want to use. Mobile devices, USB tokens, virtual smart cards, and smart card devices are all supported by MyID Enterprise

Mobile Authentication as standard

With MyID Enterprise's authenticator app turn your end users' mobile device into a PKI credential and enable passwordless multi-factor authentication into cloud resources, corporate systems and networks through touch ID, face ID or PIN.

MyID Enterprise includes

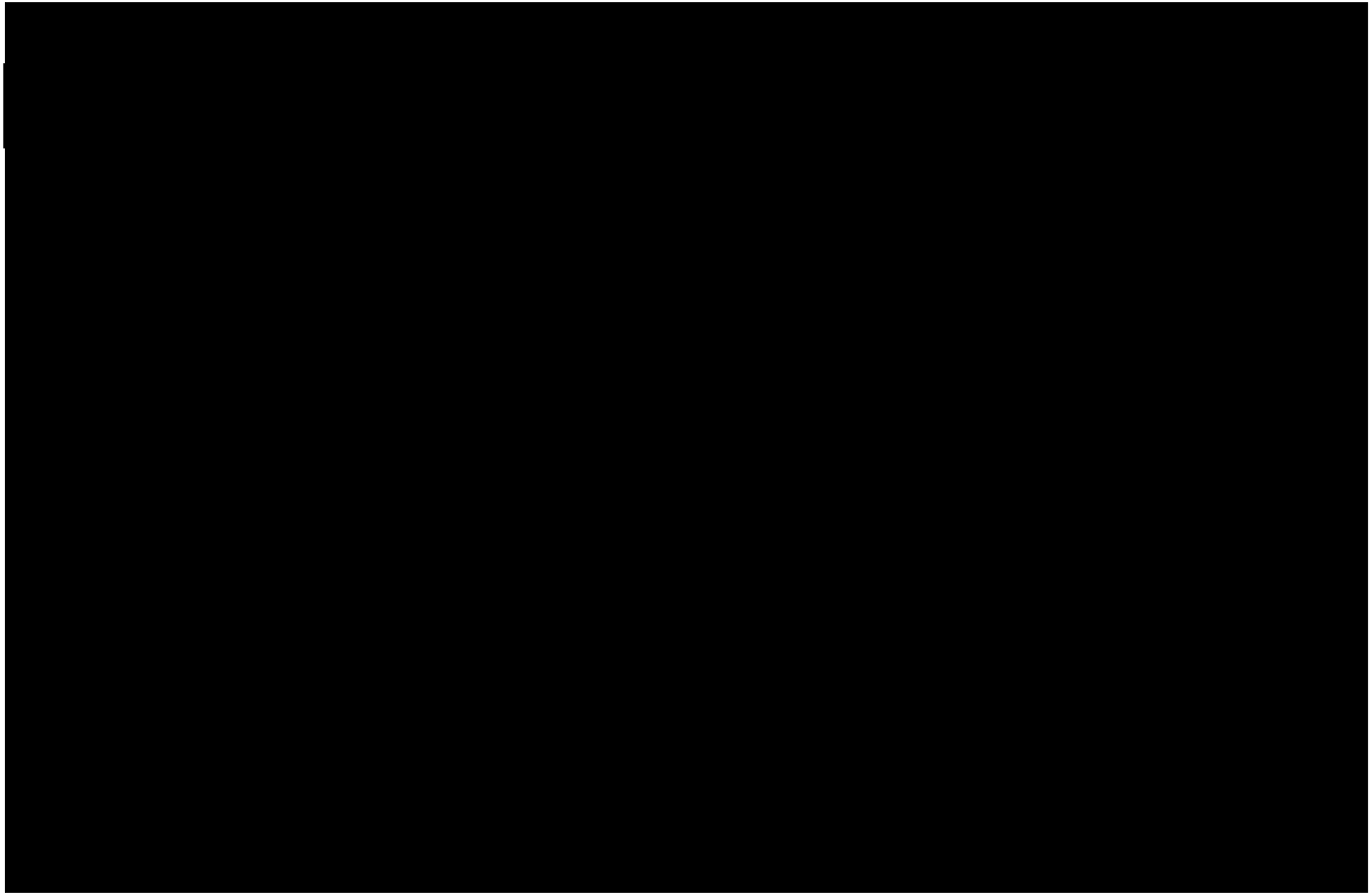
- Software including connectors to directories, PKI, hardware security modules, smart cards, USB tokens, virtual smart cards, smart card printers and mobile devices
- Operator desktop for administration and management
- End user self-service kiosk and client application
- APIs and SDKs for integration and customisation
- Configurable credential management policies
- Mobile authentication for end users into cloud resources, corporate systems and networks using MyID's Authenticator app

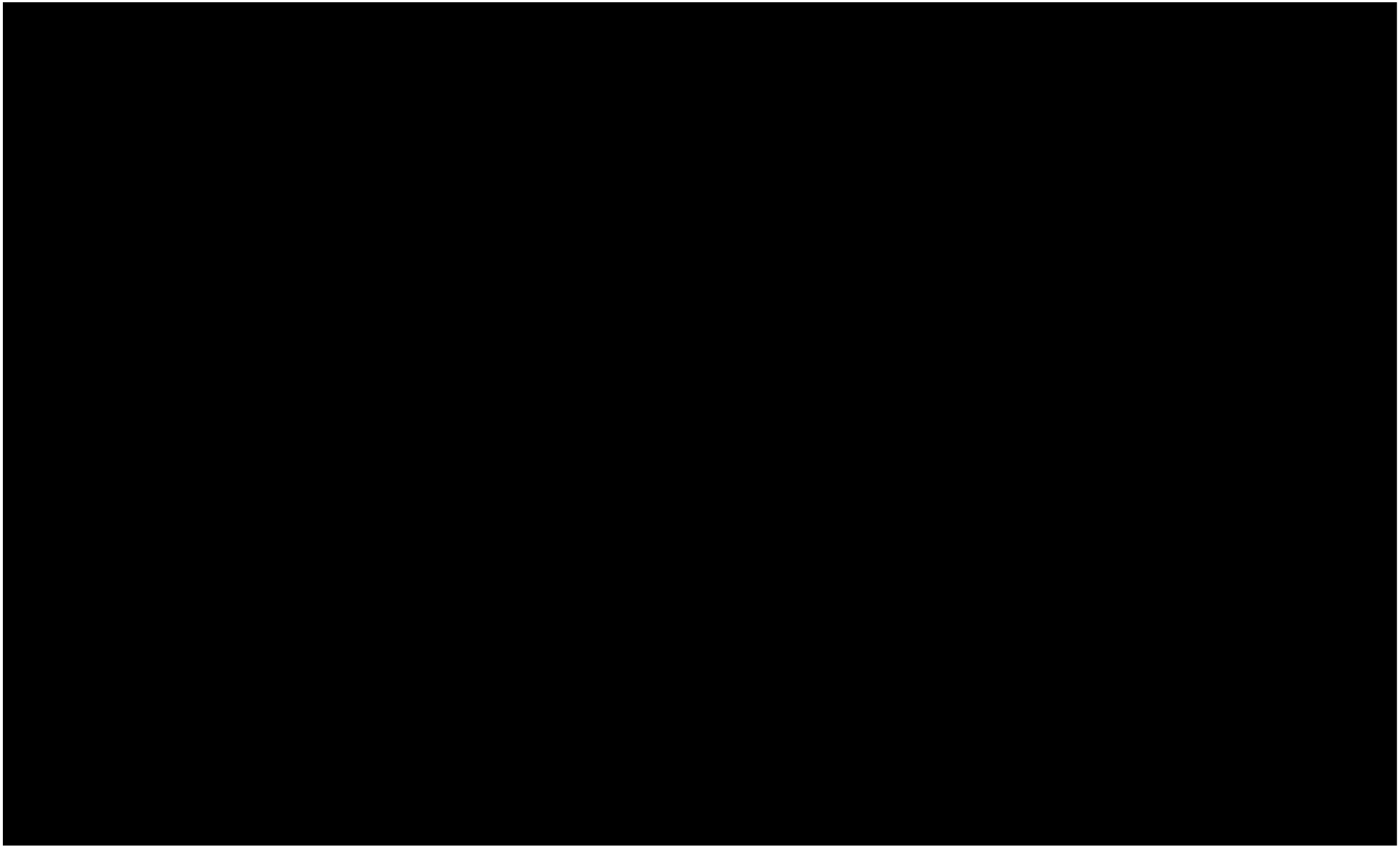
MyID Enterprise works with

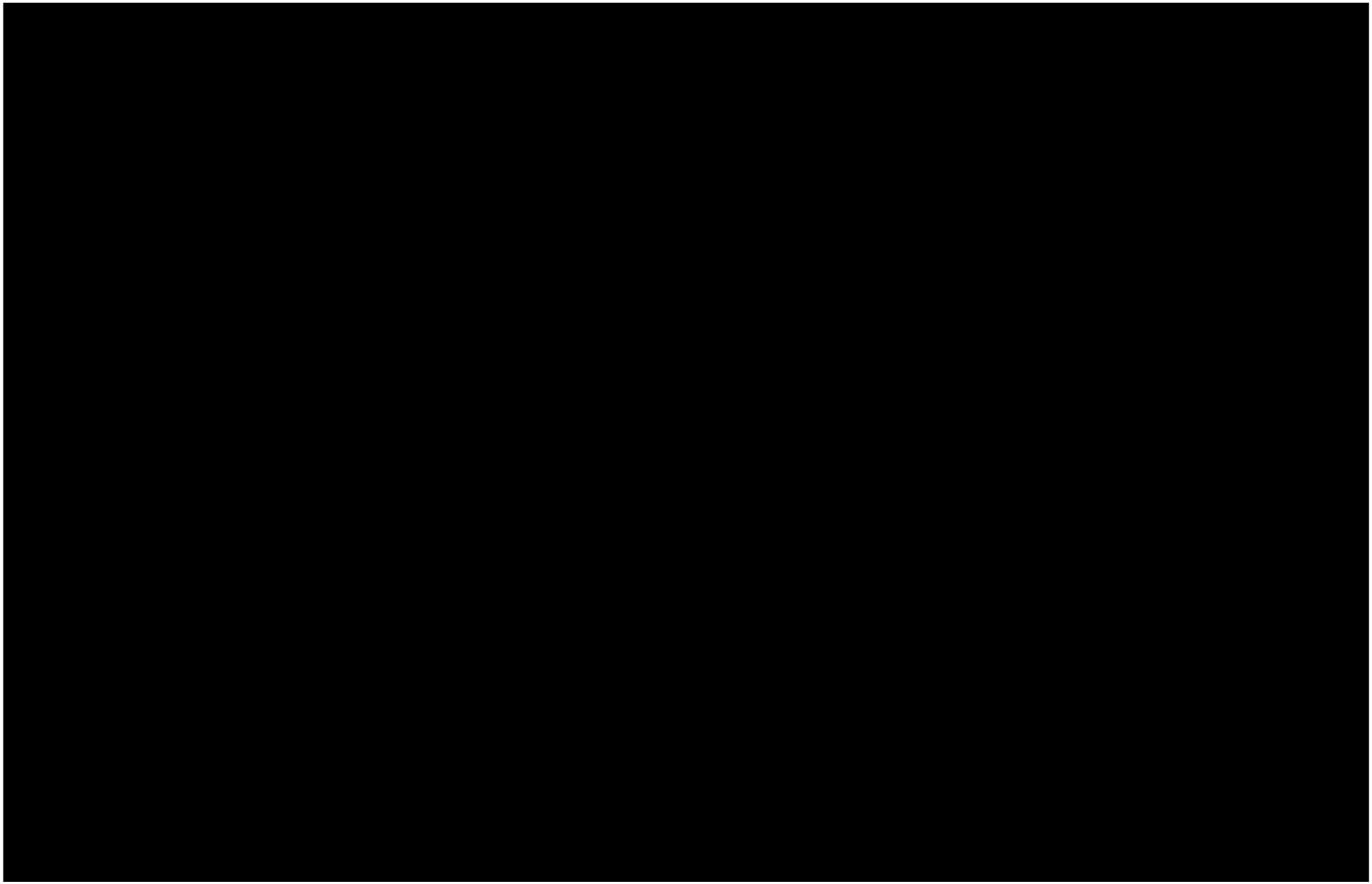
Technology	Vendor	Product
Smart Cards	NXP	Athena IDProtect
	Gemalto	ID Prime smart card ID Prime PIV smart card
	Giesecke & Devrient	SmartCafe Expert SCE PIV card
	Idemia	ID-One Cosmo ID-One PIV
	Thales Trusted Cyber Technologies	TCT SC650
	T-Systems	TCOS smart card
	Cryptas	TicTok
Mobile Device Management	VMware	AirWatch Workspace ONE
	Citrix	XenMobile (Endpoint Management)
	MobileIron	MobileIron Core
	Centrify	Identity Service
	Microsoft	Intune
USB Tokens	Yubico	Yubikey Yubikey FIPS
	Thales Trusted Cyber Technologies	TCT eToken TCT eToken FIPS
Certificate Authorities	DigiCert	Symantec MPKI
	Entrust Datacard	Entrust Authority PKI
	HID Global	Indentrust PKI
	Microsoft	Certificate Services
	PrimeKey	EJBCA
	Verizon	UniCERT
Virtual Smart Cards	Intel	Intel Authenticate
	Microsoft	TPM Virtual Smart Card Windows Hello for Business
	Cryptas	Cryptas VSC
Hardware Security Modules	Thales Trusted Cyber Technologies	TCT Luna Network HSM
	nCipher	nShield HSM
	Thales Trusted Cyber Technologies	TCT Luna SA for Government
	Thales Trusted Cyber Technologies	T-Series HSMs
Image Capture	Webcam	Webcams supporting video for windows
	Document Scanners	Scanners supporting WIA2 integration
Identity Provider	Microsoft	Active Directory Federation Services (ADFS)
Mobile OS	Apple	iOS
	Google	Android

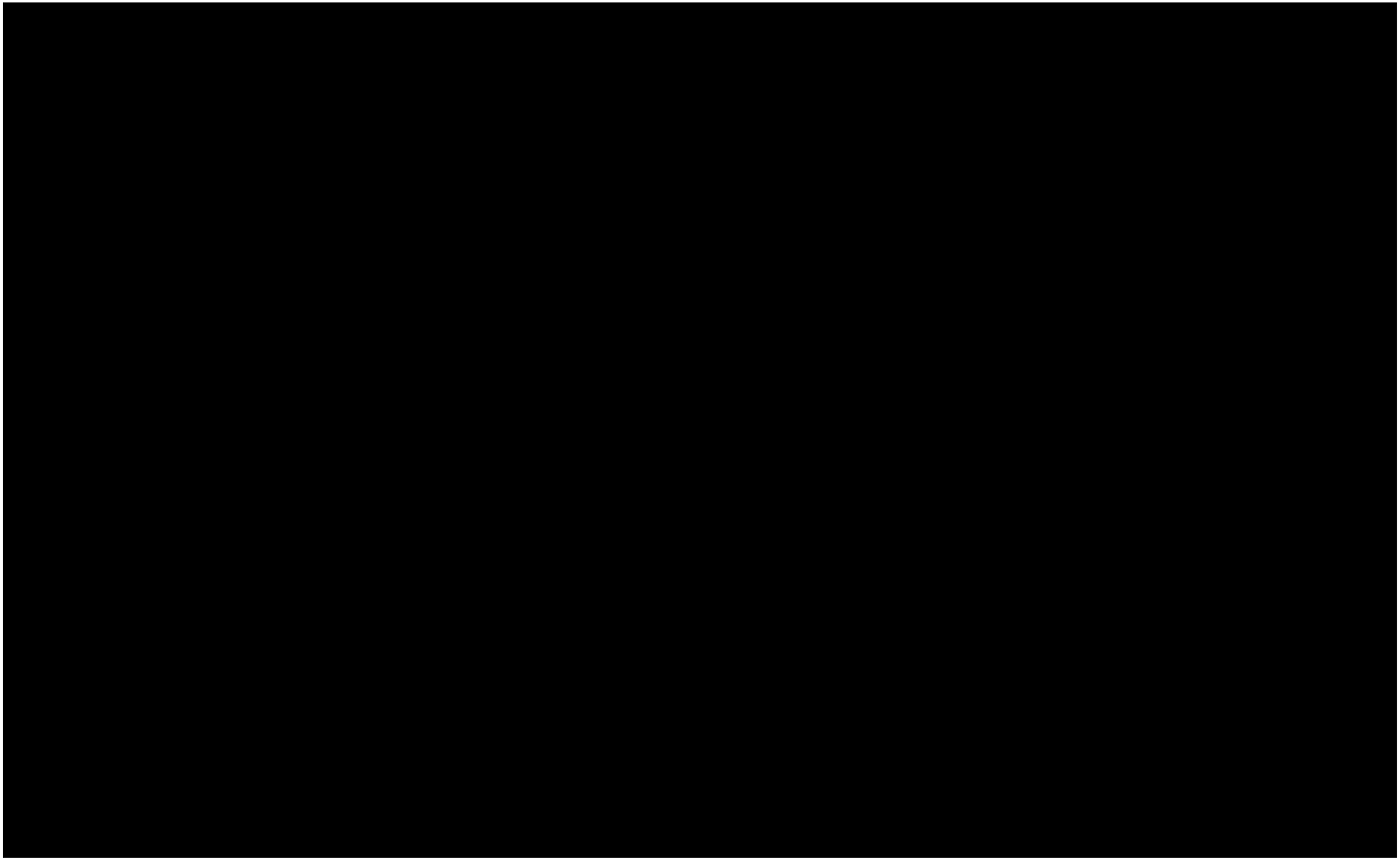
Příloha č. 2

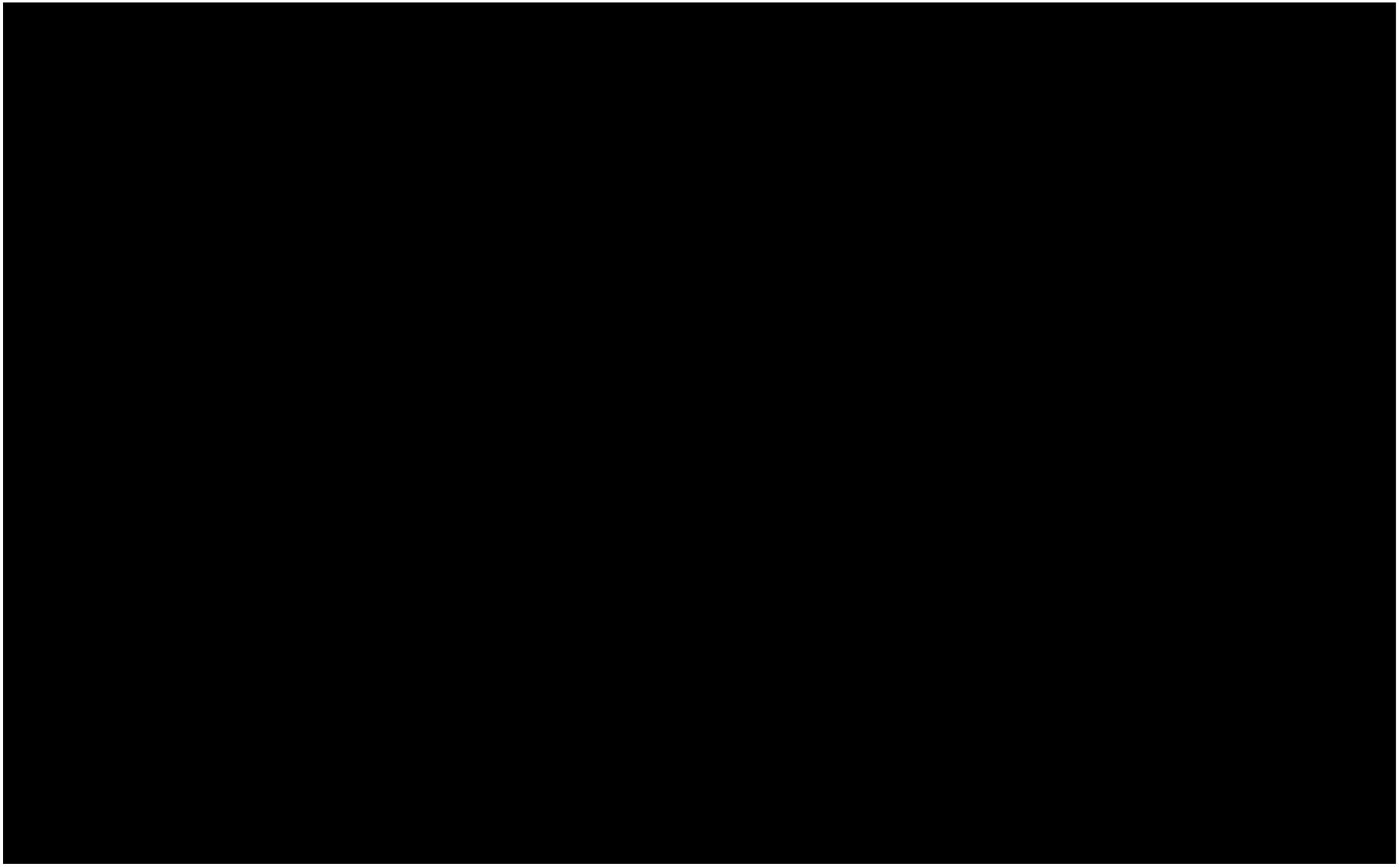
Příloha č. 3

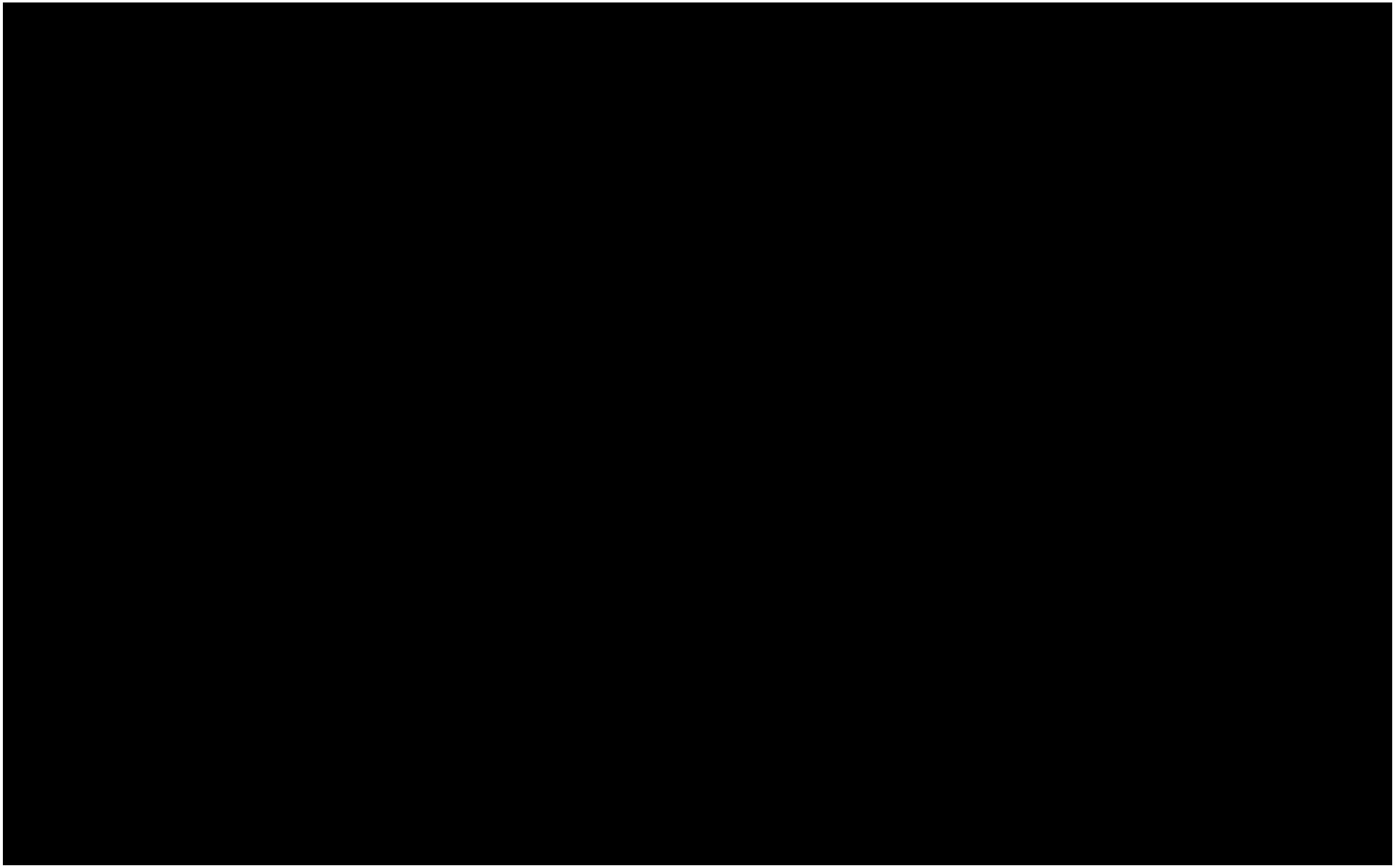


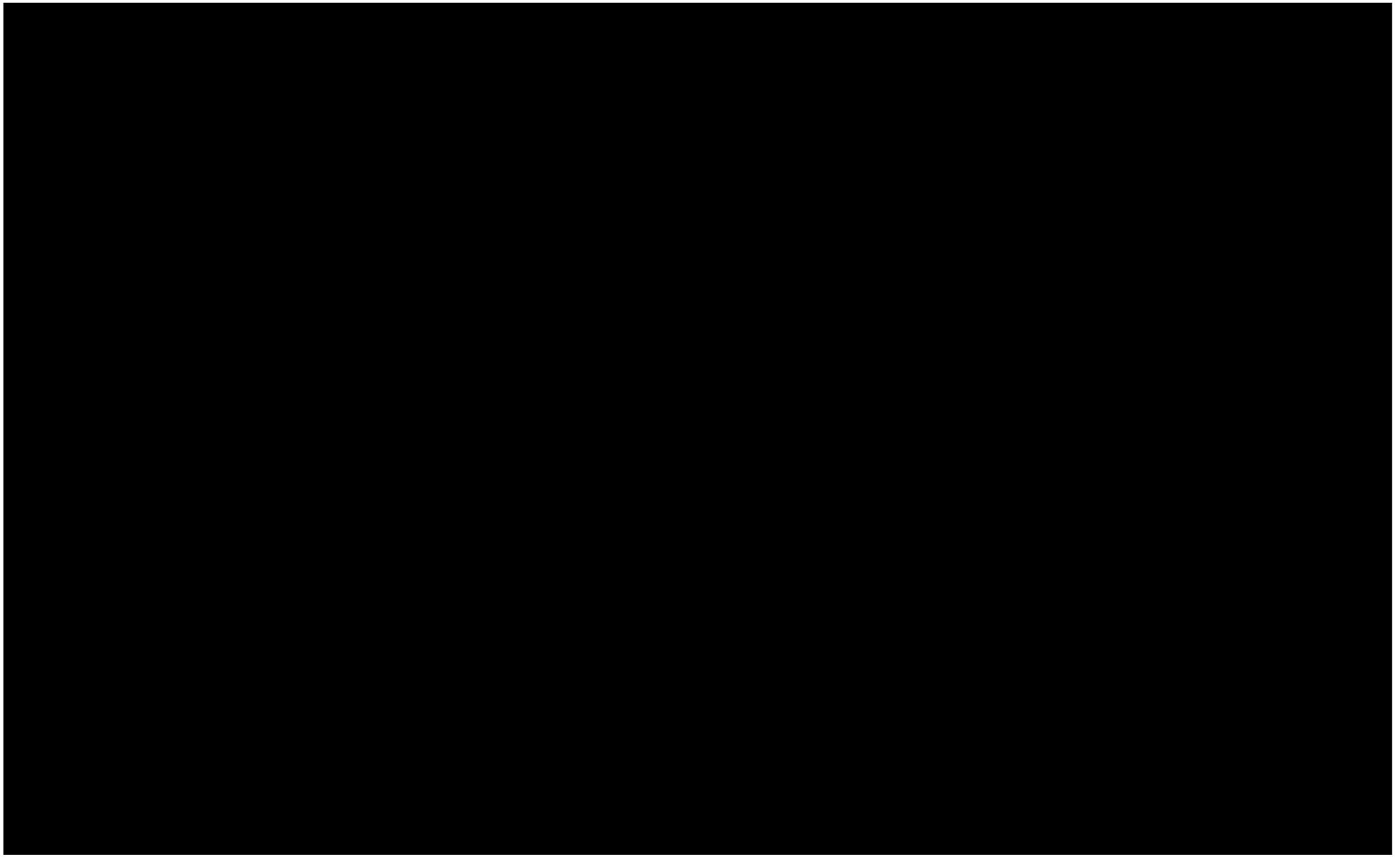












Příloha č. 4

Technické podmínky předmětu plnění

1. **Striktně vyžadované funkce a vlastnosti**:

V následující tabulce jsou uvedeny požadavky, které musí být zhotovitelem ve finálním Řešení splněny. U jednoho „požadavku“ (=řádku tabulky) může být současně i několik požadovaných vlastností (viz např. požadavek „spolehlivost“), které musí být splněny všechny.

Použité výrazy jsou poplatné obecné terminologii a nejrozšířenějším technologiím. V některých místech se však mohou lišit od technologie nabízené zhotovitelem (vše není možné popsat zcela obecně). V tom případě musí zhotovitel jasně vysvětlit vzájemný vztah nabídnutého řešení a požadavku objednatele a zdůvodnit způsob splnění požadavku. Rozhodující je splnění příslušné funkce nebo vlastnosti po její funkční/výkonové stránce nikoliv způsob jakým je výsledku dosaženo.

1.1 Požadavky na SCK

Požadavek	Popis	Poznámka/zdůvodnění
Konfigurace a provoz SCK	Musí být vytvořena provozní konfigurace SCK a přenos stávajících nastavení tak, aby současní uživatelé mohli s čipovou kartou pracovat jako v současnosti a se stávajícími klíči a certifikáty. Musí být realizován ostrý přechodu na podporované operační systémy a SW.	
Dostupnost	Řešení musí být odolné proti výpadku. Jednotlivé komponenty musí být zdvojené, nesmí existovat tzv. „Single Point of Failure“.	Pro potřeby ČNB je důležitá spolehlivost a bezvýpadkovost systému jako celku.
Spolehlivost	Je vyžadováno: - zajištění provozu 12x5 včetně garance dostupnosti dat na úrovni operačního systému serveru alespoň v jedné lokalitě v pracovních dnech do 24 hodin. V tomto případě není rozhodující, zda se jedná o chybu HW nebo SW; - výměna libovolné jedné vadné komponenty za provozu (bez přerušení přístupu k datům, výkonnost může být částečně snížena); - SCK cluster nesmí mít SPOF (Single Point of Failure);	Vysoká spolehlivost provozu je součástí zajištění dostupnosti dat. V noci probíhá dávkové zpracování v délce několika hodin. Případné odstávky při výměně vadných komponent, upgrade FW/mikrokódu nebo konfigurační změny mající dopad na provoz systému jsou v ČNB organizačně náročné.

	- konfigurační změny online (viz dále); - zajištění podpory výrobce zařízení tak, aby v případě vážné chyby byl výrobcem vytvořen fix pro tuto vážnou chybu, která se vyskytla v ČNB; - přetížení jedné komponenty nesmí způsobit zastavení celku. Jmenovitě nesmí dojít k situaci, kdy přetížením jednoho komponenty dojde k podstatnému ovlivnění dostupnosti a výkonnosti poskytované druhou komponentou. - dodávané technické prostředky musí být vyráběny sériově, nesmí být vyvíjeny pro potřeby této konkrétní zakázky. Dodaná verze FW/mikrokódu v době instalace musí být stabilní provozní verze instalovaná ve světě nejméně u 50 zákazníků v jejich produkčním prostředí. Splnění požadavku je nutné doložit prohlášením výrobce.	Zajištění bezchybného uložení dat je pro ČNB jedním z prioritních požadavků. Zhotovitel musí na základě svých kontraktů s výrobce/distributorem zajistit takovou úroveň podpory, aby bylo možné problém eskalovat k výrobci (případně pověřené organizaci), kde se tímto problémem budou seriózně zabývat. Výsledné stanovisko samozřejmě může být závislé na konkrétní situaci (bude/nebude vytvořen fix, bude implementováno do nové verze FW apod.). Každá závada znamená čas zaměstnanců ČNB strávený její řešením. A to přináší na straně objednatele určité náklady. Není přípustné, aby zhotovitel prováděl jakékoliv ladění FW/mikrokódu nebo jiného dodaného SW v prostředí ČNB.
Kompletnost	Dodávka musí zahrnovat všechny komponenty nezbytné pro provoz.	
Režim vysoké dostupnosti	V rámci Řešení musí být zajištěn režim vysoké dostupnosti. Mezi dvěma různými instalačními lokalitami. Technologie musí být transparentní a může vyžadovat pouze konfigurační zásah do IS.	ČNB má v provozu tzv. nouzové záložní pracoviště, které je provozováno systémem aktiv-aktiv, tj. v obou lokalitách jsou provozovány různé IS. V případě výpadku/odstávky je zpracování převedeno do druhé lokality. Toto nouzové pracoviště je také koncipováno jako „disaster recovery“ centrum ČNB.
Zabezpečení dat	Data musí být zabezpečena proti selhání nebo přetížení prostřednictvím clusterového řešení (zdvojení komponent) a zálohováním dat do bezpečného úložiště.	Pro případ selhání obou nodů clusteru musí být k dispozici odpovídajícím způsobem zabezpečená záloha.

	Pokud je vyžadován pro tuto funkci speciální HW nebo SW, musí být dodán v takovém množství, aby odpovídal minimální poptávané kapacitě a dvěma nezávislým zálohám.	
Zabezpečení proti úniku dat	Servery jsou umístěny v prostorech s omezeným přístupem v dedikovaném uzamčeném racku. Komunikace mezi CMS a databází musí být zabezpečena, stejně tak komunikace mezi klientem a CMS.	HW, kde bude nainstalován CMS i SQL včetně záloh, bude umístěn v prostorech s omezeným přístupem v dedikovaném uzamčeném racku nebo v trezoru podle typu média.
Ochrana investic	Požadované funkce Řešení musí být aplikačně nezávislé (změna verze IS/aplikace nesmí mít vliv na funkce poskytované řešením).	Všechny poskytované funkce musí být nezávislé na IS. Pro všechny informační systémy musí být poskytované služby transparentní, tj. nesmí existovat vazba mezi informačními systémy a řešením ve smyslu nutnosti certifikace výrobcem dodaného HW nebo SW.
Kapacitní rozšiřitelnost	Navržená technologie musí umožňovat rozšíření o další uživatele a dokup dalších komponent dle množství uvedeném ve smlouvě.	V budoucnu se předpokládá navýšení počtu uživatelů.
Kapacita a prostor pro data	Celková kapacita na nově dodávaných čipových kartách a USB tokenech musí být minimálně 10 klíčových párů a certifikátů o velikosti každého klíče/certifikátu v rozmezí od 1024 do 4096 bitů. Kapacita pro kvalifikované certifikáty musí být minimálně 2 klíčové páry a certifikáty o velikosti každého klíče/certifikátu v rozmezí od 1024 do 4096 bitů.	Požadavek na celkovou kapacitu vychází, ze současného stavu a z očekávaného nárůstu pro další období.
Výkonnost	Výkonové parametry musí být splněny tak, aby časová odezva všech operací karty byla srovnatelná s operacemi v současném systému před čipových karet SCK. Jedná se zejména o časovou odezvu při přihlášení uživatele do domény s využitím certifikátu. Tento čas nesmí být delší než 10 s.	
Homogenita	Navržené řešení musí být homogenní, tzn. že ke všem komponentám musí být přistupováno rovnocenně. Tím je míněno, že veškeré komponenty stejného významu nebo funkce musí mít také stejná privilegia, omezení, stejné funkce a odpovídající výkonnost.	Z důvodu flexibility (možnost bezproblémové změny umístění aplikací) a z důvodu zjednodušení správy musí být navržené řešení stejné pro obě lokality (ústředí/ZP).

	Je vyžadováno jednotné Řešení z hlediska zajištění jeho správy. Navržené řešení musí být symetrické (shodné) pro obě lokality.	
Ladění výkonnosti/přesun zpracování na jiný CMS	Je požadována funkcionalita SW umožňující přesun zpracování na druhý CMS s menším zatížením. Přesun musí proběhnout on-line vzhledem k aktivitě serveru a bez narušení jeho provozu. Tato funkcionalita nemusí zajišťovat automatický návrh přesunů ani jej automaticky provádět. Pokud bude SW umět automatické přesuny, musí být možné je zablokovat nebo alespoň konfigurovat na uživatelské úrovni.	Jedná se o „poloautomatickou“ optimalizaci zátěže CMS bez nutnosti odstávek provozu.
Kompatibilita s prostředím ČNB	Při realizaci informačního systému je nutné zajistit, aby programové komponenty realizovaného IS nebyly v rozporu s komponentami dalších provozovaných IS. Realizovaný IS tedy musí být provozovatelný v systémovém prostředí ČNB a současně nesmí narušovat funkčnost ostatních IS. Navržené řešení musí dodržovat standardy uvedené v části „Popis současného stavu a infrastruktury ČNB“.	Není přípustný zásah do konfigurace MS Active Directory.
Kompatibilita se stávajícím řešením CMS	Případně nově dodané komponenty musí být tato plně funkční s výše uvedenými, již provozovanými komponenty informačního systému (viz popis současného stavu) a tato funkcionalita musí být garantována dodavatelem i pro nové verze dodaného SW.	
Kompatibilita aplikací	Musí být zajištěn provoz s aplikačním nasazením popsaným v popisu současného stavu. Přesun aplikací mezi lokalitami nesmí mít vliv na funkčnost clusteru těchto aplikací, ani dodaného Řešení jako celku. Navržené řešení musí být funkční se SW Safenet Autentication Client, které slouží jako obslužný SW pro USB tokeny Gemalto SafeNet eToken 5110 CC, používané jako kvalifikované prostředky pro vytváření elektronických podpisů	

Kompatibilita se zařízeními	Navržené řešení musí umožnit použití čipových karet a tokenů na serverech a klientech na platformách uvedených v tabulce „Seznam relevantních zařízení objednatele“. Možnost použití těchto serverů v kombinaci s operačním systémem musí být výrobcem SCK podporována. Jedná se zejména o serverové operační systémy/platformy: MS Windows Server 2008R2, 2012R2 a 2016 a RHEL 6, 7 a 8, které mohou být provozovány buď na fyzickém HW, nebo na virtualizační platformě VMware. Zároveň navržené řešení musí být funkční s USB tokeny Gemalto SafeNet eToken 5110 CC, které slouží jako kvalifikované prostředky pro vytváření elektronických podpisů.	Navržené řešení musí zajistit funkčnost na stávajícím technickém vybavení klientů i serverů a umožňovat i rozvoj do budoucna (přechod na vyšší verze provozovaného programového vybavení-operačních systémů). Vynucená změna operačních systémů nebo jejich verzí je v rámci nasazení Řešení zcela vyloučena.
Základní funkce	Realizace dvoufaktorového přihlášení do domény CNB a pro lokální přihlášení do Linuxových pracovních stanic, Vydání certifikátu na čipovou kartu interní certifikační autoritou prostřednictvím CMS i prostředky Windows. Vydání certifikátu z ESCB PKI prostřednictvím Active-X komponenty (PKCS11) v Internet Exploreru 11. Přihlášení do domény prostřednictvím certifikátu na čipové kartě ze standardních PC s Windows 7 a Windows 10, v případě Citrixu pak z terminálů a donglů Igel s Igel OS a notebooků s OS Windows 7, Windows 10 a OSX 10.13, 10.14 a 10.15. Přihlášení prostřednictvím protokolů RDP a TLS na servery 2008R2, 2012R2, 2016 a 2019. Realizace podpisů a to jak běžných, tak v případě USB tokenů i nově dodaných čipových karet také kvalifikovaných.	Jedná se o základní výčet funkcí. Další požadavky jsou konkretizovány v druhé části tabulky.

	Realizace podpisů v interně vyvíjených aplikacích a v prohlížeči Firefox prostřednictvím rozhraní PKCS11. Realizace podpisů ve standardních aplikacích jako jsou Outlook, Spisová služba, Podpisová kniha a prohlížečích IE a Chrome prostřednictvím rozhraní CSP nebo KSP. Využití čipové karty jako bezpečného úložiště pro přihlašovací certifikáty a pár klíčů, dále pro tři páry klíčů a certifikátů ESCB PKI, certifikát PostSignum a případně i pro další klíče a certifikáty pro přihlášení, pokud má uživatel více přihlašovacích účtů Použití čipové karty jako úložiště pro další textové údaje a jejich záloha a obnova.	
Množina podporovaných kryptografických algoritmů	Musí být podporován asymetrický algoritmus RSA o délce klíče až do velikosti 4096 bitů, hešovací algoritmy SHA-1, SHA-256, SHA-384, SHA-512, symetrický algoritmus AES o velikosti klíče 128 a 256 bitů a 3DES.	
Zabezpečení proti infiltraci a odposlechu komunikace	Proti zneužití odposlechem na sběrnici nebo na síti musí Řešení umožnit vytvoření důvěryhodného kanálu mezi sebou a participujícím aplikační komponentou Řešení i aplikace musí být nastavené tak, aby vyžadovaly vytvoření důvěryhodného kanálu před tím, než si mezi sebou začnou vyměňovat jakékoliv kryptograficky citlivé informace.	Objednatel bude realizovat pravidelné testy CMS monitorovacím nástrojem Qualys.
Bezpečnostní certifikace čipových karet a tokenů	Řešení musí zajistit minimálně certifikaci odpovídající úrovni EAL 4+ QSCD nebo vyšší a musí v tomto módu také pracovat.	Certifikace musí být doložena příslušným certifikátem.
Systém provozu	V obou lokalitách budou IS provozovány systémem active-active, tj. v každé lokalitě mohou s kteroukoliv částí Řešení v režimu HA komunikovat za běžného provozu různí klienti.	Tento systém umožňuje využití pořízených kapacit v běžném provozu k rozložení zátěže mezi jednotlivé klienty.
Duální připojení serverů	Požadován je nejen FailOver, ale i load balancing (všechny cesty mezi klientem a CMS musí být v normálním režimu aktivní a musí nad nimi	

	být zajištěn load balancing). Tato povinnost platí pro klienty (servery) dle přílohy č. 2. Ztráta některé z cest k CMS nesmí mít dopad na činnost klienta s výjimkou snížení propustnosti, tj. nesmí dojít k činnosti serveru, která povede k jeho nefunkčnosti (např. přesun zpracování aplikací na jiný uzel geoclusteru).	Ztrátou dostupnosti některé z cest k CMS nesmí být ovlivněna řádná činnost operačního systému nebo aplikací.
Dopad na provoz serverů	Dodávaný SW nesmí mít zásadní dopad na výkonnost serveru. Vyžadováno je tedy řešení, které má minimální dopad na celkovou zátěž serveru (tj. jeho CPU, RAM, NIC,….). Pokud bude navřeno řešení s dopadem na výkonnost serveru, nesmí mít větší dopad, než 10% výkonu CPU, nejvýše 10% kapacity RAM a nejvýše 10% LAN.	Zatížení serveru dodávanými komponentami nesmí zásadním způsobem omezovat výkonnost provozovaných aplikací.
Zátěž komponent síťového prostředí ČNB	Navržené řešení nesmí neúměrně zvyšovat zátěž prvků stávajícího systémového prostředí ČNB. Navýšení zátěže každé z komponent systémového prostředí je povoleno nejvýše o 5%.	Navržené řešení nesmí zcela svévolně, resp. pouze pro zajištění své vlastní režie navyšovat zátěž síťových komponent současného prostředí ČNB. Tím by mohla vzniknout nutnost některé z komponent posílit.
Rozměry a chlazení	Případně nově dodávané technické prostředky musí být umístitelné v těchto prostorech ČNB: Praha 1, Senovážná ul. 3 (místnosti VP304) Praha 5, Strojírenská 175 (místnost PP117) Zařízení bude v objektu ústředí umístěno do standardního 19“ stojanu ČNB (výrobce Triton, 42U 600x900mm, bez podstavce, s krytím IP20). Zařízení musí být dodáno včetně komponent, které umožní montáž do tohoto typu stojanu. V objektu ústředí je vytvořen systém tzv. teplé uličky. Zařízení jsou tedy ve stojanech s přívodem chladného vzduchu před stojan a výdech ohřátého vzduchu je zadem do zastřešené uličky a odtud je odváděn pryč.	Požadavek vychází ze specifikace prostor očekávaného umístění. Jiný stojan by přinesl problémy se zastřešením teplé uličky a s chlazením prostoru.

	V objektu ZP bude k dispozici stojan obdobných parametrů jako v ústředí. V ZP Zličín je v současné době chlazení zajištěno foukáním chladného vzduchu do zdvojené podlahy. V budoucnu se předpokládá stejný systém jako v Senovážné, tedy systém teplé a studené uličky. Dodávaná zařízení musí splňovat podmínku sání na přední straně a výdech na zadní straně v kombinaci s umístěním do stojanu ČNB.	
Napájení	Požadováno je připojení na rozvod s napětím 230V (=jednofázové) s jištěním nejvýše 25A. Je požadováno zajištění uložených dat tak, aby i při výpadku napájení trvajícím nejvýše 24 hodin nebyla tato ztracena (např., baterie pro zálohování).	Ve výpočetních střediscích ČNB jsou rozvaděče připraveny pro připojení systémů s 1 fázovým napájením.
Diagnostika	SCK musí mít zajištěnu trvalou diagnostiku poruch. V případě poruchy musí SCK problém hlásit objednateli, který rozhodne o urgentnosti odstranění závady.	Pro zajištění maximální spolehlivosti a včasného zajištění nápravy je vyžadována trvalá diagnostika poruch Řešení.
Synchronizační komponenta/skript	Součástí musí být komponenta, která zajistí objednatelem definovanou synchronizaci uživatelů SCK s AD. To znamená, že musí být možné definovat, které skupiny uživatelů s AD budou synchronizovány a v případě odebrání uživatele z AD bude zaslán minimálně jednou denně v definovaném intervalu notifikační mail o odebrání těchto uživatelů z SCK. Pokud budou mít úpravy stávajícího řešení vliv na funkčnost stávající komponenty pro synchronizaci, musí být v rámci dodávky upravena.	
Zálohování konfigurace	Musí být zajištěna možnost zálohování konfigurace klientského řešení a CMS (pokud systém sám o sobě neprovádí tuto zálohu i do jiného vzdáleného prostoru). Musí být také zajištěna možnost zálohování konfigurace související databáze SQL	Jedná se minimálně o požadavek na možnost automatického vytvoření textového (čitelného) reportu o konfiguraci CMS a konfigurace klientského SW pro potřeby případné nutné obnovy (ruční vložení).

Auditing	Logy řešení musí být externě ukládány ve formátu se stanovenou strukturou a významem dat – dokumentace formátu a možnost jeho strojového zpracování je veřejně dostupná.	Textový výstup je nezbytný pro systém SIEM.
Migrace dat	Po provedení rozšíření bude důležitým a náročným okamžikem migrace dat. Na tuto operaci bude kladen zřetel a ČNB neumožní dlouhodobé odstávky, maximální přípustné doby provozních odstávek jsou uvedeny níže v požadavku „Provozní odstávky“. Zhotovitel vypracuje postup pro migraci a rovněž kompletní migraci/import zcela zajišťuje. Podmínky pro provedení migrace dat jsou následující: 1) Musí být proveden testovací provoz SCK s implementovaným Řešením vč. jeho akceptace, aby byla zajištěna ochrana a zachování stávajících dat. 2) Migrace musí být provedena tak, aby mezi testovacím provozem a ověřovacím provozem došlo k vytvoření provozního prostředí SCK s implementovaným Řešením na podporovaných OS (viz též příloha č. 2). 3) Migrační postup pro migraci MS PKI 2008R2 na MS PKI 2016: Musí být zajištěna možnost migrace/import klíčů stávající PKI bez nutnosti generace nových klíčů a certifikátů a reinstalace PKI. Pokud bude nutné realizovat reinstalaci PKI pro testování, pak musí být také provedena zhotovitelem. Podmínkou realizace je zachování vrstvy MSCS v prostředí Windows, zachování stávajících dat a funkčnosti všech dalších souvisejících služeb CRL, OCSP, SCEP (NDES), Web enrollment a notifikací o konci platnosti certifikátů.	Prioritními požadavky jsou ochrana dat, minimalizace odstávek a minimalizace rizik plynoucích z přechodu (např. performance problémy). V nabídce musí být uvedeny navržené principy migrace a jejich dopady na nedostupnost dat.

	4) Migrační postup pro CMS a klientský SW: Musí být zajištěna migrace/import stávajících dat bez nutnosti generace nových čipových karet a bez změny konfigurace. <u>Podmínkou realizace je dále zachování stávajících dat, tj. jak klíčů, tak certifikátů a ostatních textových údajů na stávajících čipových kartách.</u>	
Provozní odstávky	Při instalaci SW vybavení a migraci dat musí být dodrženy následující podmínky: - odstávka pouze jednoho node clusteru (aplikačního) na nejvýše 8 hodin v běžné pracovní době - odstávka celého clusteru serveru (aplikačního) na maximálně 4 hodiny a to jen v době o víkendu - odstávka non-cluster serveru na nejvýše 4 hodiny dle významu serveru buď po pracovní době, nebo jen během víkendu Odstávky jsou možné jen po předchozí domluvě se zadavatelem!	
Opravy HW	Pro případ poruchy čipové karty, tokeny a případné další technické prostředky ČNB nevrací a zajistí jejich mechanické zničení.	Tento způsob oprav se týká všech nosičů, které obsahují data ČNB a současně na nich nedochází k jejich ztrátě dat při odpojení napájení (tedy veškeré technologie pevných disků, flash disků, čipových karet apod.) Znehodnocení nebo zničení zajišťují zaměstnanci objednatele.
Licencování	V případě klientského SW je nutné, aby byl SW licencován pro 1 750 uživatelů. Zhotovitel ve své nabídce musí uvést veškerý dodávaný SW včetně způsobu jeho licencování a včetně počtu dodávaných kusů. Součástí dodávky budou i veškeré licenční podmínky a případné licenční klíče.	Licence musí pokrýt minimální požadované množství uživatelů podle čl. 1 smlouvy.

1.2 Specifické požadavky na dílčí komponenty SCK

Požadavek	Popis	Poznámka/zdůvodnění
Funkční požadavky na kontaktní rozhraní čipové karty	- Privátní klíče generované čipovou kartou není možné exportovat. - Ochrana dat a operací pomocí PIN. - Omezení počtu pokusů o zadání PIN. - Zablokování čipové karty po vyčerpání pokusů o zadání PIN. - Odblokování PIN zablokované čipové karty jak lokálně tak vzdáleně. - Životnost čipové karty nesmí být programově omezena, případně musí být libovolně nastavitelná. - Velikost paměti min. 64kB.	
Kapacitní požadavky na kontaktní rozhraní čipové karty a USB tokenu	Čipová karta musí umožnit současné uložení: - min. 10 párů klíčů a 10 certifikátů (X.509 v.3) uživatele, - min. 2 páry klíčů a 2 certifikáty (X.509 v.3) kvalifikovaných certifikátů uživatele - min. 50 textových údajů (poznámek), jejichž délka může být až 500 znaků.	
Kryptografické požadavky na kontaktní rozhraní hybridní čipové karty a USB tokenu	- Implementace algoritmu SHA-1 a rodiny SHA-2. - Certifikace CC EAL4+ nebo vyšší / PP QSCD. - Podpora délky klíče RSA nových čipů až 4096 bitů. - Implementace rozhraní v souladu se standardy PKCS#11, MS-CAPI, MS-CNG a CSP Minidriver. - Generace RSA páru klíčů kartou. - RSA podpis realizovaný kartou.	
Fyzické požadavky na čipové karty	- Hybridní čipová karta musí mít integrovanou kontaktní a bezkontaktní část. - Čipová karta s kontaktním rozhraním musí být osazená pouze kontaktním čipem. - Kompatibilita s požadavky vyplývajícími z normy ČSN EN 7816, části 1-4.	

	- Čipové karty nesmí být vybaveny magnetickým pruhem a čip musí být umístěn na zadní straně karty. - Čipové karty musí být lesklé bílé nepotištěné pouze se sériovým číslem kontaktního čipu na zadní straně karty v dolní části max. do výšky 8 mm. - Čipová karta nesmí mít žádný otvor. - Osazení čipu na kartě musí být zajištěno vhodnou technologií umožňující následný bezproblémový potisk.	
Funkční požadavky na bez kontaktní rozhraní čipové karty	Rozhraní HID s pracovní frekvencí 13,56MHz dle HID iClass Reference Guide, iCLASS Prox 16K/16 s následujícími parametry výrobce: - Model 2112CGGNN nebo 2132CGGNNN, kde se část Prox nebude využívat - 16k Bits (2k bytes) with 16 Application Areas. - Configured. - Non-Programmed iClass.	
Požadavky na čtečky čipových karet	- Čtečky musí mít ovladače MS Windows 7, 8, 10 a MS Windows Server 2008, 2012, 2016, RHEL 6, 7 a 8, Igel OS a OSX 10.13, 10.14 a 10.15 - Čtečky musí být funkční v MS Windows 7, 8, 10 a MS Windows Server 2008, 2012, 2016, RHEL 6, 7 a 8, Igel OS a OSX 10.13, 10.14 a 10.15 - Vyhovovat standardu PC/SC. - Vložení karty alespoň 100 000 cyklů (pro USB čtečky). - Podpora rychlosti komunikace s kartou 38,4 kbps. - Podpora protokolů T=0, T=1. - Životnost alespoň 500 000 hodin. - USB čtečky musí být kompatibilní jak s rozhraním USB 2.0 tak 3.0. - USB čtečky musí a mít délku přívodního kabelu alespoň 170 cm.	
Obecné požadavky na klientský SW	- SW musí být plně funkční pro uživatele, který nemá přidělena práva lokálního administrátora a v implementovaném systému čipových karet má přidělenu roli uživatele.	

	- Činnosti související s certifikáty, klíči, přihlašovacími a ostatními údaji je možné provádět nezávisle na SW pro centrální správu čipových karet. - Bezpečná záloha textových údajů uložených na čipové kartě. - Obnova údajů ze zálohy. - Vyžadovaná podpora standardů PKCS#12, PC/SC, PKCS#11v2.01, Microsoft CryptoAPI a CNG, RSA Public Key Cryptography, SHA-2, SHA-3. - Podporované OS Widows Server 2008R2 až 2019, Windows 7 až Windows 2010, Linux RHEL 6, 7 a 8, Igel OS a OSX 10.13, 10.14 a 10.15.	
Funkční požadavky na klientský SW související s klíči a certifikáty	- Uložení klíčů a certifikátů vydaných CA na platformě MS Windows Serveru 2008, 2012, 2016 prostřednictvím nativního rozhraní Windows. - Lokální přihlášení do systému Linux - Přihlášení prostřednictvím Citrix receiveru - Obnova certifikátů vydaných CA na platformě MS Windows Serveru 2008, 2012, 2016. - Automatizovaná registrace certifikátů do operačního systému MS Windows. - Volba defaultního certifikátu pro přihlášení do domény na platformě MS Windows. - Import certifikátů a klíčů uložených v souboru na čipovou kartu (PKCS#12). - Odebrání (smazání) klíčů a certifikátů uložených na čipové kartě. - Využití uložených certifikátů v aplikacích (1) MS Internet Explorer 11, Chrome, Firefox a Edge Chromium (2) MS Outlook 2010 a 2016 (3) MS Terminal Services (4) Citrix	

	- Uložení textových údajů na čipovou kartu, jejich záloha, obnova a bezpečné smazání - Operace s privátními klíči a textovými údaji musí být podmíněna úspěšným zadáním PIN.	
Funkční požadavky na klientský SW související s PIN	- Nastavení minimální délky PIN. - Nastavení struktury PIN (povinné znaky) z množiny: malé písmeno, velké písmeno, numerický znak. - Vynucení změny PIN po uplynutí stanoveného intervalu. - Kontrola nově zadávaného PIN proti stanovenému počtu historie PIN. - Změna PIN po úspěšném zadání platného PIN.	
Obecné požadavky na SW pro centrální správu čipových karet	- Přístup k serveru pro centrální správu bude realizován z pracovní stanice. Pokud vyžaduje přístup instalaci dodatečných komponent na pracovní stanici, musí být jejich instalace provedena prostřednictvím služby MS Installer (standardní služba operačního systému) s využitím Group Policy MS Windows Serveru 2008 a 2016, nezávisle na jazyku operačního systému - Pro přístup je vyžadována minimálně autentizace prostřednictvím čipové karty, volitelně také prostřednictvím jména a hesla.	
Funkční požadavky na SW pro centrální správu čipových karet	- Přiřazení a vydání karty uživateli (nahrání certifikátu pro přihlášení). - Nastavení požadavků na PIN: (1) Nastavení počáteční hodnoty PIN. (2) Nastavení minimální délky PIN. (3) Nastavení struktury PIN (povinné znaky) z množiny: malé písmeno, velké písmeno, numerický znak. (4) Změna PIN po úspěšném zadání platného PIN - Dostupnost mechanismu pro odblokování karet po opakovaném chybném zadání PIN a to jak lokální, tj. s přístupem k CMS, tak vzdálené, bez přístupu k CMS.	

	- Automatické zasílání avíza o konci platnosti certifikátu jeho držiteli s odkazem do centrální správy, kde si uživatel může certifikát obnovit. - Oddělení rolí umožňující vykonávat jednotlivé činnosti. - Centrální audit - Systematické a chronologické zaznamenávání provozních informací, které umožňují zpětnou rekonstrukci činností a identifikaci uživatelů. - Podpora databáze MS SQL 2016 i 2019. - Vygenerování žádosti o certifikát. - Podpora MS Active Directory. - Zabezpečení komunikace s klientským SW. - Podporu archivace šifrovacích klíčů v CA a databázi. - Smazání všech údajů uložených na čipové kartě (klíčů, textových údajů atd.)	
Požadavky na konfiguraci SQL	- Konfigurace musí být provedena na objednatelem dodaném SQL serveru. - Všechny kroky konfigurace databáze musí být zdokumentovány a zároveň dodavatel přebírá plnou odpovědnost za funkčnost této konkrétní databáze, jako by byla nedílnou součástí dodaného systému čipových karet.	
Požadavky na instalaci a konfiguraci SW pro centrální správu	- Instalace musí být provedena na serveru poskytnutém objednatelem. Požaduje se instalace aktuální podporované verze. - Konfigurace musí být provedena tak, aby spolupracovala s certifikační autoritou na platformě MS Windows Serveru 2008, 2016. - Konfigurace musí být dále nastavena takovým způsobem, aby byly odděleny jednotlivé role a bylo možné vydat kartu uživateli pouze po schválení. Výsledná konfigurace musí umožnit správu všech čipových karet, tj. jak nově pořizovaných tak stávajících (viz charakteristika současného stavu)	

Požadavky na instalaci a konfigurace klientského SW	- SW vybavení bude instalováno na pracovní stanice uživatelů, terminály Igel a servery. HW a SW viz seznam relevantních zařízení objednatele. - Instalace tohoto SW vybavení bude objednatel provádět v prostředí MS Windows především prostřednictvím vzdálené automatické instalace. Instalace bude realizována v prostředí MS domény prostřednictvím služby MS Installer (standardní služba operačního systému) s využitím Group Policy MS Windows Serveru 2008R2 a 2016, nezávisle na jazyku operačního systému. Lokální instalace musí být k dispozici pro Linux, terminály Igel a stanice s MacOS. - Instalační balíček musí být dodán nakonfigurován i v konfigurovatelné podobě včetně nástroje umožňujícího jeho úpravy a změnu konfigurace. - Případně nově dodaný klientský SW musí být interoperabilní a vzájemně slučitelný se stávajícím klientským SW tak, aby na pracovní stanici umožňoval bezproblémový souběžný provoz stávajících i nově dodaných čipových karet. - Programové vybavení pro Windows platformu vyžadující zvýšená oprávnění musí umožnit bezobslužnou automatizovanou instalaci s parametry zadávanými v rámci příkazového řádku, bez vynuceného restartu.	
Programová komponenta pro synchronizaci	- Zhotovitel případně upraví stávající nebo vytvoří novou programovou komponentu pro synchronizaci uživatelů CMS s MS AD. - Musí být zajištěna funkce pravidelné synchronizace vybraných organizačních jednotek mezi AD a CMS. Zajištění notifikace o možnosti zrušení uživatelů v CMS, pokud již nebudou v AD.	
Požadavky na podpůrné systémy.	- Zachování stávajících funkcí a rozsahu nasazení MS PKI uvedeného v popisu současného stavu - Zajištění funkce odesílání emailové notifikace o blížícím se konci platnosti certifikátů všech typů vydávaných certifikátů MS PKI	

	s možností volby intervalu zasílání a na email uvedený v certifikátu.	

Omezení

A) *Technická omezení*

V rámci implementace (realizace) musí zhotovitel dodržet standardy ČNB a současně musí respektovat současnou infrastrukturu tak, aby nedošlo ke změnám, které by mohly ovlivnit funkčnost systémů ČNB.

Jedná se zejména o specifikace uvedené v popisu současného stavu, standardech ČNB, kompatibilitu Řešení se stávajícími technologiemi (příloha č. 4), dodržení požadovaných funkcí a vlastností a zajištění dostatečné bezpečnosti.

B) *Dopad na IS a servery*

Navržené řešení nesmí mít negativní dopad na vlastní IS a servery na kterých běží, tj. zvýšení jejich zátěže z pohledu CPU, RAM, síťových interface apod. Vzhledem k tomu musí být striktně dodrženy definované parametry viz „Striktně vyžadované funkce a vlastnosti".

Z hlediska výkonnosti musí nové řešení zajistit minimálně stejné odezvy (při realizaci podpisu nebo dešifrování) jako jsou v současné době, aby nedošlo ke zpomalení provozovaných IS.

C) *Zachování stávajícího stavu aplikací/IS a uživatelů*

Stávající aplikace/IS mimo SCK nebudou přeprogramovány a budou i nadále používat současná volání služeb OS a souvisejících volání čipových karet prostřednictvím OS nebo rozhraní PKCS11. Stejně tak uživatelé nesmí negativně ve svých rutinních činnostech pocítit omezení.

Příloha č. 5

Bezpečnostní požadavky ČNB

1. Zhotovitel odpovídá za to, že do objektů objednatele (dále jen „ČNB“) budou vstupovat nebo vjíždět pouze ti jeho pracovníci, kteří jsou jmenovitě uvedeni v písemném seznamu schváleném ČNB (dále jen „seznam“). Tato povinnost se vztahuje i na posádky vozidel zhotovitele vjíždějících do garáží ČNB za účelem složení a naložení nákladu. Seznam zhotovitel předloží ČNB nejpozději den před zahájením prací.
2. Seznam bude obsahovat tyto položky: jméno, příjmení a číslo průkazu totožnosti každého z pracovníků zhotovitele. Zhotovitel se zavazuje zajistit, aby všichni jeho pracovníci uvedení v seznamu byli ještě před předložením seznamu ČNB proškoleni o podmínkách zpracování osobních údajů a o právech subjektů údajů ve smyslu obecného nařízení o ochraně osobních údajů - 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 (dále jen „GDPR“). Zhotovitel se zejména zavazuje, že všichni jeho pracovníci uvedení v seznamu budou nejpozději do okamžiku předložení seznamu ČNB poučeni:
   a) o tom, že zhotovitel předá jejich osobní údaje v rozsahu: jméno, příjmení a číslo průkazu totožnosti České národní bance, sídlem Na Příkopě 28, Praha 1 v rámci plnění této smlouvy, a to za účelem ochrany práv a oprávněných zájmů ČNB (zajištění evidence osob vstupujících do budovy ČNB z důvodu ochrany majetku a osob a správy přístupového systému ČNB);
   b) o veškerých právech subjektu údajů, která mohou uplatnit vůči zhotoviteli a ČNB, zejména o právu na přístup k osobním údajům, které jsou o nich zpracovávány, právu na námitku proti zpracování osobních údajů, právu požadovat nápravu situace, která je v rozporu s právními předpisy, a to zejména formou zastavení nakládání s osobními údaji, jejich opravou, doplněním či odstraněním, jakož i o právu podat stížnost k Úřadu pro ochranu osobních údajů.
3. Za poučení svých pracovníků ponese zhotovitel vůči ČNB následně odpovědnost. V případě nesplnění povinnosti podle bodu 2. nahradí zhotovitel újmu, která v souvislosti s uvedeným ČNB vznikne, a to včetně případné nemajetkové újmy vzniklé poškozením dobrého jména a dobré pověsti, újmy vzniklé v důsledku postihu pravomocně uloženého ČNB správním nebo jiným k tomu oprávněným orgánem veřejné moci a újmy vzniklé ČNB v důsledku úspěšného uplatnění práv pracovníků zhotovitele vůči ČNB.
4. Požadavky na případné doplňky a změny schváleného seznamu je nutno neprodleně oznámit ČNB. Případné doplňky a změny seznamu podléhají schválení ČNB. Osoby neschválené ČNB nemohou vstupovat do objektů ČNB, přičemž ČNB si vyhrazuje právo neuvádět důvody jejich neschválení.
5. Při příchodu do objektů ČNB pracovníci zhotovitele sdělí důvod vstupu, prokáží se osobním dokladem a podrobí se bezpečnostní kontrole. Osoby, které nejsou uvedeny v seznamu, nebudou do objektů ČNB vpuštěny.
6. Schválení pracovníci zhotovitele musí dbát pokynů bankovních policistů, které se týkají režimu vstupu, pohybu a vjezdu do objektu ČNB. Pracovníci zhotovitele budou do prostor ČNB vstupovat a v těchto prostorách se pohybovat v režimu návštěv, to znamená vždy pouze v doprovodu zaměstnance ČNB nebo zaměstnance referátu bankovní policie ČNB.
7. V případě mimořádné události se pracovníci zhotovitele musí řídit pokyny bankovních policistů nebo dozorujícího zaměstnance ČNB, a dále instrukcemi vyhlašovanými vnitřním

rozhlasem ČNB.

8. Pracovníci zhotovitele nesmí vnášet do prostor ČNB nebezpečné předměty, jako jsou střelné zbraně, výbušniny apod. O tom, co je či není nebezpečný předmět, rozhodují bankovní policisté v souladu s vnitřními předpisy ČNB.
9. ČNB si vyhrazuje právo nevpustit do objektů ČNB pracovníka zhotovitele, který je zjevně pod vlivem alkoholu, drog nebo jiné omamné látky.
10. Bez písemného povolení ČNB je zakázáno fotografování a pořizování videozáznamů z interiéru objektů ČNB.
11. Ve všech prostorech objektů ČNB je přísný zákaz kouření a používání otevřeného ohně. O povolení práce se zvýšeným požárním nebezpečím požádá zhotovitel písemnou formou vždy nejpozději jeden pracovní den před zahájením prací dozorujícího zaměstnance ČNB. Dále se pracovníci zhotovitele musí zdržet poškozování či odcizování majetku ČNB, a dále i jakéhokoli nevhodného chování vůči zaměstnancům a návštěvníkům ČNB.
12. Pracovníci zhotovitele uvedení v seznamu se musí před započetím výkonu práce v objektech ČNB seznámit, ve smyslu předpisů o požární ochraně, bezpečnosti a hygieně práce, se specifiky daných objektů ČNB (např. způsob vyhlášení požárního poplachu, určení ohlašovny požáru, seznámení s únikovými cestami, poplachovými směrnicemi, evakuačním plánem, umístěním věcných prostředků požární ochrany apod.). ČNB je oprávněna kdykoliv podrobit kontrole kterékoliv pracovníka zhotovitele uvedeného na seznamu ohledně dodržování těchto předpisů a ustanovení.

Příloha č. 6

Návrh technického řešení

Veřejná zakázka:
„Úpravy stávajícího systému čipových karet (SCK), jeho provozní podpora a související dodávky HW a SW“

Česká národní banka

Návrh technického řešení

Zodpovídá: [redacted]	[redacted]	Schválil:	[redacted]
	Vedoucí projektu		Místopředseda představenstva
V Praze dne:	3.3.2021	V Praze dne:	3.3.2021

Vypracováno na základě veřejné zakázky „Úpravy stávajícího systému čipových karet (SCK), jeho provozní podpora a související dodávky HW a SW“. Materiál je určen pouze pro vnitřní potřebu České národní banky a společnosti T-SOFT a.s.

Zpracovali: [redacted]

T-SOFT a.s., U Zásobní zahrady 2552/1a, 130 00 Praha 3 – Žižkov, tel.: 261 710 561/62, fax: 261 710 563,
e-mail: tsoft@tsoft.cz

OBSAH

1. ÚVOD

2. RÁMCOVÝ POPIS ÚPRAV A ROZŠÍŘENÍ STÁVAJÍCÍHO ŘEŠENÍ

2.1 Popis úprav a rozšíření

2.1.1 Upgrade a migrace stávajících prvků

[redacted]

2.1.2 Doplnění nových prvků

[redacted]

2.2 Zapojení technických a softwarových prostředků

2.2.1 Využití stávající infrastruktury

[redacted]

2.2.2 Schéma zapojení

2.2.3 Popis funkčnosti

3. NÁVRH POSTUPU MIGRACE NASTAVENÍ

3.1 Postup migrace nastavení

[redacted]

3.1.1 Testovací provoz

[redacted]

3.1.2 Ověřovací provoz

[redacted]

3.2 Předpokládané odstávky

[redacted]

Příloha č. 7

Specifikace cen včetně podrobného rozpisu ceny plnění (v Kč bez DPH)

Dílo		
		Cena v Kč bez DPH
1. etapa (realizační studie)		140 000,00 Kč
2. etapa		2 121 154,00 Kč
z toho	dodávka technických prostředků	628 520,00 Kč
	zajištění programových prostředků	638 634,00 Kč
	školení zaměstnanců	14 000,00 Kč
	instalace, implementace, vytoření testovacího prostředí a další plnění jinde nezahrnutá	840 000,00 Kč
3. etapa (realizační dokumentace)		84 000,00 Kč
	školení zaměstnanců	14 000,00 Kč
	realizační dokumentace	70 000,00 Kč
Dílo celkem		2 345 154,00 Kč
z toho školení celkem		28 000,00 Kč

Provozní podpora	
	Cena za 1 hodinu v Kč bez DPH
Cena za budoucí rozvoj podle čl. VI odst. 6 písm. a) až d)	1 750,00 Kč
	Cena za čtvrtletí v Kč bez DPH
Paušální cena za provozní podporu podle čl. VI odst. 3 až 5	187 707,00 Kč

Další dodávky technických a programových prostředků (HW a SW)	
	Cena za 1 kus v Kč bez DPH
Cena za dodatečné dodávky hybridní čipové karty	1 225,00 Kč
Cena za dodatečné dodávky kontaktní čipové karty	567,00 Kč
Cena za dodatečné dodávky USB tokenu	537,00 Kč
Cena za dodatečné dodávky USB čtečky čipových karet	674,00 Kč
Cena za dodatečné dodávky bluetooth čtečky čipových karet	5 012,00 Kč
Cena za dodatečné dodávky klientského SW	261,00 Kč
Cena za dodatečné dodávky SW pro centrální správu	650,00 Kč

Specifikace technických prostředků a programových prostředků				
název (popis)	rozlišení HW/SW (Appliance zařaďte do HW)	Množství (u HW počet ks, u SW počet licenčních jednotek)	Cena za jednotku v Kč bez DPH	Cena v Kč celkem bez DPH
Specifikace technických prostředků				
hybridní čipové karty MD 940 v konfoguraci dle technické specifické ZD	HW	500	1 189,00 Kč	594 500,00 Kč
Specifikace programových prostředků				
Licence MyID pro druhý server - HA režim se stávajícím MyID	SW	1	476 434,00 Kč	476 434,00 Kč
MyID Client license	SW	100	1 622,00 Kč	162 200,00 Kč

Příloha č. 8

ČESKÁ ČNB NÁRODNÍ BANKA

Projekt *ID projektu*

„*Název projektu*“

Realizační studie

Verze	
Datum verze	
Autor	
Vedoucí projektu zhotovitele	
Vedoucí projektu objednatele	

Historie změn

Verze	Datum	Autor	Popis změny

Obsah

Hlavní kapitoly realizační studie jsou povinné, struktura podkapitol je doporučená, možno ji rozšiřovat či upravovat dle potřeb projektu.

1. ÚVOD

- Účel dokumentu

[Dokument realizační studie popisuje způsob realizace, aktivace a následného provozu služby včetně analýzy funkčních požadavků, softwarové architektury a systémových požadavků tak, aby byla prokázána realizovatelnost všech objednatelem zadaných požadavků. ***Text kurzívou v hranatých závorkách je návodem, neměl by zůstat součástí výsledného dokumentu.****]*

- Seznam pojmů a zkratek

[Výčet klíčových zkratek a pojmů s jejich vysvětlením]

Termín/Zkratka	**Popis/Význam**

- Přehled použitých symbolů

[Popis použitých grafických symbolů v dokumentu]

Grafický symbol	**Význam**

- Legislativa, technické normy a standardy

[Seznam legislativy, standardů a norem používaných při realizaci řešení.]

Č. zákona/ ČSN..... ISO.....	**Název/Popis**

2. REALIZACE VĚCNÉHO ZADÁNÍ

- Analýza procesů

[Kapitola obsahuje analýzu procesů spojených s používáním nyní implementovaného řešení SCK v prostředí objednatele a jejich převod/změnu pro nově implementované SCK. Pro jejich grafické znázornění lze použít například UML Activity diagram, nebo BPMN (Business Process Model and Notation), dále diagramy typu MS Visio apod.].

- Analýza funkčních a procesních požadavků

[Kapitola obsahuje mapování požadavků na cílové řešení – viz příloha č. 4 návrhu smlouvy („Technická a funkční specifikace předmětu plnění"). Popis tak ve stručné formě představuje způsob realizace jednotlivých požadavků.]

ID[2)]	Popis požadavku	Název funkcionality	Poznámka / jak bude realizováno

3. TECHNICKÁ REALIZACE ŘEŠENÍ

- Integrace s IS ČNB

[Kapitola obsahuje:
- *popis možností integrace řešení SCK s jednotlivými stávajícími a budoucími (projektovanými) IS ČNB,*
- *detailní popis rozhraní pro komunikaci s IS ČNB.]*

- Migrace dat

[Kapitola obsahuje analýzu přechodu z původního zapojení a provozu SCK a nově projektované zapojení z hlediska jejich převoditelnosti a datové migrace (tj. jednoznačné srovnání datových objektů, které budou využívány při migraci dat mezi oběma systémy) a popis vlastní migrace. Na analýze se podílejí jak zadavatel, tak zhotovitel.]

- Bezpečnost

[Kapitola obsahuje popis řešení z hlediska bezpečnosti, integrity a důvěrnosti dat, relevantní normy, politiky a standardy, vnitřní předpisy objednatele.]

3..1. Analýza bezpečnostních požadavků

[Podkapitola obsahuje analýzu bezpečnostních požadavků.]

3..2. Autentizace a autorizace, řízení přístupu

[V podkapitole je popsán princip řízení přístupů k informacím resp. informačním aktivům nové řešení SCK: jakým prostřednictvím přistupují interní a externí uživatelé, popis technických (aplikačních) účtů – bez časového omezení; způsob automatického blokování účtů uživatelů při ukončení zaměstnaneckého poměru v ČNB, povolené protokoly apod.]

[2)] ID požadavku objednatele ze zadávací dokumentace případě identifikace části smlouvy, kde se požadavek nachází.

3..3. Logování

[V podkapitole je popsán způsob logování a monitorování logů, napojení na SIEM.]

3..4. Zabezpečení síťové komunikace a uložených dat

[V podkapitole je popsán způsob, jak je zabezpečena síťová komunikace mezi SCK a klientskými informačními systémy a zabezpečení uložených dat – FileSystem/DataBase/jiné.]

3..5. Soulad s legislativou (Compliance)

[V podkapitole je popsán způsob, jak je zabezpečen soulad s legislativou – např. ZoKB, ISO20022, eIDAS apod. V případě, že navrhované řešení nebude splňovat nějaké legislativní požadavky, uvede se to v této kapitole včetně zdůvodnění proč.]

- Návrh architektury technického řešení

[Kapitola popisuje globální architekturu řešení SCK a fyzickou architekturu nasazení řešení v infrastruktuře ČNB s ohledem na provoz, high-availability, monitoring, zálohování a archivaci.]

3..1. Požadavky na systémové prostředí

[Podkapitola obsahuje SW a HW specifikaci pro nasazení v prostředí ČNB. Součástí je i sizing HW prostředků pro účely implementace. Různá prostředí provoz/test/vývoj/školení/atd. jsou popsána zvlášť.]

Tabulka 1: HW specifikace

Prvek	Typ	Výkon	RAM	Disková kapacita	Síťové rozhraní	Poznámka
APP1	*Virtuální server*	*2 – 4 virtuální CPU, 2 – 3 GHz*	*4 – 8 GB*	*15 GB*	*100 Mbps*	

Tabulka 2: SW specifikace

Prvek	OS	Databázové služby	Aplikační služby	Poznámka
APP1	*Windows Server 2008 R2 ENG x64*	*Oracle client 10g*	*MS IIS 7.5 ASP.NET 3.5 SP1*	

- Způsob implementace do systémového prostředí ČNB

[Kapitola obsahuje postup nasazení řešení do cílového prostředí s ohledem na stanovení příslušné součinnosti ze strany ČNB.]

4. Návrh projektové realizace

- Detailní harmonogram realizace

[Harmonogram realizace uvádí rozpad realizace projektu do jednotlivých přírůstků (dílčích plnění), etap, fází a činností s ohledem na dodržení stanovených termínů/lhůt. Harmonogram *musí obsahovat milníky pro předání díla nebo jeho částí k akceptačnímu řízení.]*

- Požadavky na součinnost (*pro externí dodávku)*

[V kapitole je uveden rozsah kapacit požadovaných zhotovitelem po objednateli]

ID	Popis součinnosti	Rozsah	Čerpání

Legenda:
ID: jedinečný identifikátor požadované součinnosti
Popis součinnosti: popis aktivit, požadovaných zhotovitelem po objednateli
Rozsah: odhadovaný rozsah požadovaných kapacit v čld
Čerpání: četnost, způsob čerpání kapacit např. 1x týdně; 2hod v Pá

- Akceptační testy

[V kapitole je uveden seznam všech připravovaných akceptačních testů, které kompletně ověří požadovanou funkcionalitu systému a zodpovědnost za vypracování testovacích scénářů]

ID testu	Testovaná oblast	Testovací scénář	Požadavek	Testovací scénář vypracovává

Legenda:
ID scénáře: jedinečný identifikátor testovacího scénáře
Testovaná oblast: oblast testování např.: Komunikace s IS na Oracle Linux, ….
Testovací scénář: popis testovacího scénáře
ID požadavku: jedinečné identifikátory požadavků objednatele, které jsou daným testovacím scénářem ověřovány.
Testovací scénář vypracovává: jméno/firma autora testovacího scénáře

- Školení

[Kapitola detailněji popisuje způsob zajištění školení a proškolení příslušných pracovníků, okruh školených uživatelů a správců, kdo zodpovídá za zpracování školící dokumentace a pokud není uvedeno v harmonogramu, tak i předpokládané termíny školení]

- Dokumentace

[V kapitole je uveden seznam technické, provozní a uživatelské dokumentace a zodpovědnost za její zpracování/aktualizaci.]

5. Popis režimu provozní podpory

[Kapitola detailněji popisuje způsob zajištění provozní podpory. Jedná se například o konkretizaci kontaktních bodů podpory. Dále o případnou doplňkovou diagnostiku a mechanizmu uzavření řešení závady.]

6. Registr změn

[V kapitole je uveden seznam změn oproti předběžné studii/zadávací dokumentaci, jejich akceptace a jejich dopady do projektu – časové, zdrojové a finanční.]

ID změny	**Popis změny**	**Akceptována Ano/Ne**	**Realizace** (termín, zdroje a finance)

Příloha č. 9

Rozsah, obsah a lhůty školení

Zhotovitel zorganizuje pro objednatele dvě školení v délce jednoho dne (8 hodin) pro nejvíce 8 odborných pracovníků objednatele v rozsahu nezbytném pro zajištění provozu SCK s implementovaným Řešením v systémovém prostředí objednatele (konfigurace, administrace, běžná správa), a to:

- Školení pro technické správce ohledně instalace, konfigurace a upgrade programového vybavení (SW) SCK s implementovaným Řešením - školení správy SCK.
- Školení pro technické správce a pracovníky helpdesku s částí ohledně instalace, konfigurace a upgrade programového vybavení (SW) a částí ohledně řešení poruch technických či programových prostředků SCK s implementovaným Řešením - školení provozu SCK.

Potřebné školící materiály zajistí zhotovitel. Prostory pro školení a konkrétní data školení určí objednatel po dohodě se zhotovitelem.

Školení správy SCK musí být provedeno nejpozději před zahájením testovacího provozu a školení provozu SCK nejpozději do 2 týdnů od ukončení ověřovacího provozu.

Příloha č. 10

Obsah realizační dokumentace

Realizační dokumentace SCK obsahuje následující součásti:

1. Popis skutečného stavu SCK s implementovaným Řešením (skutečný stav zapojení, nastavení systému, komunikační protokoly a porty).
2. Provozní postupy pro správce infrastruktury (postupy při provozu, nastavení omezení přístupu, základních každodenních činností obsluhy), zejména:
   - Instalaci a konfiguraci programového prostředku (SW) pro centrální správu čipových karet a konfiguraci databáze SQL – zahrnuje především detailní popis instalace a následné konfigurace pro vydávání certifikátů, bezpečnostních nastavení a vytvoření přístupových rolí, profilu vydávané čipové karty a administrativních skupin včetně konfigurace obnovy přihlašovacích certifikátů na čipové kartě a nastavení auditování.
   - Administraci programového prostředku (SW) pro centrální správu čipových karet a databáze SQL – zahrnuje především činnosti související se zavedením uživatele do systému pro centrální správu, vystavením čipové karty, odblokováním čipové karty a zrušením uživatele.
   - Zálohu a obnovu programového prostředku (SW) pro centrální správu čipových karet a databáze SQL – zahrnuje především detailní popis procedur vytváření záloh, včetně popisů zálohovacích skriptů a popisů jednotlivých scénářů obnovy v případě selhání operačního systému, databáze SQL, případně programového prostředku (SW) pro centrální správu.
3. Havarijní plán, obsahující všechny nezbytné informace pro pracovníky objednatele, jak mají postupovat v případě řešení závad a krizových stavů [jako např. obnova po havárii programového prostředku (SW) pro centrální správu nebo obnova po havárii klientského programového prostředku (SW)] a jakou součinnost mají zhotoviteli poskytovat v případně, že závadu nebo krizový stav řeší zhotovitel, zejména:
   - Informace o umístění nezbytných záznamů (logů) vedoucí k bližší identifikaci závady a základní informace o tom, jak logy analyzovat (případně informaci, že konkrétní log je určen pro analýzu ve vyšších stupních podpory a jak se tento log dá uložit do souboru, aby mohl být odeslán např. e-mailem).
   - Informace o postupech při typických závadách a chybových hlášeních a popis postupu/ů, jak blíže identifikovat závadu. V této části by měl být uveden popis typických závad, které mohou nastat a mohou být odstraněny pracovníky objednatele (např. při výpadku jednoho CMS -> je potřeba uvést CMS do stavu on-line příkazem „abcd“; nefunguje komunikace mezi klientem a CMS -> je potřeba ověřit, zda je příslušný port CMS funkční, a následně provést akci „xyz“; atd.). Rozsah těchto typických závad bude záviset na složitosti navrženého Řešení.
   - Informace o postupech při atypických závadách (např. informaci o tom, že se má kontaktovat servisní podpora).
   - Informaci o postupu při havárii lokality, tj. zejména postup, jak zprovoznit příslušné komponenty SCK s implementovaným Řešením ve druhé lokalitě.

Příloha č. 11

Ověřování funkčnosti a akceptace

Zhotovitel umožní objednateli kontrolovat průběh plnění dle smlouvy prostřednictvím akceptace jednotlivých níže určených výstupů z plnění a dále prostřednictvím provedení testovacího provozu a ověřovacího provozu SCK s implementovaným Řešením; za tím účelem poskytne objednateli potřebnou součinnost.

Podrobnosti testovacího provozu

Testovací provoz bude zahájen **do 3 pracovních dnů** od doručení písemné výzvy zhotovitele pověřeným osobám objednatele, že bylo vytvořeno dedikované testovacího prostředí dle čl. I odst. 2 písm. c) smlouvy, byla dodána uživatelská dokumentace výrobce/výrobců technických prostředků (HW) a dokumentace programových prostředků (SW) dle čl. I odst. 2 písm. d) smlouvy a do SCK bylo implementováno Řešení v souladu se smlouvou.

Testovací provoz bude trvat **4 týdny; o zkrácení testovacího provozu rozhoduje objednatel**. V rámci akceptace je možné opakování testovacího provozu nebo jeho části i **nad stanovený časový rámec; o uvedeném rozhoduje objednatel.**

Vyskytne-li se během testovacího provozu jakákoliv závada dedikovaného testovacího prostředí nebo SCK s implementovaným Řešením bránící dalšímu testování, **testovací provoz se přerušuje až do jejího odstranění** zhotovitelem. **Odstraňování dalších závad zjištěných v průběhu testovacího provozu se řídí ustanoveními o podpoře dle smlouvy.**

Průběh testovacího provozu ani jeho opakování či opakování jakékoliv jeho části nemá vliv na lhůty a doby podle smlouvy.

Testovací provoz zahrnuje:

- Vytvoření a instalaci testovací konfigurace SW pro testovací klienty;
- posouzení souladu navrhovaného řešení se zadáním provedením akceptačních testů podle realizační studie;
- odzkoušení základních funkcí a operací s SCK s implementovaným Řešením;
- test migrace CA;
- provedení dalších nedestruktivních postupů potřebných dle objednatele k otestování naplnění požadavků objednatele na implementované Řešení (viz příloha č. 4 smlouvy „Technické podmínky předmětu plnění“), např. ověření v testovacích aplikacích;
- dokumentaci celého postupu.

Ověření naplnění požadavku „Migrace dat“ dle přílohy č. 4 smlouvy bude během testovacího provozu provedeno pouze **po teoretické stránce a testováním funkčnosti postupů a nástrojů**. **Migraci ostrých (skutečných, provozních) dat provede zhotovitel až po ukončení testovacího provozu na základě plánu ostrého přechodu.**

Testovací provoz je ukončen akceptací nebo akceptací s výhradami, neakceptace vždy znamená opakování testovacího provozu nebo jeho části.

Podrobnosti ověřovacího provozu

Ověřovací provoz bude zahájen **do 3 pracovních dnů** od doručení písemné výzvy zhotovitele pověřeným osobám objednatele, že bylo dokončeno naplnění požadavku „Migrace dat“ dle

přílohy č. 4 smlouvy a byla provedena kompletní konfigurace SCK s implementovaným Řešením.

Ověřovací provoz bude trvat **4 týdny; o zkrácení ověřovacího provozu rozhoduje objednatel**. V rámci akceptace je možné opakování ověřovacího provozu nebo jeho části i **nad stanovený časový rámec; o uvedeném rozhoduje objednatel.**

Vyskytne-li se během **ověřovacího** provozu jakákoliv závada SCK s implementovaným Řešením bránící dalšímu testování, **ověřovací provoz se přerušuje až do jejího odstranění** zhotovitelem. **Odstraňování dalších závad zjištěných v průběhu ověřovacího provozu se řídí ustanoveními smlouvy o podpoře.**

Průběh ověřovacího provozu ani jeho opakování či opakování jakékoliv jeho části nemá vliv na lhůty a doby podle smlouvy.

Ověřovací provoz zahrnuje:
- ověření naplnění požadavků objednatele na SCK s implementovaným Řešením (viz též příloha č. 4 „Technické podmínky předmětu plnění“);
- ověření režimu vysoké dostupnosti;
- dokumentaci celého postupu;
- měření významných provozních stavů dodaného řešení.

Akceptace

Akceptaci podléhá:
- realizační studie;
- SCK s implementovaným Řešením v rámci testovacího provozu;
- SCK s implementovaným Řešením v rámci ověřovacího provozu;
- realizační dokumentace.

Akceptaci části díla není možné zahájit, není-li akceptována předchozí část díla.

Průběh akceptace ani její opakování či opakování jakékoliv její části nemá vliv na lhůty a doby podle smlouvy.

1) Akceptace dokumentů: Akceptace bude zahájena **do 3 pracovních dnů** od předání příslušného dokumentu či dokumentů zhotovitelem objednateli a bude probíhat ověřením, že předaný dokument je prostý závad, tj. že má touto smlouvou (vč. příloh) stanovený obsah, neobsahuje vnitřní logické rozpory a je technicky i jazykově jednoznačný.

Do 5 pracovních dnů, u realizační studie, a do 15 pracovních dnů, u realizační dokumentace, od zahájení akceptace informuje objednatel písemně zhotovitele:

a) Že dokument je bez závad a akceptována bez výhrad.

b) Že dokument sice obsahuje závady, avšak je akceptován.

c) Že dokument obsahuje závady a není proto akceptován.

2) Akceptace SCK s implementovaným Řešením: Akceptace bude zahájena **spolu se zahájením příslušného provozu** a v jejím rámci bude sledováno, zda SCK s implementovaným Řešením v rámci užívání a dalších operací v příslušném provozu nevykáže závady. Za závadu se považuje též nesoulad s touto smlouvou (vč. příloh, zejména s požadavky objednatele dle přílohy č. 4 této smlouvy „Technické podmínky předmětu plnění“) a s realizační studií.

Současně s ukončením příslušného provozu informuje objednatel písemně zhotovitele:

a) Že SCK s implementovaným Řešením nevykazuje závady a je akceptováno bez výhrad.

b) Že SCK s implementovaným Řešením sice vykazuje závady, avšak je akceptováno.

c) Že SCK s implementovaným Řešením vykazuje závady a není proto akceptováno.

3) Společná ustanovení:

a) **Obsahuje-li dílo, resp. jeho příslušná část, závady, a proto nebylo akceptováno, opakuje se** příslušná část posuzování dokumentu, popř. posouzení dokumentu jako celku, nebo příslušná část příslušného provozu, popř. provoz jako celek, a to **do 3 pracovních dnů ode dne, kdy zhotovitel předá příslušnou část díla s odstraněnými závadami objednateli nebo písemně informuje pověřené osoby objednatele o odstranění závad příslušné části díla a toto plnění objednateli zpřístupní.**

b) **O akceptaci příslušné části díla bude vždy sepsán protokol**, který podepíší pověřené osoby smluvních stran. Je-li akceptováno se závadami, musí protokol obsahovat soupis závad, jejich kategorizaci (je-li možná dle smlouvy) a lhůty k jejich odstranění; tyto lhůty mají přednost před lhůtami podle ustanovení o podpoře dle smlouvy (je-li možné takovou lhůtu dle smlouvy užít). Není-li v protokolu lhůta pro odstranění závady uvedena, platí lhůta podle ustanovení o podpoře dle smlouvy (je-li možné takovou lhůtu dle smlouvy užít).

c) O tom, zda vada brání akceptaci nebo lze SCK s implementovaným řešením akceptovat rozhoduje objednatel.

[redacted]ODNÍ BANKA
Na [redacted] 03 Praha 1
47