Příloha č. 4

Technická specifikace systému cPortal

1 Úvod

1.1 Rozvoj systému

V rámci rozvoje systémů se jedná zejména o:

- vytvoření nových a úpravy stávajících softwarových komponent (programových modulů) pro jednotlivé dále specifikované oblasti a jejich zprovoznění v prostředí informačních systémů Zadavatele,
- modernizace systému v rozsahu specifikace dané metodicko-technickým popisem,
- úpravy databázových struktur, včetně přechodu používaného SW na nové verze (podle rozsahu) či produkty,
- úpravy na základě požadavků provozu a zákonných změn,
- konfigurace a úpravy komunikačních rozhraní pro jednotlivé dále specifikované oblasti
- vytvoření a udržování odpovídající dokumentace v aktuálním znění,
- uvedení do provozu, včetně konfigurace provozních parametrů a vyškolení pracovníků Zadavatele.

Zadavatel požaduje, aby první tři uvedené oblasti tvořily kompaktní řešení využívající v maximální míře stávající již implementovanou funkcionalitu Informačního systému celní správy (dále jen „ISCS“) a zachovávající maximální kompatibilitu na rozhraních se systémy spolupracujících orgánů státní správy a EU. Poptávané řešení představuje další krok při zpracování dat v celním a daňovém řízení, jehož se stane jeho součástí, a jeho nasazení nezbytně zvýší celkovou komplexnost stávajícího systému.

Pro plnění dle bodů zadavatel předpokládá následující činnosti, které musí být Dodavatelem zajištěny v rámci realizace:

- mít po celou dobu smluvního vztahu k dispozici kapacity (realizační tým) na plnění požadavků na rozvoj systému v předpokládaném ročním objemu, dle plánu rozvoje systému
- převzetí požadavků na vývoj systému
- globální analýza řešení – shrnutí požadované funkcionality,
- detailní analýza a návrh implementace řešení,
- implementační práce, předání díla,
- v případě zákonných změn evropské i národní legislativy, či modernizace SW a HW maximalizuje dodavatel práce tak, aby byly dodrženy termíny realizace pro provozní prostředí s ohledem na vazbu na jiné systémy v rámci CS, ČR a EU,
- technická a uživatelská dokumentace,
- testování na straně Dodavatele, testy u Zadavatele,
- školení dle potřeb Zadavatele (uživatelské, administrátorské),

- integrace úprav v technologickém rámci stávajícího prostředí CS, se zohledněním bezpečnostních požadavků, vyplývajících z kybernetického zákona a z požadavků bezpečnostního systému CS.

Následující kapitoly popisují požadavky na systém cPortál (Transakční portál pro elektronická podání), požadavky na jeho další rozvoj, jeho vývojovou modernizaci a nasazení do provozního prostředí, další navazující rozvoj, předpokládané přínosy projektu, jednotlivé části řešení (věcné a technické požadavky na nové řešení).

Specifikaci zadání pro systém cPortál (vývojová modernizace) musí Dodavatel považovat za specifikaci rámcovou, která bude upřesněna v rámci fáze analýzy Dodavatelem.

Modernizovaný systém cPortál bude spolupracovat s dalšími navazujícími systémy, které jsou reálně provozované aplikační systémy, které podléhají provozním a vývojovým změnám vyplývajícím ze změn legislativy, oprav chyb atp. Možné navýšení pracnosti realizace díla, vyplývající z analytického zpřesnění touto technickou specifikací definovaného zadání, musí být, proto zohledněno již v nabídce a zahrnuto v celkové ceně uvedené v nabídce.

1.2 Technická podpora

Technickou podporou se rozumí zejména:

- Instalace, resp. implementace produktů do testovacího prostředí, včetně ověření funkčnosti a nastavení,
- zapracování požadovaných grafických změn pro zobrazování výstupních dat na obrazovkách, většinou na základě změny logických datových vazeb,
- zapracování požadovaných grafických změn zobrazování výstupních dat v tiskových sestavách, většinou na základě změny logických datových vazeb,
- zajištění procesů testování nových verzí aplikací na straně zhotovitele a podporu a konzultaci testovacích procesů na straně objednatele,
- zajištění instalací na testovací prostředí a případně součinnost při instalacích na provozní prostředí informačního centra CS,
- aplikační zajištění monitoringu běhu aplikací, analýza a vyhodnocování logů aplikací, a spolupráce při zajištění plánovaných i neplánovaných nedostupností jednotlivých SW komponent. Monitoring je zajištěn rozsahem oprávnění přístupu do testovacího a provozního prostředí, (viz v čl. 2.6),
- úpravy databázových struktur, včetně přechodu používaného SW na nové verze (podle rozsahu) či produkty,
- provádění úprav stávajících funkčností, které vyplývají z legislativních změn, souvisejících procesních změn nebo požadavků uživatelů, ale nepřinášející funkčnosti nové,
- provádění úprav rozhraní uvedených programových produktů k nově vyvinutým aplikacím, případně k nově vyvinutým verzím již existujících aplikací třetích stran, a to na základě plánovaných nebo operativních požadavcích objednatele,
- provádění úprav stávajících funkčnosti na základě provozních potřeb vyplývajících z hlášení provozních problémů z aplikace SŘZ,

- úpravy a nastavení funkčností odpovídající vývoji aplikace v omezeném rozsahu,
- zajištění aktualizace zhotovitelem vytvořené technické a uživatelské dokumentace v souvislosti s prováděnou technickou podporou,
- zajištění provozní podpory (odstraňování závažných technických problémů) a správy databází uvedených programových produktů,
- zajištění úprav aplikace, programového produktu na testovacím prostředí a případně součinnost při úpravách na provozním prostředí objednatele, na základě změn v prostředí objednatele, jak z důvodu přechodu na vyšší verze, tak i z důvodu změny HW, SW i s vazbou na prostředí třetích subjektů,
- zajištění chodu aplikace, programového produktu v prostředí objednatele na testovacím prostředí a případně součinnost při úpravách na provozním prostředí, jak z důvodu přechodu na vyšší verze, tak i z důvodu změny HW, SW i s vazbou na prostředí třetích subjektů,
- pravidelná i nepravidelná osobní jednání zhotovitele a objednatele, písemné a telefonické konzultace, školení k chodu systému
- zajištění funkčností aplikace v rozsahu definovaných stavů kvality a parametrů pro hodnocení funkčností systému jako bezproblémové,
- analytická a procedurální podpora provozu (diagnostika a návrh řešení nestandardních stavů a jednotlivých problémů uživatelů pro garanty objednatele, podpora při tvorbě vnitřních aktů řízení, aby odpovídaly navrženým procesům, které jsou či budou implementovány v aplikaci a případně budou upravovány během úprav),
- zajištění vstupních analýz nákladovosti požadavků na vývoj aplikace, předběžné vývojové konzultace,
- stanovení plánu vývojových, rozvojových prací s objednatelem
- schválení dílčích objednávek rozvoje
- při změně, aktualizaci nebo přechodu na vyšší verzi operačních systémů bude v rámci díla zaměstnanci zhotovitele provedeno testování vlivu takové změny na aplikace v příloze č.1, na testovacím prostředí a případně na provozním prostředí objednatele umístěného v informačním systému celní správy (dále jen „ISCS “).
- úpravy databázových struktur a jejich optimalizace, která zabezpečí efektivní provoz s co nejmenšími technickými nároky,
- zabezpečení kompatibility dat ve vztahu k datům v databázi evropského systému, je-li aplikace na evropské systémy napojena,
- vytvořit dokumentaci, dle definovaného zadání:
  - pro modelování architektury informačních systémů a aplikací (SW) ve frameworku ArchiMate(verze ArchiMate 2.0., ArchiMate 3.0. a další),
  - pro modelování Use Case diagramů v UML grafickém jazyce (verze 2.5 a další),
  - pro modelování procesů BPMN notaci (verze 2.0 a další).
- plnění Ansa aplikace (Ansa, Servery) příslušnými soubory, dle definovaného zadání,
- zpracování datového modelu a jeho průběžná aktualizace,
- při přechodu na nový informační systém zajistit součinnost při migraci stávající databáze(í) do nového prostředí,
- optimalizace databáze(í) v průběhu provozního cyklu aplikace,
- popis aktuálních komunikačních rozhraní (wsdl soubory, pohledy, apod.)

Poskytování technické podpory se předpokládá v rozsahu pracovních dní a pracovní doby. V případě řešení závažných technických incidentů se řídíme podle časových specifik při řešení incidentů.

2 Systém cPortál (Transakční portál pro elektronická podání)

2.1 Popis systému cPortál

Systém cPortál vzniká na základě požadavku na eGovernment a umožní uživatelům komunikovat s Celní správou elektronicky.

Vybrané právní normy upravující kompetence Celní správy ČR s vazbou na služby poskytované cPortál:

a) zákon č. 17/2012 Sb., o Celní správě České republiky, ve znění pozdějších předpisů,

b) zákon č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů (dále jen „DŘ“),

c) zákon č.353/2003 Sb., o spotřebních daních, ve znění pozdějších předpisů (dále jen „zákon o SPD“),

d) zákon č. 261/2007 Sb., o stabilizaci veřejných rozpočtů „Energetické daně“ ve znění pozdějších předpisů,

e) zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů ve znění pozdějších předpisů (dále jen „rozpočtová pravidla“),

f) speciální zákony upravující dělenou správu,

g) zákona 365/2000 Sb. o Informačních systémech veřejné správy,

h) nařízení Evropského parlamentu a Rady (EU) č. 952/2013 ze dne 9. října 2013, kterým se stanoví celní kodex Unie (dále jen „UCC“),

i) nařízení Komise v přenesené pravomoci (EU) 2015/2446 ze dne 28. července 2015, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) č. 952/2013, pokud jde o podrobná pravidla k některým ustanovením celního kodexu Unie, v platném znění (dále jen „DA“),

j) prováděcí nařízení Komise (EU) 2015/2447 ze dne 24. listopadu 2015, kterým se stanoví prováděcí pravidla k některým ustanovením nařízení Evropského parlamentu a Rady (EU) č. 952/2013, kterým se stanoví celní kodex Unie (dále jen „IA“),

k) nařízení Komise v přenesené pravomoci (EU) 2016/341 ze dne 17. prosince 2015 kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) č. 952/2013, pokud jde o přechodná pravidla k některým ustanovením celního kodexu Unie, pokud příslušné elektronické systémy dosud nejsou v provozu, a kterým se mění nařízení v přenesené pravomoci (EU) 2015/2446 (dále jen „TDA“),

l) prováděcí rozhodnutí Komise 2014/255/EU ze dne 29. dubna 2014, kterým se zavádí pracovní program pro celní kodex Unie (dále jen „UCC WP“),

m) nařízení Rady (EHS) č. 2913/92 ze dne 12. října 1992, kterým se vydává celní kodex Společenství, publikovaným v Úředním věstníku EU L 302, 19. 10. 1992, ve znění platném k 30. 4. 2016 (dále jen „celní kodex“),

n) nařízení Komise (EHS) č. 2454/93 ze dne 2. července 1993, kterým se provádí nařízení Rady (EHS) č. 2913/92, kterým se vydává celní kodex Společenství, publikovaným v Úředním věstníku EU L 253, 11. 10. 1993, ve znění platném k 30. 4. 2016 (dále jen „prováděcí nařízení“),

o) zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „správní řád“),

p) nařízení Evropského parlamentu a Rady (ES) č. 70/2008 ze dne 15. ledna 2008, o bezpapírovém prostředí pro celnictví a obchod, v platném znění.

Obecné požadované chování systému cPortál:

cPortál má umožnit úplné elektronické podání a elektronickou komunikaci směrem k CS fyzickým (tuzemci i cizozemci) a právnickým osobám, orgánům veřejné moci, případně ověření identity vůči Evropské unii. Ve své konečné podobě prezentuje informace pro stávající System-To-System (S2S) komunikaci, a zajišťuje komunikaci rozhraním pro User-To-System (U2S) komunikaci, prostřednictvím inteligentních formulářů. Podání pomocí elektronických formulářů a poskytované webové služby pro komunikaci s informačními systémy CS zajišťují požadované služby eGovernmentu.
cPortál umožnuje autentizaci uživatelů všemi legislativně stanovenými způsoby včetně propojení s evropským autentizačním portálem, využití vybraných centrálních sdílených služeb státu (IS Datových schránek, Základní registry, Portál veřejné správy).
cPotál nepodporuje propojený datový fond (PPDF/eGSB) ani jednotnou identifikační platformu pro zaměstnance veřejné správy (JIP/KAAS), napojení na eGSB je také řešeno jinými technickými prostředky).
Mandátní rejstřík u přihlášených osob dohledá u osoby její oprávnění, či oprávnění jí udělená jinými osobami a tyto oprávnění vypíše. Přihlášený uživatel se dále rozhodne, v rámci kterého oprávnění bude v cPortál vystupovat. Přihlášené osoby si sami spravují svá oprávnění, oprávnění svých zaměstnanců a zavedení certifikátů pro elektronickou komunikaci.
cPortál má umožnit poskytnout uživatelům privátní prostor pro zobrazení informací o vlastních podáních a stavu jejich vyřízení a umožnit autorizaci, tedy ověření přístupových práv do aplikací a zajistit přístupy do těchto aplikací na základě jediné autentizace. Systém cPortál byl nasazen na testovací prostředí k 30. 6. 2019 a na provozní prostředí v září 2019 a v současné době obsahuje pouze omezené množství služeb.

Provozní stav:

Celní správa ČR v současné době provozuje k systému cPortál ještě původní web Celní správy. Systém cPortál má nahradit původní web Celní správy. Systém cPortál má poskytnout nepřihlášeným uživatelům informace k oprávněním celní správy podle jednotlivých oblastí kompetencí a formuláře. Přihlášeným uživatelům systém cPortál umožňuje podávat e-formuláře a umožňuje služby daňové informační schránky (DIS).

V rámci předchozí předchozího projektu byla pořízena platforma cPortál jako řešení, která umožní úplné elektronické podání. Jedná se o webovou aplikaci, která je umístěna na cloudu. Platforma umožňuje přihlášení uživatele prostřednictvím Národní identitní autority (NIA), tj. včetně přihlášení bankovní identitou nebo pomocí přístupu k Informačnímu systému datových schránek (ISDS). Služba cPortálu tgz. „Mandátní rejstřík" dohledá u uživatele jeho oprávnění v rejstřících. Zjistí, zda je např. jednatelem, advokátem, insolvenčním správcem, daňovým poradcem, či podnikající fyzickou osobou. Zároveň umožňuje nastavit zastupování v celkovém, či přesně vymezeném rozsahu specifikovanému pro jednotlivé aplikace, formuláře, oprávnění apod.

Mimo speciálních formulářů (např. daňových přiznání, jednotné celní deklarace, či intrastatu atd…) byl zapracován formulář obecného podání. Pokud učiní uživatel elektronické podání, tak je mu dostupný dokument – potvrzení o elektronickém úkonu a má možnost nahlížet do spisové služby a na osobní daňový účet u celního řízení.

U celního řízení poskytuje cPortal nápovědu pomocí „umělé inteligence" tgz. Celničkou. Tato služba pomáhá uživateli v procesu projednání zboží v příslušném celním režimu.

2.1.1 Popis modulů:

Úvodní obrazovka v současnosti obsahuje tři rozcestníky (Mohu vyřídit, Moje záležitosti, Nejčastěji se řeší) s jednotlivými odkazy podle daného zaměření, které pak mohou vést na další rozcestníky. Přidání dalších odkazů do rozcestníků není nijak omezeno.

1) Mohu vyřídit (obsahuje karty)

A. Clo, se dělí na:

- **Přehled celních prohlášení (rozděleno na dovoz, vývoz)**
- **Celní řízení (rozdělení na oblasti - EORI, AEO, CDS (Trade Portal), eCeP, Ostatní k celnímu řízení)**
- **Původ Zboží**
- **Sazební zařazení**
- **Problematika TARICu a kvót**
- **Zkoušky profesní způsobilosti podle celních předpisů**
- **Surové diamanty**

B. **Daně, se dělí na:**

- **Spotřební daně (rozdělení na oblasti – Přiznání daně, Uplatnění nároku na vrácení daně, Registrace k daním, Povolovací řízení, Zvláštní minerální oleje, Surový tabák, Doprava VV, Evidence ke spotřebním daním, Ostatní ke spotřebním daním, Zahřívané tabákové výrobky)**
- **Energetické daně**
- **Distributoři PHM**
- **Značení a distribuce lihu**
- **Biopaliva**
- **Bankovní záruky - vzory**

C. **Ostatní, se dělí na:**

- **Intrastat**
- **Hazardní hry**
- **Převoz peněžní hotovosti**
- **Mák a konopí**
- **Dražby**
- **Duševní vlastnictví**

2) Moje záležitosti

- **Náhled do spisu**
- **Vydaná povolení**
- **Placení daní (rozdělené na oblasti – Moje přeplatky a nedoplatky, Náhled na ODÚ, Úlevy při placení daní)**

3) Nejčastěji se řeší

- **Intrastat**
- **eCeP (rozdělení na části – Vytvoření celního prohlášení, Přehled celních prohlášení, Zjednodušené zařazení zboží)**
- **EORI**

2.2 Obecné principy evidence dat v cPortál

Základní myšlenka digitalizace Celní správy ČR je na jednom místě umožnit odkudkoliv zakládat transakce, mít možnost komunikovat bez nutnosti osobní návštěvy úřadu. K tomuto účelu je budován systém cPortál.

Systém cPortál zajišťuje transakce dat ze zdrojových evidenci, případně data založená do cPortál předává do zdrojových evidencí, či jednotlivá podání zakládá do spisové služby. Aby k této transakci mohlo dojít, musí být uživatel přihlášen do systému cPortál.

Nepřihlášený uživatel má možnost nahlížet do jednotlivých oblastí podle karet (clo, daně.....) a formulářů. Není mu umožněno prostupovat do napojených systémů či nahlížet na data.

Systém cPortál neobsahuje databázové struktury zdrojových evidencí a ani z dat zdrojových evidencí nevytváří žádné nové datové struktury. Data jsou v systému cPortál po zadání příslušné transakce znázorněna v dané masce, nebo předána v čitelném formátu uživateli k dalšímu zpracování.

2.3 Vstupy do aplikace

Systém cPortál je napojen na NIA i na ISDS a systém základních registrů prostřednictvím aplikace CRS (Centrální registr subjektů) a veškeré ověřování subjektů je prováděno vůči těmto registrům. S ohledem na směrnici k GDPR komunikují systémy CS pouze s „klíčí subjektu“ místo osobních údajů. Předávaná data jsou anonymizována. Systém cPortál bude klíče subjektu překládat prostřednictvím aplikace CRS. Systém zpracovává a předává data do dalších systémů ISCS:

- CEPAN: CEPAN předkládá informace o přeplatcích a nedoplatcích;
- ECDC: ECDC data pro ODÚ (finančně platební) z dovozu zboží;
- Datový sklad: datový sklad předává sestavy pro dovoz a vývoz zboží bez platební části;
- eSAT: eSAT umožňuje nahlížet do spisu a vystavuje potvrzení o digitálním úkonu
- CEPP (předchozí systém CEPAN) bude poskytovat pouze informace předané ze zdrojových evidencí VSD, ECDC, MED, daňové správy a CRS. Funguje jako „kukátko“. Uživatelům informace sumarizuje přehledným způsobem v aplikačním výstupu.

2.4 Výstupy z aplikace

Systém cPortál poskytuje uživatelům informace třemi výstupy. Jedná se o zobrazení dat na obrazovce, do dokumentu (sestavy, podání, rozhodnutí) a formou datového výstupu (může obsahovat strukturovaná data, ale i tiskové výstupy ve formátu PDF):

- Obrazový výstup bude výsledkem zadání uživatele pro konkrétní datový výběr podle příslušného oprávnění a řešeného tématu v dané kartě. Každý další výběr rozšiřující původní volbu je detailnější.
- Sestavy, podání a rozhodnutí jsou součástí jednotlivých témat a karet. Systém cPortál automaticky u přihlášených uživatelů e-formuláře automaticky vyplňuje hlavičkové údaje, včetně zastupování.

- Datové výstupy jsou realizovány formou webových služeb. Datové výstupy obsahují stejné údaje jako zdrojové evidence, popř. jsou předány ve formě uzavřeného souboru ve formátu excel. Rozsah předávaných dat je nastaven podle oprávnění systému ve webové službě.

Clo poskytuje základní informace a služby vztahující se k dovozu/vývozu zboží ze/do zemí mimo EU, se dělí na:
Přehled celních prohlášení (rozděleno na dovoz, vývoz) - Přehled celních prohlášení je možné získat u dovozu a vývozu zboží v příslušné části výběru při vyplnění povinných údajů, které je možné dále zpřesnit volitelnými údaji. Výběr bude vygenerován ve formátu určeném pro stažení přehledu.
Celní řízení (rozdělení na oblasti - EORI, AEO, CDS (Trade Portal), eCeP, Ostatní k celnímu řízení) - Při celním řízení rozhodují celní orgány na základě podaného celního prohlášení o tom, zda bude zboží propuštěno na celní území EU nebo zda toto území opustí, případně prostřednictvím jakého celního režimu. Při té příležitosti se stanoví příslušné poplatky a rovněž se kontroluje, zda jsou dodržovány všechny příslušné zákazy a omezení při dovozu, vývozu a tranzitu zboží. Před zahájením celního řízení je nutné nejprve získat číslo EORI. Obdržet lze rovněž různá povolení a zjednodušení. Dělíme dále na:
EORI - Číslo EORI slouží jako jedinečný identifikátor hospodářského subjektu pro následnou komunikaci s celními orgány všech členských států Evropské unie. Před podáním celního prohlášení nebo před podáním žádosti o rozhodnutí se hospodářský subjekt musí registrovat u celních orgánů.
AEO - Hospodářské subjekty, tj. právnické nebo podnikající fyzické osoby, dovážející nebo vyvážející zboží ze/do třetích zemí, mohou získat povolení (status) tzv. Oprávněného hospodářského subjektu (AEO).
CDS - Centrální Systém Customs Decisions (CDS) je používán pro všechny žádosti a povolení, které mohou mít dopad ve více než jednom členském státě Evropské unie a pro jakékoli následné události, které se takové žádosti či povolení týkají (zrušení, zamítnutí, pozastavení, změny).
eCep - eCeP je aplikace pro podávání elektronického celní prohlášení, jehož prostřednictvím umožňuje nepodnikajícím fyzickým osobám přímé (vlastní) celní odbavení tzv. zásilek e-commerce. Jde o zásilky v hodnotě do 150 EUR např. z e-shopu, ale i o dary od nepodnikajících fyzických osob.
Ostatní k celnímu řízení - Formuláře, kterými je možné podat příslušnému celnímu úřadu např. žádost o vrácení/prominutí cla, žádosti o povolení celního zjednodušení, žádosti o povolení zvláštního režimu a další žádosti související s režimem tranzitu.
Původ Zboží - Prokázáním původu zboží v zemi, s níž má EU uzavřenu příslušnou dohodu, lze v celním řízení použít pro hospodářský subjekt výhodnější celní sazbu
Sazební zařazení - Z obecného hlediska je sazebním zařazením zboží stanovení kódu nomenklatury celního sazebníku, do níž má být dané zboží zařazeno.
Problematika TARICu a kvót - TARIC (Integrovaný tarif Evropské unie) je nástroj určený k přehledu a aplikaci celních sazeb a zákazů a omezení při dovozu a vývozu zboží do/z Evropské unie. Součástí problematiky TARICu jsou celní kvóty, které pro určité vymezené období stanovují množství zboží, po které je dané zboží propouštěno do volného oběhu v EU za sníženou celní sazbu.
Zkoušky profesní způsobilosti podle celních předpisů - e-learningový modul celní problematiky pro subjekty, jehož úspěšné absolvování umožní subjektům splnění podmínky

profesní způsobilosti dle čl. 39 celního kodexu Unie a čl. 27 prováděcího nařízení Komise, která je jednou z podmínek pro vydání povolení AEO, souborné jistoty a některých dalších celních zjednodušení.
Surové diamanty - Registrace subjektů obchodující se surovými diamanty v rámci dovozu a vývozu ze třetích zemí, včetně podávání pravidelného hlášení.

Daně poskytují informace, formuláře a aplikace pro poskytování digitálních služeb v oblasti spotřebních a energetických daní, zvláštních minerálních olejů, surového tabáku, distribuce pohonných hmot, značení a distribuce lihu, biopaliv a dopravy vybraných výrobků, se dělí na:
Spotřební daně (rozdělení na oblasti – Přiznání daně, Uplatnění nároku na vrácení daně, Registrace k daním, Povolovací řízení, Zvláštní minerální oleje, Surový tabák, Doprava VV, Evidence ke spotřebním daním, Ostatní ke spotřebním daním, Zahřívané tabákové výrobky) - Předmětem spotřebních daní jsou minerální oleje, líh, pivo, víno a meziprodukty, tabákové výrobky, surový tabák a zahřívané tabákové výrobky. Dále dělíme na:
Přiznání daně - Formuláře služeb CS spojených s podáním přiznání ke spotřebním daním, registrací cen cigaret, objednáním tabákových nálepek a oznámením o nevzniknutí daňové povinnosti.
Uplatnění nároku na vrácení daně - Formuláře služeb CS k uplatnění nároku na vrácení daně (diplomati, NATO, minerální oleje) a žádost o úřední dozor nad zničením tabákových nálepek.
Registrace k daním - Formuláře služeb CS pro registraci ke spotřebním daním, jakož i změnu registračních údajů a zrušení registrace
Povolovací řízení - Formuláře služeb CS k žádostem o vydání a změnu povolení dle zákona o spotřebních daních či jejich zrušení
Zvláštní minerální oleje - Formuláře služeb CS pro registraci k nakládání se zvláštními minerálními oleji (oleje s vymezenými vlastnostmi), žádost o změnu registrace či její zrušení a Formuláře služeb CS spojených s plněním oznamovacích povinností při nakládání se zvláštními minerálními oleji, včetně vzoru evidence.
Surový tabák - Formuláře služeb CS k registraci a k přiznání daně ze surového tabáku, k registraci ke skladování surového tabáku, plnění oznamovacích povinností, vzor evidence a další související
Doprava VV - Formuláře a aplikace služeb CS využívaných pro dopravu vybraných výrobků po ČR a EU, a to ve volném daňovém oběhu i v režimu podmíněného osvobození od daně a s tím související informace
Evidence ke spotřebním daním - Vzory pro vedení evidencí dle zákona o spotřebních daních – univerzální i pro jednotlivé komodity (vybrané výrobky)
Ostatní ke spotřebním daním - Formuláře služeb CS vztahující se dalším kompetencím CS v oblasti spotřebních daní
Zahřívané tabákové výrobky - Formuláře CS z oblasti zahřívaných tabákových výrobků, registrace k dani, oznámení o změně registračních údajů, přiznávání daně.
Energetické daně - Předmětem energetických daní je plyn (zemní, bioplyn a další), elektřina a pevná paliva (hnědé a černé uhlí, koks, rašelina a další).
Distributoři PHM - Formuláře služeb CS k registraci distributora pohonných hmot a plnění oznamovací povinnosti ve vztahu k nákupu a prodeji PHM
Značení a distribuce lihu - Formuláře služeb CS pro registraci osoby povinné značit líh a distributora lihu, včetně objednávky kontrolních pásek.

Biopaliva - Formuláře služeb CS pro plnění povinností dle zákona o ochraně ovzduší vztahujících se k biopalivům zahrnující oznámení o dopravě/dovozu PHM s biopalivem, hlášení o splnění objemové biopovinnosti a zprávu o emisích.
Bankovní záruky – vzory - Vzory bankovních záruk a jejich dodatků pro potřeby spotřebních daní, povinného značení lihu a distributorů pohonných hmot.

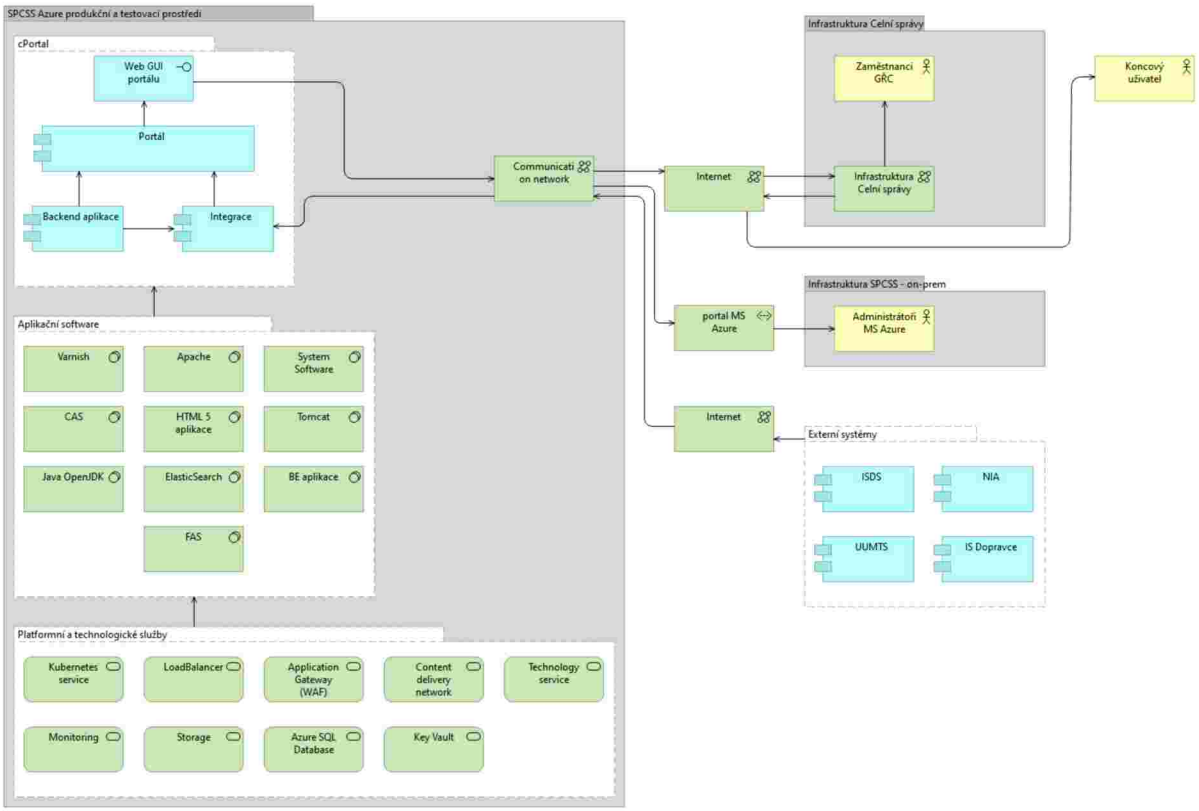
Ostatní poskytují informace, formuláře a aplikace pro poskytování digitálních služeb v oblasti Intrastatu, hazardních her, pěstování máku a konopí a dražeb realizovaných CS ČR a možnost stažení formuláře pro splnění oznamovací povinnosti v oblasti opatření proti legalizaci výnosů z trestné činnosti., se dělí na:
Intrastat - Aktuální informace o systému statistiky obchodu se zbožím mezi Českou republikou a ostatními členskými státy Evropské unie - Intrastatu-CZ.
Hazardní hry - Celní správa je orgánem státního dozoru a orgánem příslušným k projednání přestupků v oblasti hazardních her.
Převoz peněžní hotovosti - Celní úřady provádí dozor v oblasti převozu peněžní hotovosti z nebo do České republiky z oblasti mimo území Evropské unie.
Mák a konopí - Osoby pěstující mák setý nebo konopí na celkové ploše větší než 100 m2 jsou povinny předat hlášení místně příslušnému celnímu úřadu podle místa pěstování, písemně nebo v elektronické podobě.
Dražby - CS ČR realizuje daňové dražby podle Daňového řádu u zboží, které propadlo v souvislosti se správou daní a současně veřejné dražby svého nepotřebného vyřazeného majetku.
Duševní vlastnictví - Celní správa České republiky se ve spolupráci s majiteli práv podílí na vymáhání průmyslových práv, autorských a souvisejících práv.
Podání trestního oznámení – pověřený celní orgán je příslušný vést trestní prověřování, jedná-li se o vybrané trestné činy spáchané porušením celních a daňových předpisů.
Ostatní podání – ostatní podání ke službám jinde nezařazeným.

2.4.1 Tiskové sestavy

Tiskové sestavy budou v systému cPortál zajištěny u všech formulářových řešení, kdy bude uživatel mít možnost daný elektronický dokument převést do formátu PDF a ten si následně vytisknout. V případě datových výběrových sestav budou tato převedena do excelu.

2.5 Technický popis aplikace

Logický model



Přístupová vrstva

Systém cPortál je provozován v prostředí MS Azure SPCSS ve dvou samostatných subskripcích (P064-21 GŘC C Portál a P064-21 GŘC C Portál Dev/Test) . Jedna je určená pro testovací část a druhá pro produkční prostředí. Obě prostředí jsou uživatelům přístupná prostřednictvím infrastruktury Generálního ředitelství cel (dále jen GŘC). Propojení mezi GŘC a prostředím MS Azure je zajištěno pomocí šifrovaného site-2-site IPSEC VPN tunelu.

Prezentační vrstva

Vlastní aplikace cPortal je nasazena v MS Azure v kontejnerizovaném prostředí Kubernetes. Nasazení a provoz aplikace spadá do kompetence dodavatelské společnosti Asseco.

Aplikační vrstva

Infrastruktura pro aplikační vrstvu je rozdělena na dvě části do samostatných subskripcí (viz 0 **Přístupová vrstva**) pro produkci a pro test, jak již bylo řečeno a je provozována na open source platformě LifeRay CE. Aplikační vrstvu spravuje společnost Asseco (stávající dodavatel).

Databázová vrstva

Jako databáze je v prostředí testovací subskripce použit zdroj SQL databáze, zatím co v produkčním prostředí je použito SQL – Managed instance.

Datová úložiště

Jako datové úložiště pro ukládání logů a errorpages je v prostředí MS Azure použit standardní StorageAccount kdy na testovacím i produkčním prostředí má celkovou sdílenou kapacitu 5TB a retenci uchování dat 18 měsíců.

Formulářové úložiště

Jako formulářové úložiště slouží redakční systém cPortálu, který je napojen na FAS Server společnosti SW 602, který zajišťuje digitalizaci formulářů a jejich služeb. Správu FAS Serverů zajišťuje společnost Asseco (stávající dodavatel).

Autentizace a autorizace uživatelů se bude provádět pomocí sdílené komponety CAS, která v rámci cPortálu zajišťuje všechny druhy autentizace a poskytuje informace o přihlášeném uživateli pomocí JWT tokenu.

Pro komunikaci mezi jednotlivými systémy bude použito webových služeb (SOAP), které budou mít svůj předpis definován pomocí WSDL, vůči kterému bude možné validovat příchozí a odchozí zprávy.

Aplikace cPortálu jsou postavené jako více vrstvé. Běhové prostředí Azure Kubernetes cluster.

Databáze:
- SQL Azure 12.0.2000.8

Backendy (včetně integračních):
- Tomcat: 9.0.63.0
- Java: 11.0.1+13 (postaveno nad Spring frameworkem)

Frontend:
- Apache: 2.4.54
- Polymer 3

CAS (přihlašení):
- Tomcat: 9.0.63.0
- Java: 1.8.0

Portál (redakční systém):
- Liferay: 7.3.6-ga7
- Elasticsearch: 7.13.1

Cache:
- Varnish: 6.3

Komunikace interní i externí probíhá výhradně pomocí webových služeb (SOAP nebo REST).

2.6 Prostředí systému cPortál

Systém cPortál bude provozován v minimálně dvou prostředích a to:
- Produkční
- Testovací

Pro potřebu vývoje, nastavení, optimalizaci atd., je možné na omezenou dobu vytvořit další prostředí systému cPortál (např. zrcadlo). Testovací prostředí neobsahuje provozní (produkční) data. Testovací data vyrábíme v testovacím prostředí s použitím testovacích subjektů. Testovací prostředí se propojuje s testovacím prostředím dalších systémů. Testovací prostředí nebude veřejně dostupné, je určené jen pro uživatele ze sítě CS a dodavatele.
Provozovaná prostředí systému cPortál jsou umístěny na cloudu v AZURE.

2.7 Požadavky na dostupnost systému cPortál

Systém bude dostupný v režimu 7x24 s povolenými plánovanými servisními odstávkami uvedenými v kapitole 2.8. V době mimo plánované servisní odstávky činí požadovaná dostupnost:

- 99,5 % na roční bázi (tj. maximální celková přípustná doba nedostupnosti za kalendářní rok činí 44 hodin)
- 98,9 % na měsíční bázi (tj. maximální celková přípustná nedostupnosti za kalendářní měsíc činí 8 hodin).

Požadovaná provozní doba, jako období, kdy musí být zajištěny všechny služby související s provozem systému a nesmí být plánovány servisní odstávky je 5x10 hodin, tedy v pracovní dny mezi 6. a 18. hodinou.
Nasazování oprav a verzí aplikací objednatelem není považováno za servisní odstávku.

2.8 Servisní odstávky systému cPortál

Servisní odstávky budou přípustné v maximálním rozsahu 96 hodin ročně. Jednotlivá servisní odstávka nesmí přesáhnout 24 hodin.

Servisní odstávky musí být realizovány mimo nadefinovanou provozní dobu systému a mimo období požadované zvýšené dostupnosti. Zvýšená dostupnost bude v období mezi 10 až 20 dnem v měsíci a poslední dva pracovní dny v měsíci a první pracovní týden nového měsíce. Přednostně by pro servisní odstávky měly být využívány víkendy a svátky.

Typy servisních odstávek

- plánované servisní odstávky
- mimořádné servisní odstávky

Plán servisních odstávek a období zvýšené dostupnosti bude sestaven vždy na celý kalendářní rok a včas předložen ke schválení Zadavatelem.

Mimořádné servisní odstávky, kromě odstávek pro řešení havarijních stavů, musí být plánované minimálně jeden týden předem a oznámeny uživatelům formou publikování informací v cPortál.

2.9 Požadavky na realizaci díla – přístup do ISCS

Ke všem implementovaným prostředím na cloudu v AZURE bude Dodavateli poskytnut vzdálený přístup pomocí VPN, nebo jako přístup jednotlivých rolí Dodavatele s využitím PC klientů a dvoufaktorové autentizace. Podporovaná technologie je Cisco VPN (Cisco

Anyconnect). Konkrétní nastavení propojení sítí bude po dohodě s Dodavatelem. Přístupová oprávnění a role dodavatele zajišťuje objednatel u provozovatele cloudu.

Umístění pracovníků Dodavatele v prostorách CS, kromě pracovníků podpory Dodavatele pro účely post implementační podpory nebo školení pracovníků CS, se nepředpokládá.

2.10 Bezpečné propojení a připojení k Internetu

Systém cPortál je provozován na cloudu v AZURE. Bezpečné propojění a připojení k internetu řeší provozovatel cloudu.

2.11 Poskytování výpočetního výkonu

Aplikace je provozována v cloudovém prostředí Azure, který je nakonfigurován s vysokou dostupností. Pro možnosti využití horizontálního škálování bude implementace založena na kontejnerovém řešení Kubernetes, které zajistí interní vysokou dostupnost pomocí balancování dotazů. Aktuální verze Kubernetes je 1.20

Produkční prostředí

Service type	Region	Description
Azure Kubernetes Service (AKS)	West Europe	7 D8s v4 (8 vCPU, 32 GB RAM) uzlů; Rezervované na 3 roky; 0 spravovaných disků s operačním systémem – S4, 0 clusterů
Storage Accounts	West Europe	Block Blob Storage, Obecné účely V2, redundance LRS, Vrstva přístupu Hot, Kapacita 100 GB - Platˇte jenom za to, co využijete, 100 000 operací zápisu, 100 000 operací výpisu a vytvoření kontejneru, 100 000 operací čtení, 100 000 operací čtení z archivu s vysokou prioritou, 1 dalších operací Načítání dat: 1 000 GB, načítání z archivu s vysokou prioritou: 1 000 GB, zápis dat: 1 000 GB
Storage Accounts	West Europe	Block Blob Storage, Blob Storage, redundance LRS, Vrstva přístupu Hot, Kapacita 10 GB - Platˇte jenom za to, co využijete, 100 000 operací zápisu, 100 000 operací výpisu a vytvoření kontejneru, 100 000 operací čtení, 100 000 operací čtení z archivu s vysokou prioritou, 1 dalších operací Načítání dat: 1 000 GB, načítání z archivu s vysokou prioritou: 1 000 GB, zápis dat: 1 000 GB
Key Vault	West Europe	Trezor: 10 000 operací, 0 pokročilých operací, 0 obnovení, 0 chráněných klíčů, 0 pokročilých chráněných klíčů za měsíc; spravované fondy HSM: 0 fondů HSM Standard B1 × 730 Hodin

Content Delivery Network		Zóna 1: 500 GB, Zóna 2: 0 GB, Zóna 3: 0 GB, Zóna 4: 0 GB, Zóna 5: 0 GB, DSA: 0 GB
Azure Monitor	West Europe	Počet ingestovaných GB: 30, počet vícekrokových webových testů: 0
Application Gateway	West Europe	Úroveň Web Application Firewall, velikost instance Střední: 1 instancí hodin brány × 730 Hodin, 1 TB jednotek zpracování dat, 500 GB jednotek zóny

Testovací prostředí

Service type	Region	Description
Azure Kubernetes Service (AKS)	West Europe	3 D8s v4 (8 vCPU, 32 GB RAM) uzlů; Rezervované na 3 roky; 0 spravovaných disků s operačním systémem – S4, 0 clusterů
Storage Accounts	West Europe	Block Blob Storage, Obecné účely V2, redundance LRS, Vrstva přístupu Hot, Kapacita 100 GB - Platťe jenom za to, co využijete, 100 000 operací zápisu, 100 000 operací výpisu a vytvoření kontejneru, 100 000 operací čtení, 100 000 operací čtení z archivu s vysokou prioritou, 1 dalších operací Načítání dat: 1 000 GB, načítání z archivu s vysokou prioritou: 1 000 GB, zápis dat: 1 000 GB
Storage Accounts	West Europe	Block Blob Storage, Blob Storage, redundance LRS, Vrstva přístupu Hot, Kapacita 10 GB – Platťe jenom za to, co využijete, 100 000 operací zápisu, 100 000 operací výpisu a vytvoření kontejneru, 100 000 operací čtení, 100 000 operací čtení z archivu s vysokou prioritou, 1 dalších operací Načítání dat: 1 000 GB, načítání z archivu s vysokou prioritou: 1 000 GB, zápis dat: 1 000 GB
Key Vault	West Europe	Trezor: 10 000 operací, 0 pokročilých operací, 0 obnovení, 0 chráněných klíčů, 0 pokročilých chráněných klíčů za měsíc; spravované fondy HSM: 0 fondů HSM Standard B1 × 730 Hodin
Content Delivery Network		Zóna 1: 10 GB, Zóna 2: 0 GB, Zóna 3: 0 GB, Zóna 4: 0 GB, Zóna 5: 0 GB, DSA: 0 GB
Azure Monitor	West Europe	Počet ingestovaných GB: 20, počet vícekrokových webových testů: 0
Application Gateway	West Europe	Úroveň Web Application Firewall, velikost instance Střední: 1 instancí hodin brány × 730 Hodin, 10 GB jednotek zpracování dat, 10 GB jednotek zóny

2.12 Poskytování diskového prostoru

Požadované řešení bude využívat diskový prostor v cloudu (Storage). Součástí detailní analýzy pak musí být specifikace, o kolik ho bude třeba navýšit pro nové komponenty v jednotlivých prostředích.

2.13 Správa operačních systémů

Instalaci, konfiguraci a správu operačních systémů na úrovni fyzických i virtuálních serverů provádí provozovatel cloudu. Systém cPortál je umístěn v AZURE. Dodavatel cPortál nemá administrátorské účty k OS cloudu. Dodavatel používá pro implementaci a podporu provozu databází a aplikací uživatelské účty, využití administrátorských účtů je možné pouze se součinností CS a provozovatele cloudu. Dodavatel musí navrhnout implementaci aplikací tak, aby eliminoval, respektive snížil na minimální nutnou úroveň, nutnost použití administrátorských účtů při provozní podpoře aplikací.
SW licence OS a virtualizace jsou součástí služby cloudu. Součástí správy operačních systémů je provádění aktualizací verzí OS a virtualizačních platforem. Aktualizace aplikačního SW bude plánována ve spolupráci s Dodavatelem.

2.14 Správa databází

Správu databází bude provádět CS i v případě cloudových řešení. Administrátorské účty databází a účty vlastníků schémat jsou v rukách CS. Dodavatel může použít pro implementaci a podporu aplikací uživatelské účty, využití administrátorských účtů a účtů vlastníků schémat je možné pouze se součinností CS. Dodavatel navrhuje implementaci databází a aplikací tak, aby eliminoval, resp. snížil na minimální nutnou úroveň nutnost použití administrátorských účtů a účtů vlastníků schémat při provozní podpoře aplikací.

Součástí správy databází je provedení aktualizací verzí DB. Aktualizace SW bude plánována ve spolupráci s Dodavatelem.

2.15 SW licence a sublicence

Licence SW na úrovni operačních systémů MS Windows, databázových služeb na platformě MS SQL, virtualizační platforma VMware, zálohování a monitoringu budou dodávány jako součást provozních služeb cPortál, zajišťovaných dodavatelem. Provozní náklady, včetně případných potřebných licencí zajistí dodavatel.

Všechny SW produkty nad touto úrovní, potřebné pro vybudování a provoz cPortál, včetně aplikačních serverů, middleware a databází, jsou považovány za součást aplikačního SW a jsou součástí Díla. Zajišťuje dodavatel systému.

3 Role, výkonnost, kapacita, škálovatelnost cPortál

3.1 Role v cPortál

U systému cPortál předpokládáme nastavení oprávnění pro níže uvedené role:

Uživatelské role systému cPortál:
01 - A_TST_CPORT_Administrator: "ADMINISTRATOR"
02 - A_TST_CPORT_Editor: "EDITOR"
03 – A_TST_CPORT_Spravce_FAS: "SPRAVCE_FAS"
04 – A_TST_CPORT_Overovatel_Certifikatu: "OVEROVATEL_CERTIFIKATU"

Správce FAS měl (má) možnost přes redakční systém nahrávat formulářové soubory (.fo) pro FAS server.
Systém cPortál kontroluje přidělení rolí interním uživatelům prostřednictvím AD. Systém podle rozsahu přidělených rolí uživateli umožňuje přístupy k uživatelským operacím. Tedy ověřujeme pouze osoby objednatele a dodavatele.

3.2 Autentizace a autorizace

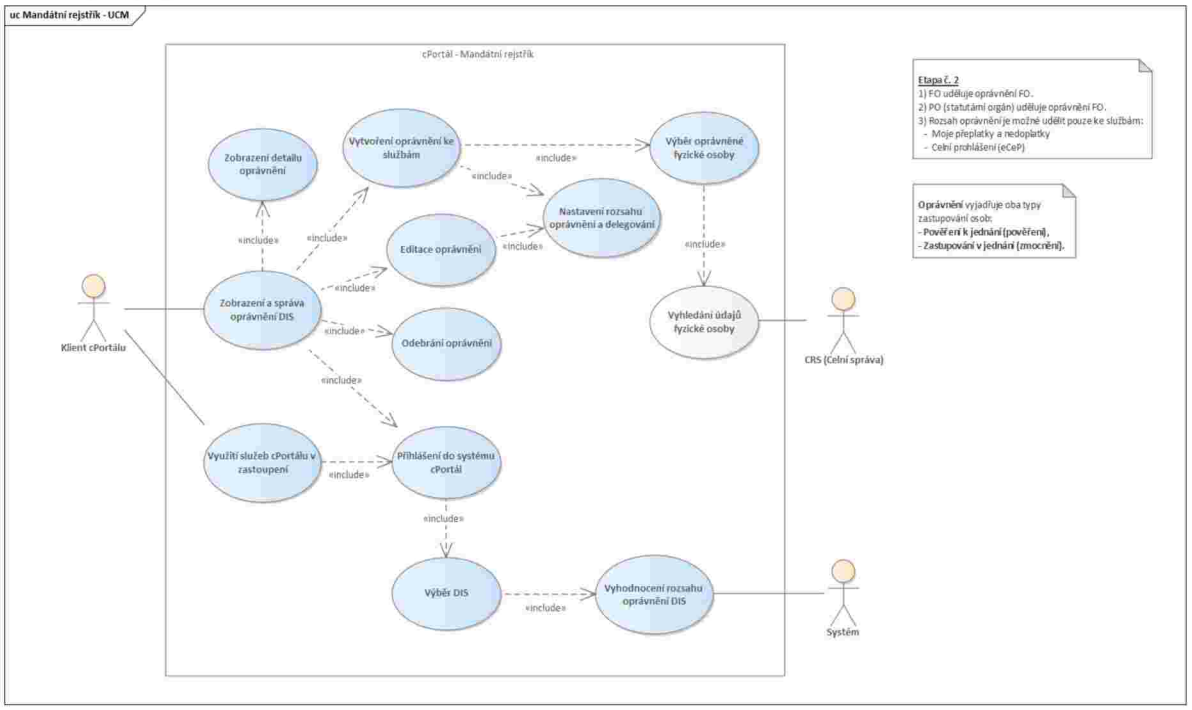
Každý interní uživatel systému z Celní správy a dodavatel musí být pro přístup do systému řádně autentizován. Autentizace probíhá přihlášením uživatele do ISCS (jméno + heslo, či kartou a PINem). Při přihlášení interního uživatele do aplikace cPortál budou zkontrolovány jeho uživatelské role z AD a zpřístupněny odpovídající části aplikace. Všechny úspěšné i neúspěšné přístupy k systému budou logovány. Záznamy o neúspěšných přístupech budou monitorovány.
Přístup veřejnosti nepřihlášeným uživatelům není omezen žádnou autorizací. Uživatel přistupuje z internetu do všech částí aplikace. Omezen je pouze v tom, že nemůže využívat služeb daňové informační schránky (podávat např. daňová přiznání, nahlížet do spisu atd…).
Veřejnost se do cPortál přihlašuje prostřednictvím identity občana, kde zvolí jemu vyhovující autorizaci.

Mandátní rejstřík:

Služba mandátního rejstříku spočívá v možnostech dohledání oprávnění přihlášené osoby, např. že je jednatelem společnosti – statutární orgán, či insolvenčním správcem, či advokátem, nebo fyzickou osobou podnikatelem atd. a zároveň umožňuje nastavit zastupování osob pro dané oblasti podle karet a oprávnění v nich až na detail použití daných formulářů.

cPortál bude umožňovat fyzickým osobám, právnickým osobám a fyzickým osobám podnikatelům elektronicky komunikovat s Celní správou ČR (dále CS) následujícími způsoby:
1) Jednání „sám za sebe“
2) Pověření k jednání
3) Zastupování v jednání

Pověření k jednání či zmocnění k zastupování v jednání uděluje osoba na cPortálu. Po přihlášení může určit, koho a v jakém rozsahu zmocňuje k zastupování či pověřuje k jednání. Následně osoba s tímto oprávněním může po svém přihlášení k cPortálu činit za osobu úkony, ke kterým ji pověřila či zmocnila.

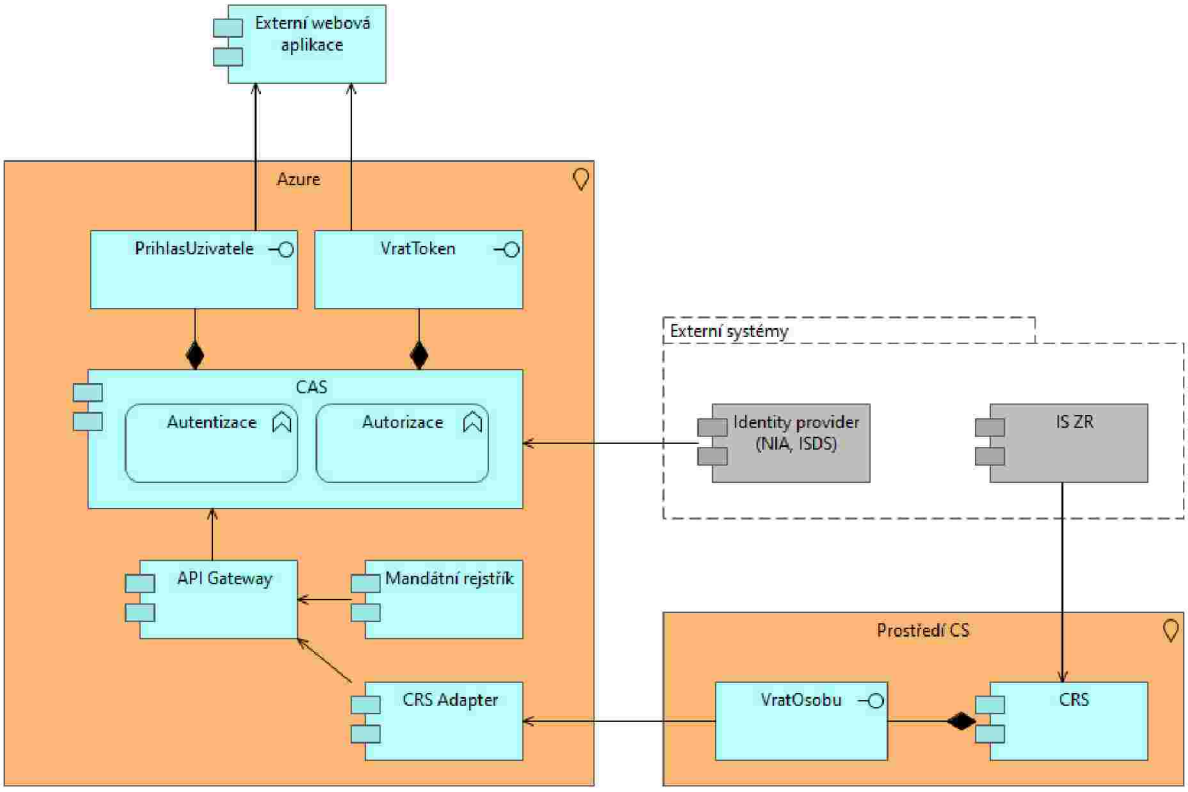


Oprávněná osoba může delegovat oprávnění na další fyzické osoby (zřetězení oprávnění), pokud je umožněno.

Tzn., že se přihlášený uživatel musí na začátku rozhodnout za jakou osobu (oprávnění) bude vystupovat a činit kroky. Systém cPortál přihlášenému uživateli vždy signalizuje, za jakou osobu jedná.

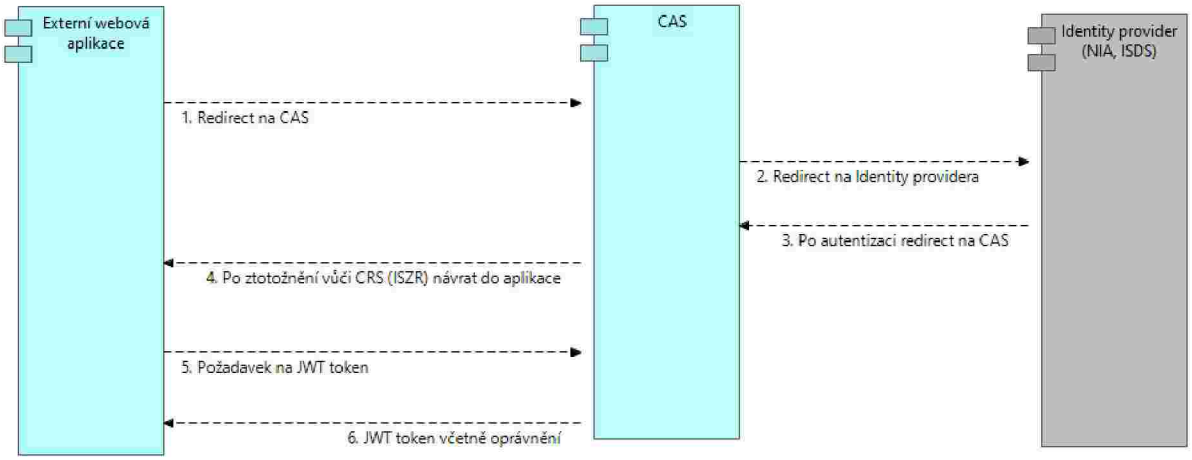
Přístup externích webových aplikací

Externí webová aplikace zavolá službu pro přihlášení a po úspěšné autentizaci vůči Identity provider (typicky NIA nebo ISDS) je uživatel přesměrován zpět do externí webové aplikace. Ta si pak může pomocí služby na vrácení JWT tokenu nechat vrátit údaje o přihlášeném uživateli včetně oprávnění, která má v rámci mandátního rejstříku.



Komunikace je popsána pomocí flow takto:

1. Externí aplikace provede zavolání GET služby pro přihlášení
   - GET /cas/login?service=<url_aplikace>
2. Uživatel je přesměrován na CAS a pokud již není v rámci svého sezení přihlášen, tak je vyzván k výběru Identity providera, kde se opět v prohlížeči přesměruje a provede svoji autentizaci.
3. Po úspěšné autentizaci je vrácen zpět na CAS v rámci přesměrování prohlížeče.
4. CAS provede ztotožnění vůči CRS (to pak případně vůči ISZR) a přesměruje v prohlížeči uživatele na URL z prvního bodu.
   - Odpověď zároveň obsahuje hlavičku Set-Cookie s cookie TGM, která je nastavena pro doménu CAS a jeho cestu /cas
5. Pro získání JWT tokenu s informacemi o uživateli externí aplikace zavolá POST službu CAS, kde se musí odeslat cookie TGM z předchozího bodu a musí odpovídat i hlavička User-agent, aby došlo ke spárování.
   - POST /cas/v1/auth/token
6. Výsledkem je vrácený JSON soubor s JWT token a informacemi o přihlášeném uživateli.



3.3 Výkonnost a kapacita systému cPortál

Odezva systému na běžné akce uživatelů (jednoduchá vyhledávání, odpovědi na dotazy webových služeb, založení záznamu, editace záznamu, výběry do 200 řádků apod.) má být následující:
- do 0,5 sekundy min. v 80 % případů
- do 1,5 sekund max. ve 20 % případů
- do 2,5 sekund max. ve 2 % případů

Odezva systému na náročnější akce uživatelů (složitější vyhledávání, odpovědi na dotazy webových služeb, komplexnější výstupní sestavy, jednodušší dávková zpracování, výběry do 200 řádků apod.) má být následující:
- do 1 sekund min. v 80 % případů
- do 3 sekund max. ve 20 % případů
- do 5 sekund max. ve 2 % případů

Doba pro zpracování sestav - dávek, jejich zpracování bez vazby na počet zpracovávaných záznamů:
- do 30 sekund v 80 % případů
- do 1 min. ve 20 % případů
- do 5 min. ve 2 % případů

Navržená architektura systému cPortál musí plnit uvedené parametry. Uvedené hodnoty budou vycházet z dat obsažených, či předaných do systému cPortál. Do doby se nezapočítává čas na získání dat z externích evidencí, či napojených systémů.
Systémové prostředky pro provoz systému cPortál v prostředí nejsou určeny pouze pro daný systém. V uvedeném prostředí a o výkon a paměti se tedy bude systém cPortál dělit s dalšími systémy. Architektura systémů, by měla být navržena tak, aby těchto prostředků využívala efektivně. Paměť, tedy střední vrstvu využíváme zejména pro výběry dat, ke kterým přidáváme

externí data z jiných systémů. V ostatním případech by systém měl data vybírat na úrovni SQL přímo bez použití střední vrstvy.
Systémové prostředky celní správa udržuje na dané konfiguraci a v průběhu jejich životních cyklů se nemění. Výkonnost daného systémů je tedy nutné průběžně udržovat pravidelnou optimalizací systému a jeho monitoringem.

3.3.1 Hodnocení kvality výkonnosti a kapacity systému cPortál

Systém cPortál a jeho funkce hodnotíme jako bezproblémové, rizikové a nefunkční.

V případě hodnocení výkonnosti a kapacity systému cPortál u hodnot uvedených v čl. 3.3 je jedná o hodnocení bezproblémové. Za rizikové se povazuje překročení hodnot v čl. 3.3., kdy trvají méně než jeden den. Za nefunkčnost se povazuje překročení hodnot v čl. 3.3 déle, jak pracovní den.

4 Logování, provozní a bezpečnostní monitoring

4.1 Popis provozního monitoringu provozovatele cloudu

Předmětem Služby je nepřetržitý bezpečnostní monitoring aktiv objednatele v režimu 24x7 (dále jen „Služba“). Bezpečnostní monitoring je prováděn dohledovým pracovištěm a expertním týmem OCKB – SOC a CSIRT-SPCSS. Součástí bezpečnostního monitoringu je detekce kybernetických bezpečnostních událostí (dále jen „KBU“) pomocí nástroje SIEM, jejich vyhodnocování a zvládání, dokumentování kybernetických bezpečnostních incidentů (dále jen „KBI“), jejich analýza a návrhy na opatření. V rámci služby je poskytován incident management včetně přípravy podkladů pro příslušné orgány v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění a podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, případně na základě dohody smluvních stran. V rámci služby jsou poskytována následující aktiva:

- **Kubernetes Service** - Služba pro orchestraci kontejnerů v open-source platformě Kubernetes, která umožňuje nahrávání, správu a škálování kontejnerů.

- **Load balancer -** Služba pro vyvážení zátěže pro příchozí síťový provoz a zajištění vysoké dostupnosti použitých služeb. V tomto řešení primárně se použije pro vyvážení příchozích dotazů do služeb Kubernetes clusteru.

- **Virtual network –** Virtuální síť je základním stavebním kamenem pro soukromé sítě v Azure. Virtuální síť umožňuje mnoha typům prostředků Azure, například Azure Virtual Machines (VM), bezpečně komunikovat mezi sebou navzájem, internetem a místními sítěmi.

- **CDN – Služba** Azure Content Delivery Network (CDN) je určena pro publikaci statických souborů. Funkcionalita CDN zvyšuje rychlost a dostupnost portálu.

- VPN – VPN Gateway zajišťuje propojení sítí k Azure prostředí.

- **Key Vault -** Key Vault je nástroje v Azure pro bezpečné uchování a přístup k citlivým datům jako například hesla, klíče, certifikáty.

- **SQL Database – Databázové** uložiště pro uložení strukturovaných dat, pro které bude použita relační databáze Azure SQL Server.

- **Storage -** Trvalé uložiště souborových dat pro portálové řešení.

- **Application Gateway-Web Application Firewall – Azure** Application Gateway je nástroj pro vyrovnávání zatížení webových přenosů, který umožní spravovat provoz webových aplikací. V projektu je využita služba Web Application Firewall (WAF), která poskytuje centralizovanou ochranu webových aplikací před běžnými zneužití a zranitelnostmi. WAF je založen na pravidlech ze základních sad pravidel OWASP (Open Web Application Security Project).

- **Monitoring – Monitorovací** nástroj Azure monitor, který přímo poskytuje MS Azure Cloud a který nabízí celou řadu různých funkcí (detekce anomálií, analytické nástroje, diagnostiky apod.).

- **Firewall – GŘC on-prem** - Služba pro správu směrování a filtraci komunikace mezi sítěmi.

4.2 Bezpečnostní monitoring na cloudu

Bezpečnostní monitoring prostřednictvím Sentinel (cloud SIEM) za pomoci defender for cloud (Kubernetes) je poskytován na následujících aktivech:

Produkční prostředí Service type	Region	Description
Azure Kubernetes Service (AKS)	West Europe	7 D8s v4 (8 vCPU, 32 GB RAM) uzlů; Rezervované na 3 roky; 0 spravovaných disků s operačním systémem – S4, 0 clusterů
Storage Accounts	West Europe	Block Blob Storage, Blob Storage, redundance LRS, Vrstva přístupu Hot, Kapacita 10 GB - Platťe jenom za to, co využijete, 100 000 operací zápisu, 100 000 operací výpisu a vytvoření kontejneru, 100 000 operací čtení, 100 000 operací čtení z archivu s vysokou prioritou, 1 dalších operací Načítání dat: 1 000 GB, načítání z archivu s vysokou prioritou: 1 000 GB, zápis dat: 1 000 GB
Key Vault	West Europe	Trezor: 10 000 operací, 0 pokročilých operací, 0

		obnovení, 0 chráněných klíčů, 0 pokročilých chráněných klíčů za měsíc; spravované fondy HSM: 0 fondů HSM Standard B1 × 730 Hodin
Content Delivery Network		Zóna 1: 500 GB, Zóna 2: 0 GB, Zóna 3: 0 GB, Zóna 4: 0 GB, Zóna 5: 0 GB, DSA: 0 GB
Azure Monitor	West Europe	Počet ingestovaných GB: 30, počet vícekrokových webových testů: 0
Application Gateway	West Europe	Úroveň Web Application Firewall, velikost instance Střední: 1 instancí hodin brány × 730 Hodin, 1 TB jednotek zpracování dat, 500 GB jednotek zóny

Testovací prostředí Service type	**Region**	**Description**
Azure Kubernetes Service (AKS)	West Europe	3 D8s v4 (8 vCPU, 32 GB RAM) uzlů; Rezervované na 3 roky; 0 spravovaných disků s operačním systémem – S4, 0 clusterů
Storage Accounts	West Europe	Block Blob Storage, Obecné účely V2, redundance LRS, Vrstva přístupu Hot, Kapacita 100 GB - Platte jenom za to, co využijete, 100 000 operací zápisu, 100 000 operací výpisu a vytvoření kontejneru, 100 000 operací čtení, 100 000 operací čtení z archivu s vysokou prioritou, 1 dalších operací Načítání dat: 1 000 GB, načítání z archivu s vysokou prioritou: 1 000 GB, zápis dat: 1 000 GB
Key Vault	West Europe	Trezor: 10 000 operací, 0 pokročilých operací, 0 obnovení, 0 chráněných klíčů, 0 pokročilých chráněných klíčů za měsíc; spravované fondy HSM: 0 fondů HSM Standard B1 × 730 Hodin
Content Delivery Network		Zóna 1: 10 GB, Zóna 2: 0 GB, Zóna 3: 0 GB, Zóna 4: 0 GB, Zóna 5: 0 GB, DSA: 0 GB
Azure Monitor	West Europe	Počet ingestovaných GB: 20, počet vícekrokových webových testů: 0
Application Gateway	West Europe	Úroveň Web Application Firewall, velikost instance

		Střední: 1 instancí hodin brány × 730 Hodin, 10 GB jednotek zpracování dat, 10 GB jednotek zóny

Součástí dodávky Služby Bezpečnostní monitoring jsou:

• proces zvládání KBU, KBI (incident management);

• detekce, sběr, uchovávání a vyhodnocování kybernetických bezpečnostních událostí a incidentů, monitoring databází a aplikací;

• zpracování Zprávy o stavu Služby určené objednateli (předávána v kvartálním intervalu);

• ukládání security logů minimálně po dobu definovanou ZoKB.

Pravidelným kvartálním výstupem Služby je zpracování dokumentu Zpráva o stavu bezpečnosti infrastruktury, který je základem pro průběžné zlepšování Služby v přirozeně proměnlivém bezpečnostním prostředí.

Zpráva o stavu bezpečnosti infrastruktury obsahuje řešení a stav BH, KBU, KBI za uplynulé období a návrhy na nápravná opatření. Tato zpráva bude zahrnuta ve Zprávách o úrovni a rozsahu poskytované Služby za dané období.

Detekce, sběr a vyhodnocování kybernetických bezpečnostních událostí a incidentů

Služba je souborem aktivit a procesů v oblastech monitoringu a detekce, jejich vyhodnocování a zvládání, dokumentování kybernetických bezpečnostních událostí, bezpečnostních hlášení a kybernetických bezpečnostních incidentů (KBI), jejich analýzy a návrhů na zlepšování IS Objednatele.
Monitoring a detekce kybernetických bezpečnostních událostí (KBU) v režimu 24x7 jsou zajištěny dohledovým pracovištěm, SIEM nástrojem provázaným s provozním monitoringem (Azure Monitor) a s reportováním výkonů a zatížení. Vyhodnocování a klasifikace bezpečnostních incidentů a určování adekvátních reakcí je prováděno, evidováno a vyhodnocováno v ServiceDesku SPCSS.

4.3 Zdrojové kódy systému cPortál

Projekt bude vyvíjen v souladu se směrnicí 9/2021. Po akceptaci díla budou odevzdány zdrojové kódy dodavatele. Dále pak opakovaně při dalších změnách v rámci provozu, případně na požádání zadavatele.

4.4 Schéma databáze cPortál

Databáze cPortálu je členěna do několika schémat, které jsou oddělené:

- PDB – základní data pro portál (číselníky, podání, mandátní rejstřík, ...)
- PORTAL – data potřebná pro Liferay portál a jeho redakční systém
- CAS – data pro přihlašovací komponentu CAS
- PDBMIG – pomocná data pro potřeby datové integrace (např. číselníky CS)

5 Popis umístění aplikace v prostředí AZURE

5.1 Popis HW prostředí

Portálová aplikace, kterou dodává a spravuje společnost Asseco využívá následující komponenty prostředí MS Azure:

- Kubernetes Service
- Služba pro orchestraci kontejnerů v open-source platformě Kubernetes, která umožňuje nahrávání, správu a škálování kontejnerů. Kubernetes orchestruje clustery virtualizací a naplánuje spuštění kontejnerů na těchto virtualizacích na základě jejich dostupných výpočetních prostředků a požadavků na zdroje každého kontejneru. Kontejnery jsou seskupeny do podů, základní operační jednotky pro Kubernetes. Kubernetes také automaticky spravuje dostupnost služeb, rozkládá zátěž, alokuje zdroje a škáluje na základě využití výpočetní techniky. Dále kontroluje stav jednotlivých prostředků.

- Load balancer
- Služba pro vyvážení zátěže pro příchozí síťový provoz a zajištění vysoké dostupnosti použitých služeb. V tomto řešení primárně se použije pro vyvážení příchozích dotazů do služeb Kubernetes clusteru.

- Virtual network
- Virtuální síť je základním stavebním kamenem pro soukromé sítě v Azure. Virtuální síť umožňuje mnoha typům prostředků Azure, například Azure Virtual Machines (VM), bezpečně komunikovat mezi sebou navzájem, internetem a místními sítěmi. Virtuální síť je podobná tradiční síti, ale přináší s sebou další výhody infrastruktury Azure, jako je škálování, dostupnost a izolace.

- CDN
- Služba Azure Content Delivery Network (CDN) je určena pro publikaci statických souborů. Funkcionalita CDN zvyšuje rychlost a dostupnost portálu.

- VPN
- VPN Gateway zajišťuje propojení sítí k Azure prostředí.

- Key Vault
- Key Vault je nástroje v Azure pro bezpečné uchování a přístup k citlivým datům jako například hesla, klíče, certifikáty.

- SQL Database
- Databázové uložiště pro uložení strukturovaných dat, pro které bude použita relační databáze Azure SQL Server.

- Storage
- Trvalé uložiště souborových dat pro portálové řešení.

- Application Gateway-Web Application Firewall
- Azure Application Gateway je nástroj pro vyrovnávání zatížení webových přenosů, který umožní spravovat provoz webových aplikací.
- V projektu je využita služba Web Application Firewall (WAF), která poskytuje centralizovanou ochranu webových aplikací před běžnými zneužití a zranitelnostmi. WAF je založen na pravidlech ze základních sad pravidel OWASP (Open Web Application Security Project).
- Webové aplikace jsou stále více terčem škodlivých útoků, které využívají běžně známé chyby zabezpečení. Mezi tyto pokusy patří běžné útoky pomocí SQL injection, útoky skripty napříč weby a další. Předcházet takovým útokům v kódu aplikace může být náročné a může vyžadovat pečlivou údržbu, opravy a monitorování na mnoha vrstvách topologie aplikace. Centralizovaný WAF pomáhá mnohem jednodušší správu zabezpečení a poskytuje lepší jistotu správcům aplikací před hrozbami.

- Monitoring
- Monitorovací nástroj Azure monitor, který přímo poskytuje MS Azure Cloud a který nabízí celou řadu různých funkcí (detekce anomálií, analytické nástroje, diagnostiky apod.).

- Firewall – GŘC on-prem

Služba pro správu směrování a filtraci komunikace mezi sítěmi.

Hardware v tomto projektu není využíván, pouze virtuální v prostředí MS Azure.

5.2 Doporučení pro provoz HW a SW v prostředí cloudu

Nespecifikováno s ohledem na 5.1

5.3 Provozní podpora, SBM

Technická podpora systému cPortál zahrnuje celou řadu činností spojených s provozem systému a jeho napojených služeb, mezi které patří i FAS server a připravovaná komunikační brána ELPORT_B. Vše provozované na cloudu v AZURE. Pro zajištění provozu ve všech prostředích systémů (provozní, testovací) týkající se dohledu, nastavení, ladění, optimalizaci chodu HW a SW je v rámci technické podpory na tyto činnosti stanoven paušální počet hodin.

Paušální počet člověkohodin	Člk. za měsíc	Člk. za rok
Dohled na cloud - technik	33	396
Dohled na cloud – služby nastavení ladění, optimalizace	41	492
Dohled na FAS server	56	672
Dohled na ELPORT_B	53	636
Celkem člk. maximálně	183	2196

5.3.1 Odstraňování provozně-technických problémů v provozním prostředí

a) Zadavatel poskytuje Dodavateli přístup do aplikace SBM (do části helpline a požadavků), ve které jsou evidovány provozní případy z provozu,

b) Řešitelem případu může být i Dodavatel, aplikace SBM informuje řešitele o přidělení případu,

c) Je-li to pro řešení případu nezbytné, Zadavatel konzultuje případ s Dodavatelem a hledají společné řešení.

d) Zadavatel předá Dodavateli případ k řešení v případě, že se jedná o provozně-technický problém, který nelze Zadavatelem vyřešit, či je to z obsahu případu vhodnější.

e) Případy Zadavatel i Dodavatel řeší průběžně. Maximální předpokládaná doba na řešení případu je 60 dní ode dne zaevidování případu. Tato lhůta neplatí u závažných technických problémů (incidentů) na provozním prostředí.

f) Zadavatel zajistí Dodavateli přístup na Service Desk Ministerstva financí v souvislosti se službami ICT MF poskytující aplikační a metodickou podporu cloudu.

5.3.2 Odstraňování závažných technických problémů v provozním prostředí

a) V případě, že dojde ke vzniku závažného technického problému (incidentu) v díle v provozním prostředí, oznámí Zadavatel tuto skutečnost bezodkladně Dodavateli prokazatelným způsobem s uvedením, jak se závažný technický problém projevuje. Závažným technickým problémem se rozumí skutečnosti způsobující nefunkčnost systému elektronického zpracování dat v díle.

b) Dodavatel je povinen zahájit práce na odstranění závažného technického problému v pracovních dnech a pracovní době (9 -17 hodin) nejpozději do 4 (čtyř) hodin od jeho oznámení Dodavateli a tento závažný technický problém odstranit tj. uvést dílo do bezchybného provozu ve lhůtě přiměřené povaze oznámeného závažného technického problému, nejdéle však do 5 (pěti) pracovních dnů.

c) Pro evidenci těchto případů se použije postup, kdy požadavky na odstranění závažného technického problému, bude Zadavatel zadávat prostřednictvím portálové aplikace SBM požadavky.

d) Zadavatel doplňuje případy závažných technických problémů z SBM HelpLine do SBM požadavky pro objednané období s ohledem na lhůtu pro odstranění technického problému.

e) Dodavatel je povinen popsat do portálové aplikace SBM HelpLine příčinu vzniku problému ve lhůtě viz bod b) a navrhnout způsob opravy, stav řešení a ukončení opravy.

f) Vznikne-li závažný technický problém musí být opraven jednotlivě hlášený případ, ale i všechny ostatní nehlášené související chyby. Má-li chyba dosah do komunikačního rozhraní a byla předána nekonzistentní data, musí být opravena i tato nesprávná komunikace.

5.4 Provoz

Systém je v rutinním provozu od roku 2019 a bude vyvíjen na míru a provozován podle potřeb organizace a dle platné legislativy.

Systém cPortál musí být připraven zvládat níže uvedené předpokládané objemy dat a počty uživatelů.

- Systém cPortál není určen pro uživatele Celní správy ČR, ta zajišťuje pouze administraci systému. Přístup bude zajištěn pro cca 25 správců Celní správy ČR a jejich případných smluvních dodavatelů. Externí počet uživatelů je nutné rozdělit do dvou částí a to nepřihlášených a přihlášených. Nepřihlášených uživatelů systému předpokládáme prohlížení až 5 000 uživatelů v jeden okamžik. U přihlášených uživatelů předpokládáme v souvislosti s dalších rozvojem aplikace (poskytování dalších služeb) až 10 000 uživatelů v jeden okamžik. Uvedené počty uživatelů nebudou dosahovány celý den. Zvýšený počet bude v pracovní dny od 8.00 hodin do 17.00 hodin. V tuto dobu budou do cPortál přistupovat zejména osoby, které se problematiku dovozu a vývozu zboží zajišťují. Ve večerních hodinách osoby realizující dovoz zboží pro soukromé účely. U problematiky spotřebních daní a DES se dá předpokládat zvýšená aktivita v pracovní dny a zejména ve dny, kdy končí lhůta pro podání daňových přiznání.

Požadavky na návazné systémy:

- CRS – 50 000 ověření pro přihlášení uživatelů do systému cPortál
- eCep – 5 000 podání celního prohlášení
- eSAT – 20 000 podání v exponovaných dnech
- Požadovaná komunikační brána pro zasílání xml. musí zajistit komunikaci tisíce až desetitisíce podání, podle toho jak se postupně budou připojovat další systémy.

Počet operací za den (průměrně):

- Vzhledem k tomu, že se jedná o systém umožňující elektronicky komunikovat s CS je nutné počítat s tisíci podání zadaných ručně s systému a desetitisíce operací denně u komunikační brány zajišťující strojové operace jiných systémů.

Průměrný počet čj. za rok:

- cca 500 tisíc,
- z toho za den: cca 500

Předpokládaný počet změn v roce (rozvoj):

- Neprobíhají významné změny, ale pouze reakce na změny legislativy a požadavky provozu. Obvykle cca 2-3 změny (RFC) (1-3 za 1/3 roku) a z toho pak 3 releasy za 1 rok.

Počet chyb – hlášení HELPLINE:

Předpokládáme – uvádíme tři možné oblasti chybových stavů. První oblast je nedostupnost NIA a služeb mandátního rejstříku a druhá oblast je dostupnost formulářů a jejich podání, třetí oblastí bude dostupnost komunikační brány a její služby.

5.5 Předmět zakázky – požadavky na podporu a rozvoj

Zhotovitel v rámci podpory přebírá systém cPortál a provádí technickou podporu vyvinutých a převzatých programových produktů.
Tato zakázka má za cíl realizovat rozšířením platformy cPortál a bude provedena integrace dalších aplikací pro celní a daňové řízení, včetně jejich služeb, elektronické komunikace prostřednictvím xml. V rámci rozvoje zhotovitel zajišťuje podle požadavků objednatele v SBM.

Nové funkce:

- Přechod na novou doménu gov.cz
- Transformace CS implementace
- Modernizace systému podle směrnice č. 9/2021 příloha č.1 kapitola 6.0. až 6.5.1. (včetně Desingu), bude-li vyhodnocena aktuálnost tohoto požadavku
- Rozšíření mandátního rejstříku o zastupování podle IČO, včetně integrace certifikátů pro ověření komunikace na nové ECR bráně
- Příprava rozhraní pro externí subjekty v souvislosti s celním řízením, realizace nové ECR brány (přihlášení deklarantské veřejnosti podle oprávnění dané evropskou legislativou do systémů dovozu a vývozu zboží)
- rozšíření logování v administraci a administrativní správa
- Realizace služeb pro systém EvDPH (vratky DPH za zboží při jeho vývozu do třetích zemí pro FO), a další systémy např. ORO, Intrastat …
- Rozšíření informací v Daňové informační schránky dle novely daňového řádu -SPD a dělená správa
- Portál obchodníka – služby pro povolovací řízení u cla
- Výměna a modernizace e-formulářů včetně realizace modulu pro formulářové řešení
- Mobilní aplikace cPortál
- Analýza a implementace dalších oblastí, které bude možné v rámci cPortálu realizovat na základě požadavků provozu a legislativy.

Rozvoj systému je řízen v SBM a předpokládá následující fáze:

1. Analýza GAN
2. Pilotní provoz, testování
3. Analýza DAN
4. Testovací provozní prostředí – souběh systémů
5. Provozní prostředí
6. Protokol o převzetí systému do provozu

Seznam aplikací, které budou cPortál využívat i pro elektronickou komunikaci

Útvar GŘC	Stav	Název, popis aplikace	Kód aplikace dle Katalogu aplikací SBM odboru 12	Dlaždice cPortálu
Odbod 21	Předpoklad zprovoznění	**EVDPH -** Aplikace pro elektronizaci vrácení DPH fyzickým osobám ze třetích zemí při vývozu zboží	EVDPH	Elektronická evidence vratek DPH
odbor 23	Předpoklad zprovoznění	**ORO Web Klient** - Zasílání oznámení osoby povinné značit líh podle § 38 zákona č. 307/2013 Sb., o povinném značení lihu (dále jen „zákon o PZL“) a oznámení distributora lihu podle § 43 zákona o PZL	ORO	Značení a distribuce lihu
odbor 23	Předpoklad zprovoznění	**EMCS klient pro deklaranty** - Připojení deklaranta k systému EMCS, podání e_AD/e-SAD, podání oznámení o přijetí, změna místa určení, storno dopravy, vysvětlení nesrovnalostí, vysvětlení nepřijetí zásilky včas	EMCS_WEB (též EMCS_DM)	Doprava VV
odbor 21	Předpoklad zprovoznění	**Webklient e-dovoz** - Komunikace deklarantů s CS ČR pro vstupní a dovozní operace	ICS_WEB	Ostatní k celnímu řízení

odbor 21	Předpoklad zprovoznění	**Web klient NWK II** - Aplikace pro deklaranty umožňující podání celních prohlášení do režimu tranzitu, vývozu a e-dap. Aplikace také umožňuje sledovat stav čerpání záruk a povolení ZJP.	NWKII	Ostatní k celnímu řízení
odbor 21	Předpoklad zprovoznění	**CDS** (EU Trader Portal Customs Decisions) - Systém pro správu celních rozhodnutí	CDS	CDS (Trader Portal)
odbor 21	Předpoklad zprovoznění	**eBTI** - Evidence závazných informací o sazebním zařazení	EBTI	Sazební zařazení zboží
odbor 21	Předpoklad zprovoznění	**eAEO** (Trader Portal) - Oprávněný hospodářský subjekt - Evidence žádostí o AEO certifikát, procesy přidělování a správy certifikátů pro evidované subjekty	AEO	AEO
odbor 21	Předpoklad zprovoznění	**Instatonline** - Pořizování a odesílání dat Intrastatu; Instatdesk (desktopová verze) **InstatEvo** (nová verze zahrnující předchozí verze)	INO; INSTAT_DESK	Intrastat
odbor 21	Předpoklad zprovoznění	**EENVS** - Elektronická evidence nezávazných vyjádření a stanovisek	EENVS	Sazební zařazení zboží
odbor 21	Předpoklad zprovoznění	**Národní portál pro podávání žádostí na vnitrostátním trhu** (pracovní název) – Podávání žádostí o přijetí opatření na vnitrostátním trhu elektronickou cestou Evidence duševního vlastnictví - Evidence a zpracování žádostí o přijetí opatření a záchytů zboží podezřelého z porušování práv duševního vlastnictví	COPIS	Duševní vlastnictví

7.

6 Harmonogram plnění vývoje projektu

Pořadí konkrétních požadavků a souboru prací, uvedených v této Zadávací dokumentaci nemusí odpovídat skutečnému pořadí požadavků objednatele. Skutečnému pořadí souboru prací bude odpovídat požadavek zadaný objednatelem do aplikace SBM i s jeho termínem splnění.

7 Vlastnická práva

U systém cPortál je výhradním držitelem autorských práv Celní správa ČR. Dodavateli produktu cPortál nebude náležet ochrana dle zákona č.121/2000 Sb., o právu autorském, o právech souvisejících a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, tj. včetně udělení souhlasu k užití díla, jeho úpravám a zásahům do celého díla souvisejícím nejen s plněním služeb rozvoje a aktualizace díla, ale i správy a servisu celého provázaného systému.

Celní správa je oprávněna do díla (aplikace cPortál) zasahovat, a to například upravovat jej, rozmnožovat jej, předkládat jej a zpracovávat jeho zdrojové kódy a to jak ze strany Zadavatele, tak ze strany jiného subjektu vybraného Zadavatelem, a to za účelem dalšího rozvoje díla (vytvoření nových funkcionalit nebo rozvoje či změny stávajících funkcionalit) anebo jeho napojení na jiné aplikace (SW), užívané, provozované nebo vytvářené Zadavatelem nebo jím vybraným subjektem, případně funkční propojení s jinými aplikacemi užívanými, provozovanými či vytvářenými Zadavatelem nebo jim vybraným subjektem.

8 Kontakty

[redacted]

9 Závěrečné ustanovení

Zadavatel si vyhrazuje právo změnit některé podmínky při vyhlášení vlastního výběrového řízení.

10 Seznam použitých zkratek

Seznam použitých zkratek

AD	Active Ditectory
ADIS	Informační systém Daňové správy
AIS	Automatic Import Systém (Dovozní systém)
AISC	Agendový IS cizinců
AISEO	Agendový IS evidence obyvatel
ARES	Registr ekonomických subjektů
AVIS	Vnitřní informační systém
CEPAN	Centrální evidence přeplatků a nedoplatků
CIS	Cizinecký informační systém
CRS	Centrální registr
COPIS	Evidence duševního vlastnictví
CS	Celní správa
ČNB	Česká národní banka
ČSSZ	Česká správa sociálního zabezpečení
DES	Registr subjektů dělené správy
DAN	Detailní analýza
ECDC	Evidence celních dluhů - centrální
ECS	Celní řízení v režimu vývoz
e-Dovoz	Systém dovozu
EORI	Identifikátor subjektu v rámci celního řízení
ETN	Automatizovaný systém pro Evidenci tabákových nálepek
eSAT	Spisová služba
EPP	Evidence porušení právních předpisů
ETN	Evidence tabákových nálepek
EOsMA	Evidence osobního majetku
EUR	Evidence vydaných EUR
EVAP	Evidence analytických produktů
EVZ	Elektronické vyhodnocení zboží
eWDIS	Původní dovozní systém
FO	Fyzická osoba
FÚ	Finanční úřad
GAN	Globální analýza
GMS	Guarantee Management Systém (Globální záruky)
Havarijní postup	Proces, jehož cílem je dosažení alespoň částečného obnovení činnosti, pokud je IS z libovolného důvodu odpojen. Havarijně obnovená činnost nemusí být nutně podporovaná IS, ale např. papírovou procedurou.
HELPLINE	Aplikace pro evidenci případů požadavků o pomoc s řešením problému v dané oblasti
HW	hardvare
IC CS	Informační centrum celní správy

ICS	Aplikace pro e-dovoz
ICT	Information and Communication Technology – obvykle ekvivalent zkratky IT, informačních a komunikační technologie
IS	Informační systém
IS CS	Informační systém celní správy
ISKN	Informační systém Katastru nemovitostí
ISPAD	Informační systém pátrání a dohledu
ISVS	Informační systém veřejné správy – ve smyslu zákona 365/2000Sb. Je ISVS definován jako „soubor informačních systémů, které slouží pro výkon veřejné správy“. Hlavními znaky ISVS tedy jsou - přímá podpora výkonu veřejné správy a existence legislativní opory pro jeho zřízení a provoz. Do ISVS nepatří např. podsystémy pro provozní zajištění potřeb orgánu veřejné správy (personalistika, správa vlastního majetku orgánu, apod.).
ISZR	Informační systém Základních registrů
LIMS	Laboratorní informační a manažerský systém
MAK	Mák a konopí
MD	Mobilní dohled
MED	Modul exekucí a dražeb
ME-SPD	Modul spotřebních daní
MF	Ministerstvo financí
MKR	Mezinárodní kontrolní režimy
MPV	Mezinárodní vymáhání
NCTS	Celní řízení v režimu tranzit
OWNRES	Evidence nesrovnalostí v rámci TOR
PBL	Objednávkový systém pro pokutové bloky
PHM	Registr pohonných hmot
PO	Právnická osoba
RegSub	Registr subjektů
RDS	Registr daňových subjektů
ROB	Registr obyvatel
ROS	Registr osob
RSDS	Registr daňových subjektů
RUIAN	Registr územní identifikace adres a nemovitostí
RZMO	Registr zvláštních minerálních olejů
RZL	Registr značení lihu
SBM	Serena Bussines manager
SPD	Spotřební daň
SPR	Sdružená podpora rozhodování
SRA	Systém rizikové analýzi
SRC	Serena Request Center (centrum žádostí SERENA) – centralizovaný systém ITSM Celní správy zajišťující i evidenci případů požadavků o pomoc s řešením problému v dané oblasti

SŘZ	Systém řízení změn – definice služby, kterou zajišťujeme registraci, evidenci a další administraci požadavků ze strany objednatele v souladu s metodologií ITSM, prostřednictvím aplikačního systému používaném u CS v daném období
SW	software
TARIC	Tarifní informační systém
Technologie	V kontextu informačních systémů: technické, programové a komunikační
TIS	Tarifní informační systém
TOR	Tradiční vlastní zdroje
VČP	Vlastní číslo plátce
VKC	Vnitřní kontrolní činnost
VSD	Vnitrostátní daně
VZP	Všeobecná zdravotní pojišťovna
VZ	Veřejná zakázka

11 Seznam příloh

Veřejná část:
Příloha č. 1: Webové služby -
Příloha č. 2: Komunikační rozhraní
Příloha č. 3: Zadání pro rozšíření služby o IČO
Příloha č. 4: Zadání pro komunikační bránu
Příloha č. 5: Komunikační rozhraní CRS
Příloha č. 6: Komunikační rozhraní eSAT
Příloha č. 7: Požadavky na formulářovou technologii

Příloha č. 5

Školení zaměstnanců externích společností ze zásad bezpečnosti a ochrany zdraví při práci, požární ochrany

Zaměstnanci externích společností jsou povinni:

1. Při vstupu do budovy se vždy ohlásit u zaměstnance odboru 12, majícího danou práci na starosti.
2. Pohybovat se jen v prostoru opravovaného zařízení, na které byli přivoláni.
3. Počínat si při práci tak, aby nedošlo k ohrožení zdraví, dodržovat předpisy o ochraně a bezpečnosti při práci a stanovené pracovní postupy.
4. Vstupovat do kontrolovaných prostor jen se svolením vedoucího střediska, mistra nebo mechanika, a to v předepsaném ochranném oděvu. Vstup do čistých a kontrolovaných prostor je povolen v kombinézách z bezúletového materiálu a příslušné obuvi.
5. Zaměstnanci externích firem jsou povinni během práce dodržovat pořádek a vždy po vykonání určené práce uvést pracoviště do původního stavu.
6. Oznámit vedoucímu zaměstnanci ihned nedostatky a závady, které by mohly ohrozit bezpečnost a zdraví ostatních zaměstnanců.
7. Řídit se bezpečnostními tabulkami, které jsou v objektu umístěny.
8. Nezabraňovat přístupu k rozvaděčům energií, hasicím přístrojům a únikovým východům.
9. Při odchodu z pracoviště odpojit elektrické spotřebiče.
10. Před započetím práce se informovat, v jakém stavu se nachází zařízení, na kterém se bude pracovat.
11. Oprava, seřizování, úprava, údržba a čištění zařízení se provádějí, jen je-li zařízení odpojeno od přívodu energií. Není- li to technicky možné, musí se učinit vhodná ochranná opatření.
12. Při práci v prostředí s nebezpečím výbuchu se musí používat nejiskřící nářadí, antistatický oděv a antistatická obuv.
13. Před zahájením prací s otevřeným ohněm a po jejich ukončení se musí o této skutečnosti informovat [redacted]
14. Při vyhlášení požárního poplachu urychleně opustit ohrožený prostor a odebrat se na shromaždiště dle evakuačního plánu pracoviště, na kterém vykonává svou činnost.
15. Počínat si tak, aby svým chováním, jednáním a činností nezavdal příčinu k požáru, ekologické nebo jiné havárií.
16. Dodržovat a respektovat platné příkazy, zákazy a nařízení, se kterými byli seznámeni, dále všechny bezpečnostní tabulky, nápisy, symboly a příkazy.
17. Počínat si při výkonu činnosti tak, aby svým jednáním nebo chováním nebo vlastní činností neohrožovali zdraví a životy zaměstnanců a osob zdržujících se v areálu nebo majetek celní správy.
18. V souvislosti se svou činností dodržovat na pracovištích pořádek a čistotu, zabezpečovat průchodnost přístupových a únikových komunikací.
19. Zajišťovat bezpečnost používaných strojů a mechanismů, provádět kontrolu stavu pracoviště, používaného nářadí a nástrojů a zjištěné závady neprodleně odstraňovat.
20. Oznamovat svým nadřízeným příp. pověřeným zaměstnancům celní správy ty závady a nedostatky, které by mohly být příčinou bezpečnostní nehody (úrazu) nebo havárie, a které nejsou schopni odstranit vlastními silami a prostředky.
21. Vykonávat pracovní činnost pouze na určených, vyhrazených a převzatých pracovištích za dohodnutých podmínek, ze kterých se nesmějí bez souhlasu pověřeného zaměstnance celní správy svévolně vzdalovat s výjimkou naléhavých případů (nevolnost, nemoc, úraz apod.) a odchodu na přestávku v práci dle zákoníku práce v platném znění.

22. Dodržovat zákaz kouření v celém areálu budovy GŘC s výjimkou míst k tomu určených a označených jako „Kuřárna“. Kouření je povoleno pouze v kuřárnách, které jsou umístěny na schodištích.
23. Používat otevřený oheň a jiné zdroje zapálení (svařování, pálení, broušení, řezání, vrtání, letování, natavování apod.) pouze na určených a schválených údržbářských pracovištích (např.
svařovna). Mimo tato místa je možné používat otevřený oheň a jiné zdroje zapálení jen se souhlasem odpovědných zaměstnanců GŘC [redacted] kteří musí před zahájením prací vyhodnotit rozsah požárního rizika v daném místě dle platné směrnice o požární ochraně. V každém případě musí být vystaveno pro externí společnost "Příkaz k provedení prací se zvýšeným nebezpečím požáru" a splněna v něm stanovená opatření. Je nutno při používání otevřeného ohně v průběhu prací i po jejich ukončení dbát zvýšené opatrnosti.
24. Oznamovat svým nadřízeným, resp. pověřeným zaměstnancům celní správy snížení zdravotní způsobilosti k výkonu práce (nevolnost, nemoc, zdravotní indispozice) nebo jiných okolností, které mohou ovlivnit bezpečný výkon práce.
25. Respektovat rozhodnutí, příkazy a doporučení pověřených zaměstnanců celní správy a zaměstnanců, kteří vykonávají kontrolní a dozorčí činnost na úseku bezpečnosti a ochrany zdraví při práci, požární ochrany, ostrahy majetku.
26. Řídit se dalšími obecně závaznými předpisy a normami, jakož i místními předpisy a organizačními normami v oblasti BOZP a PO, se kterými byly zaměstnanci externí společnosti seznámeny v rámci proškolení BOZP a PO.
27. Na základě vyhledání rizik při vykonávané pracovní činnosti používat vhodné OOPP.
28. V případě vzniku požáru v budově GŘC jsou zaměstnanci externích společností povinni zakročit k odvrácení škody, pokud tím nevystavují vážnému ohrožení sebe, nebo ostatní přítomné zaměstnance a ohlásit požár dle požárních poplachových směrnic na ohlašovnu požáru kl. 2782.
29. Každý zaměstnanec externí společnosti, který se stane svědkem úrazu je povinen na místě, v rámci svých schopností a možností poskytnout okamžitou předlékařskou první pomoc a přivolat lékaře. Lékařskou první pomoc zajišťuje v pracovní dny v ordinačních hodinách [redacted] v ostatních případech ZZS HMP na tel. č. 155, případně integrovaný záchranný systém tel. č. 112. Neprodleně oznámit vedoucímu zaměstnanci celní správy kde došlo k úrazu.
30. Dodržovat zákaz požívání alkoholických nápojů, návykových látek a omamných prostředků na všech pracovištích. Uvedený zákaz se vztahuje i na donášení alkoholických nápojů a omamných prostředků ve všech prostorách a objektech celní správy. Dodržovat povinnost přicházet na pracoviště ve střízlivém stavu a setrvat v něm po celou pracovní dobu.

<u>Používání OOPP:</u>

1. OOPP nutné pro běžnou servisní činnost je povinna zajistit externí společnost sama.
2. Zaměstnanci externích společností jsou povinni předepsaným způsobem použít speciální OOPP dle rizik, vyplývajících z povahy vykonávané práce. (např. rukavice, polomasky, antistatická obuv, spec. oděvy - kombinézy, ochranné brýle atd.).

Zaměstnancům je zakázáno:

1. Přinášet a používat (i před vstupem) alkoholické nápoje do objektů či areálu Celní správy ČR.
2. Požívat či jinak zneužít účinné látky nebo přípravky, které se na střediscích používají nebo vyrábějí.
3. Odstraňovat nebo poškozovat bezpečnostní zařízení, kryty, značky. Odstraňovat nebo poškozovat instalované bezpečnostní, požární a informativní tabulky, nápisy, symboly, vyřazovat z činnosti další bezpečnostní opatření (ochrany, kryty, zábradlí, zábrany apod.) svévolně provádět další nepovolené úpravy bezpečnostního a protipožárního vybavení pracoviště.
4. Pokud se provádí práce v čistém prostoru musí se dodržet pravidla chování v čistých prostorech podle provozního řádu střediska.
5. Používat nástroje, nářadí, stroje, zařízení a dopravní a manipulační prostředky, které nesplňují požadavky bezpečnosti a ochrany zdraví při práci a nebyly u nich provedeny předepsané prohlídky, zkoušky a revize.

Seznámení zaměstnance externích společností s rizikem požáru:

1. Každý zaměstnanec provádějící činnost v areálu společnosti je povinen řídit se požárním řádem pracoviště a v případě vzniku mimořádné události (požár, havárie apod.) také požárním evakuačním plánem a poplachovými směrnicemi.
2. Při zpozorování požáru je každý povinen jej uhasit pomocí ručních hasicích přístrojů případně
spuštěním stabilního hasicího zařízení. Není-li to možné, bezodkladně vyhlásit požární poplach
a ohlásit vznik požáru - tel.kl.150 nebo tlačítkem EPS.

Životní prostředí:

Je povinností všech zaměstnanců externích společností zdržovat se veškerých činností, které by mohly vést k ohrožení či poškození životního prostředí (např. volně odhazovat či netřídit odpad do nádob k tomu určených, vylévat zbytky kapalin do kanalizace, používat zařízení, která nevyhovují technickým požadavkům, aj.).

Příloha č. 6

Zásady spolupráce

Spolupráce zhotovitele s objednatelem je prestižní záležitostí pro zhotovitele a tento si této vzájemné spolupráce cení.
Zásady spolupráce vycházejí z principů firemní kultury, metod práce, oprávnění a povinností objednatele dané zákonnou úpravou.

Vzájemná spolupráce slouží k budování prestiže objednatele, ale i samotného dodavatele.

Základem pro vzájemnou spolupráci je dodržování povinností dané touto smlouvou, ale i vzájemné respektování členů týmu, jejich vzájemná sounáležitost při řešení úkolů, komunikativnost, vstřícnost a hospodárnost. Spolupráce je i odpovědnost.

Zásady:

Komunikativnosti a vstřícnosti – Objednatel i zhotovitel spolu komunikují takovým způsobem, aby se žádná ze stran nemohla jednáním druhé strany cítit poškozená. Obě strany společně komunikují tak, aby si vzájemně porozuměly. Výklad objednatele je pro zhotovitele závazný.

Zákonnosti - smluvní strany jednají v souladu s platnými zákony a jinými právními předpisy, interní předpisy objednatele souvisejícími se smluvním vztahem

Sounáležitosti s firemní kulturou – Firemní kultura objednatele je specifický sociální systém nastavený vnitřními procesy organizace a její organizační strukturou. Osoby spolupracující s objednatelem a tedy i zhotovitel HW i SW je povinen se této firemní kultuře přizpůsobit.

Hospodárnosti – v rámci této smlouvy postupují smluvní strany tak, aby nevznikaly zbytečné, nebo neodůvodnitelné náklady.

Příloha č. 7

Hodnocení kvality

Popis oblasti:	Hodnocení kvality			Hodnota malusu u nefunkčnosti v %
	Bezproblémové do:	**Rizikové do:**	**Nefunkčnost více než:**	
Obecný incident:				
Řešení jednotlivého závažného technického problému – incidentu (používáme v případě, že se nejedná o definovaný incident)	Neurčeno, aplikační pravidla	Neurčeno, aplikační pravidla	2 prac.dny	8
Definovaný incident:				
Požadavky z SBM:				
Nacenění požadavku na vývoj od zadání	30 dní	45 dní	60 dní	30
Schválení plánu vývoje, rozvoje dle bodu 1.21	30 dní	45 dní	60 dní	40
schválení dílčích objednávek vývoje , rozvoje dle bodu 1.21	10 dní	20 dní	30 dní	40
Složení pracovního týmu dodavatele složení dle smlouvy čl. 16.4 smlouvy	Neurčeno, řeší smlouva	Nedostupnost týmu do 50% po dobu 30 dnů	Nedostupnost, neuplnost týmu, po více než 30 dní, nedoplnění člena týmu dle čl. 16.4 smlouvy	70
Dostupnost formulářů a možnost podat elektronický úkon	Odezva, znázornění a doplnění do 5 sekundy	Odezva, znázornění a doplnění do 1 minuty	Nedostupnost formulářů a podání více jak 2 hodiny od zjištění a neodstranění chyby do druhého dne	30
Plnění povinností dle zákona o kybernetické bezpečnosti bod 2.1	60	60	Nedodržení povinností vyplývající ze zákona o kybernetické bezpečnosti a	50

			zpracování auditu	
Webové služby, pohledy:				
Komunikace s aplikacemi, systémy, službami a číselníky	Komplexní dostupnost služeb	S výpadky ne delšími než jeden den	1 prac. den	25
Zajištění služeb provozu cloudu:				
Dohled na cloud	Komplexní dostupnost poskytovaných služeb	S výpadky ne delšími než jeden den	2 prac. den	25
Dohled na FAS server	Komplexní dostupnost poskytovaných služeb	S výpadky ne delšími než jeden den	2 prac. den	25
Dohled na ELPORT-B	Komplexní dostupnost poskytovaných služeb	S výpadky ne delšími než jeden den	2 prac. den	50

Příloha č. 8

Seznam použitých zkratek

AD	Active Ditectory
ADIS	Informační systém Daňové správy
AIS	Automatic Import Systém (Dovozní systém)
AISC	Agendový IS cizinců
AISEO	Agendový IS evidence obyvatel
ARES	Registr ekonomických subjektů
AVIS	Vnitřní informační systém
CEPAN	Centrální evidence přeplatků a nedoplatků
CIS	Cizinecký informační systém
CRS	Centrální registr
COPIS	Evidence duševního vlastnictví
CS	Celní správa
ČNB	Česká národní banka
ČSSZ	Česká správa sociálního zabezpečení
DES	Registr subjektů dělené správy
DAN	Detailní analýza
DS	Datová schránka
ECDC	Evidence celních dluhů - centrální
ECS	Celní řízení v režimu vývoz
e-Dovoz	Systém dovozu
EORI	Identifikátor subjektu v rámci celního řízení
ETN	Automatizovaný systém pro Evidenci tabákových nálepek
eSAT	Spisová služba
EPP	Evidence porušení právních předpisů
ETN	Evidence tabákových nálepek
ELPORT_B	Elektronická portálová brána (umístěná na cloudu)
EOsMA	Evidence osobního majetku
EUR	Evidence vydaných EUR
EVAP	Evidence analytických produktů
EVZ	Elektronické vyhodnocení zboží
eWDIS	Původní dovozní systém
FO	Fyzická osoba
FÚ	Finanční úřad
GAN	Globální analýza
GMS	Guarantee Management Systém (Globální záruky)

Havarijní postup	Proces, jehož cílem je dosažení alespoň částečného obnovení činnosti, pokud je IS z libovolného důvodu odpojen. Havarijně obnovená činnost nemusí být nutně podporovaná IS, ale např. papírovou procedurou.
HELPLINE	Aplikace pro evidenci případů požadavků o pomoc s řešením problému v dané oblasti
HW	hardvare
IC CS	Informační centrum celní správy
ICS	Aplikace pro e-dovoz
ICT	Information and Communication Technology – obvykle ekvivalent zkratky IT, informačních a komunikační technologie
IS	Informační systém
IS CS	Informační systém celní správy
ISKN	Informační systém Katastru nemovitostí
ISPAD	Informační systém pátrání a dohledu
ISVS	Informační systém veřejné správy – ve smyslu zákona 365/2000Sb. Je ISVS definován jako „soubor informačních systémů, které slouží pro výkon veřejné správy“. Hlavními znaky ISVS tedy jsou - přímá podpora výkonu veřejné správy a existence legislativní opory pro jeho zřízení a provoz. Do ISVS nepatří např. podsystémy pro provozní zajištění potřeb orgánu veřejné správy (personalistika, správa vlastního majetku orgánu, apod.).
ISZR	Informační systém Základních registrů
LIMS	Laboratorní informační a manažerský systém
MAK	Mák a konopí
MD	Mobilní dohled
MED	Modul exekucí a dražeb
ME-SPD	Modul spotřebních daní
MF	Ministerstvo financí
MKR	Mezinárodní kontrolní režimy
MPV	Mezinárodní vymáhání
NCTS	Celní řízení v režimu tranzit
OWNRES	Evidence nesrovnalostí v rámci TOR
PBL	Objednávkový systém pro pokutové bloky
PHM	Registr pohonných hmot
PO	Právnická osoba
RegSub	Registr subjektů
RDS	Registr daňových subjektů
ROB	Registr obyvatel
ROS	Registr osob
RSDS	Registr daňových subjektů
RUIAN	Registr územní identifikace adres a nemovitostí
RZMO	Registr zvláštních minerálních olejů
RZL	Registr značení lihu

SBM	Serena Bussines manager – centralizovaný systém ITSM Celní správy zajišťující i evidenci případů požadavků o pomoc s řešením problému v dané oblasti
SPD	Spotřební daň
SPR	Sdružená podpora rozhodování
SRA	Systém rizikové analýzy
SW	software
TARIC	Tarifní informační systém
Technologie	V kontextu informačních systémů: technické, programové a komunikační
TIS	Tarifní informační systém
TOR	Tradiční vlastní zdroje
VČP	Vlastní číslo plátce
VKC	Vnitřní kontrolní činnost
VSD	Vnitrostátní daně
VZP	Všeobecná zdravotní pojišťovna
VZ	Veřejná zakázka

Příloha č. 9

Vymezení pojmů

Provozní prostředí	Je práce s ostrými daty zpracovávanými v provozním prostředí (běžný provoz)
Testovací prostředí	Je práce s testovacími daty mimo provozní prostředí
Přístup na provozní prostředí celní správy zhotovitelem	Přístup na provozní prostředí zhotovitele je omezen přístupovým oprávněním pro daný uživatelský účet, pod dohledem pracovníků objednatele, který určí dle daných podmínek na dobu určitou rozsah přístupových práv. Přístup je bez možnosti změny dat a umožňuje analyzovat řešené provozní události i s vazbou na incidenty
Přístup na testovací prostředí celní správy zhotovitelem	Přístup na testovací prostředí zhotovitele je omezen přístupovým oprávněním pro daný uživatelský účet, pod dohledem pracovníků objednatele, který určí dle daných podmínek na dobu určitou rozsah přístupových práv.
Monitoring běhu aplikací zhotovitelem	Monitoring aplikací je umožněn zhotoviteli rozsahem přístupovým oprávněním pro provozní a testovací prostředí.
Incident	Jedna nebo více neočekávaných a nechtěných událostí majících za následek nefunkčnost aplikace a existuje vysoká pravděpodobnost nedostupnosti aplikačních služeb, nekonzistentnost zpracovaných dat či jejich nezpracování. Incidenty dělíme na blokující a neblokující celní a daňové řízení.
Závažný incident	Je incident blokující daňové řízení
Obecný incident	Z hlediska popisu hodnocení kvality se jedná o blokující incident, který není vyjmenován v definovaném incidentu.
Definovaný incident	Z hlediska popisu hodnocení kvality se jedná o blokující incident, který je vyjmenován v seznamu definovaných incidentu (viz příloha č. 7).
Incident z provozu cloudu	Jedna nebo více událostí majících za následek zvýšené náklady objednatele v souvislosti s provozem systému a jeho služeb na cloudu.
Vývoj aplikace v omezeném rozsahu	Jedná se o úpravu stávajících funkčnosti spočívající v doplňování či odebírání podmínek, nastavení filtrů, úpravy zobrazení výstupů, úpravy šablon, úpravy webových služeb, pohledů, úpravy z důvodu řešení incidentů

Závažné technické problémy	Závažným technickým problémem se rozumí skutečnosti způsobující nefunkčnost systému elektronického zpracování dat v díle
Bezproblémový chod aplikace	Odpovídá stavu aplikace bez závažných technických problémů, incidentů a závažných incidentů
Notifikace	Zaslání informace s odkazem na webovou stránku do emailové schránky zhotovitele či objednatele
Prokazatelné předání informace	Za prokazatelné předání informace je považováno zaslání emailu či zasílání notifikací do emailu.
Realizační tým	Realizační tým tvoří skupina oprávněných osob zhotovitele podle kvalitativních požadavků vyhlášené veřejné zakázky (zadávací dokumentace) řešící předmět smlouvy
Aplikací	Rozumíme jakýkoliv softwarový produkt pracující samostatně i s vazbou v prostředí celní správy
Systém řízení změn	Celní správa používá pro systém řízení změn systém Serena Bussines manager (SBM), který slouží k registraci, evidenci a další administrací požadavků. V případě přechodu objednatele z aplikace SBM na jinou aplikaci, má se za to, že povinnosti spojené v této smlouvě se SBM jsou přeneseny na aplikaci novou.
Centrum žádostí	Celní správa používá pro evidenci případů požadavků o pomoc s řešením problému v dané oblasti systém SBM, který slouží k registraci, evidenci a další administrací požadavků. V případě přechodu objednatele z aplikace SBM na jinou aplikaci, má se za to, že povinnosti spojené v této smlouvě se SRC jsou přeneseny na aplikaci novou.
Uživatel díla	Uživatelem se rozumí orgány státní správy a samosprávy a jejich zaměstnanci.
Rodný list aplikace	Je soubor definovaných informací o systému týkající se provozního chodu systému pro katalog aplikací.
Technická podpora a SBM	Zahrnuje údržbu veškerého aplikačního programového vybavení systému cPortál (nebo také jako „Programový produkt“) a související dokumentace, aktualizace Programového produktu ve vazbě na legislativní změny související s obecně závaznými právními předpisy, a to nejpozději do data nabytí jejich účinnosti, poskytování servisních prací zahrnujících řešení problémů s provozem Programového produktu, školení uživatelů, odborná poradenská, konzultační a metodická pomoc. Specifikace Programového produktu je obsažena v Příloze č. 1 této Smlouvy a specifikace Technické podpory a SBM je obsažena v Příloze č. 4 této Smlouvy.

	Zadávací a akceptační proces pro tyto práce a služby popisuje čl. 3.1 a následující této Smlouvy.
Poskytnutí prací a služeb	Poskytnutí prací a služeb spočívá: - ve zpracování detailních analýz (dále jen „DA“) ohledně možností úprav Programového produktu, transformace a migrace dat, - v samotných dílčích úpravách Programového produktu, - v transformaci a migraci dat v databázi, které není možné realizovat z uživatelského prostředí Programového produktu. Zadávací a akceptační proces pro tyto práce a služby popisuje čl. 3.1 a následující této Smlouvy.
Poskytnutí služeb	Poskytnutí služeb spočívá ve zpracování DA, v transformaci a přípravě dat pro umožnění jejich prezentace prostřednictvím BI nástrojů, a to dle požadavků Objednatele. Zadávací a akceptační proces pro tyto práce a služby popisuje čl. 3.1 a následující této Smlouvy.
Poskytnutí služeb v oblasti bezpečnostní problematiky	Poskytnutí služeb v oblasti bezpečnostní problematiky ve smyslu realizace opatření v oblasti kybernetické bezpečnosti systému při penetračním testování, implementaci a optimalizaci bezpečnostních opatření včetně reakce na kybernetické bezpečnostní incidenty v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZoKB“) a vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „VoKB“), a to dle požadavků Objednatele. Zadávací a akceptační proces pro tyto práce a služby popisuje čl. 3.1 a následující této Smlouvy.
Uplatnění doložky pro mimořádné stavy a události	Uplatnění doložky pro mimořádné stavy a události bude realizováno na základě nepředvídaných provozně technických změn, transformace, migrace, přechod na cloud apod., které objednatel nemohl při realizaci zakázky předvídat. Zadávací a akceptační proces pro tyto práce a služby popisuje čl. 3.1 a následující této Smlouvy.

Konzultační monitoring provozu	Konzultační monitoring provozu spočívá v komunikaci zhotovitele s IT provozem objednatele i v případě umístění systému(ů) na cloudu, zahrnující monitoring systému jeho výstupy, odezvy, chybová hlášení, nedostupnosti, HW a softwarové požadavky provozního prostředí. Konzultací se rozumí osobní, emailová, či telefonická konzultace, dále předání dohledových sestav, provozních a sledovacích výstupů HW ze systémového prostředí a SQL. V rámci konzultačního monitoringu mohou být po vyhodnocení bezpečnostních rizik dána zhotovitelům práva do provozního prostředí pro sledování chodu aplikace i dočasně. Zhotovitel obdrží kontakty na IT provoz.
IT provoz	Je provozní prostředí zajišťované v režii celní správy a jejími zaměstnanci či prostředí mimo režii celní správy např. cloud.
Modernizace systému	Modernizací se rozumí optimalizace chodu a výkonnosti systému, povýšení verzí, částečný nebo úplný přepis systému a jeho funkčností, cloudová řešení.
Zákaznický audit	Zákaznický audit objednatele ověřuje dodržování zákona o kybernetické bezpečnosti dodavatele. Zákaznický audit objednatele předpokládá vyplnění dotazníku, doložení skutečností a pohovor.
Pokyn k zahájení prací	Pokynem k zahájení práci při uplatnění doložky pro mimořádné události a smluvní opce je písemná výzva objednatele, která bude doručena do DS zhotovitele.
Privátní programy	Za privátní program je považován jakýkoliv programový produkt, který nesouvisí s předmětem plnění podle této smlouvy.

Příloha č. 10

BEZPEČNOSTNÍ PRAVIDLA PRO VÝZNAMNÉ A PRO BĚŽNÉ DODAVATELE INFORMAČNÍHO SYSTÉMU CELNÍ SPRÁVY ČESKÉ REPUBLIKY

ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI
Zákon č. 181/2014 Sb., kybernetické bezpečnosti a o změně souvisejících zákonů (ZoKB)
Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti (VoKB)

	Požadavky	Instrukce pro dodavatele - upřesnění
1.	***Řízení dodavatelů***	
1.1.	Dodavatel má povinnost se seznámit s pravidly objednatele, která zohledňují jeho požadavky systému řízení bezpečnosti informací a plnit je.	Dodavatel má povinnost dodržovat při plnění předmětu smlouvy příslušná ustanovení bezpečnostních politik, metodik a postupů předaných dodavateli objednatelem, resp. platné řídící dokumentace objednatele či její části anebo platné řídící dokumentace, k jejímuž dodržování se objednatel zavázal, pokud byl zhotovitel s takovými dokumenty nebo jejich částmi prokazatelně seznámen, a to bez ohledu na způsob, jakým byl s takovou dokumentací objednatele seznámen (např. školením, protokolárním předáním příslušné dokumentace zhotoviteli, elektronickým předáním prostřednictvím e-mailu, zřízením přístupu dodavateli na sdílené úložiště aj.) Dodavatel se dále zavazuje k zavedení a dodržování veškerých souvisejících bezpečnostních opatření požadovaných ZoKB a VoKB, a to minimálně po dobu poskytování plnění dle podmínek smlouvy.

2.	***Zvládání kybernetických bezpečnostních událostí a incidentů***	
2.1.	Dodavatel má povinnost oznamovat objednateli neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti.	

3..	***Příloha č. 7 VoKB - Řízení dodavatelů - bezpečnostní opatření pro smluvní vztahy***	
3.1.	Obsah smlouvy uzavírané s významnými dodavateli:	

	a) ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity),	Dodavatel se během plnění předmětu smlouvy pro objednatele zavazuje dostatečně zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost.
3.2.	b) ustanovení o oprávnění užívat data,	1. Vlastníkem všech dat a informací poskytnutých objednatelem dodavateli za účelem plnění předmětu smlouvy je objednatel, který k nim má primární užívací právo. 2. Dodavatel je při plnění předmětu smlouvy pro objednatele oprávněn užívat data předaná dodavateli objednatelem za účelem plnění předmětu smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu smlouvy. 3. Dodavatel se při poskytování plnění pro objednatele zavazuje nakládat s daty pouze v souladu se smlouvou a příslušnými právními předpisy, zejména ZoKB, VoKB a dalšími souvisejícími právními předpisy.2. Dodavatel je při plnění předmětu smlouvy pro objednatele oprávněn užívat data předaná dodavateli objednatelem za účelem plnění předmětu smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu smlouvy. 4. Dodavatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části technologického nebo komunikačního systému programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci technologického nebo komunikačního systému objednatele nebo nelegální získání dat a informací. V případě, že objednatel povolí dodavateli přístup do interní sítě a/nebo k technologickým a komunikačním systémům objednatele ze zařízení dodavatele, musí veškerá tato zařízení dodavatele splňovat příslušné bezpečnostní standardy objednatele.
3.9.	i) ustanovení o povinnosti dodavatele informovat povinnou osobu o:	

3.10.	1. kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,	1. Zhotovitel je povinen bezodkladně informovat objednatele prokazatelným způsobem o případném výskytu bezpečnostního incidentu souvisejícího s plněním smlouvy u zhotovitele. Kybernetický bezpečnostní incident je definován ustanovením § 7 odst. 2 ZoKB. 2. Zhotovitel informuje objednatele prostřednictvím zprávy zaslané na e-mailové adresy technického garanta objednatele a v kopii na e-mailové adresy: [redacted] Součástí informace o výskytu bezpečnostního incidentu budou základní údaje o povaze incidentu, čas jeho vzniku, popř. dopady na povinnosti zhotovitele spojené s plněním předmětu smlouvy. 3. Zhotovitel je povinen informovat objednatele o ukončení řešení bezpečnostního incidentu souvisejícího splněním smlouvy u zhotovitele. Zhotovitel informuje objednatele obdobným způsobem jako je uvedený v bodě 2.
	2. způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy,	Dodavatel se zavazuje informovat objednatele o způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním předmětu smlouvy.
	3. významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem,	Dodavatel má povinnost informovat neprodleně objednatele o změně ovládání dodavatele podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s aktivy určených k plnění dle předmětu smlouvy.
	j) specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně),	V případě jakéhokoliv ukončení smlouvy je dodavatel povinen poskytnout objednateli nebo objednatelem určené třetí osobě maximální nezbytnou součinnost za účelem plynulého a řádného převedení činností dle smlouvy či jejich části na objednatele nebo objednatelem určenou třetí osobu tak, s výjimkou případu, že by novým dodavatelem předmětu smlouvy byl stávající dodavatel této smlouvy, aby objednateli nevznikla újma (škoda) související s přechodem plnění předmětu smlouvy na nového dodavatele předmětu smlouvy. Dodavatel se zavazuje tuto součinnost poskytovat s odbornou péčí, zodpovědně v rozsahu, který po něm lze spravedlivě požadovat, a to do doby úplného

		převzetí takových činností objednatelem nebo objednatelem určenou třetí osobou.
3.11.	k) specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností),	Dodavatel se zavazuje dodržovat požadavky objednatele na řízení kontinuity činností, a to zejména požadavky na zahrnutí dodavatele do havarijních plánů, úkolů dodavatele při aktivaci řízení kontinuity činností apod.
3.12.	l) specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,	Dodavatel bere na vědomí, že objednatel může určit typ, rozsah, strukturu a formát dat, které dodavatel předá objednateli na základě požadavku objednatele. Nedohodne-li se objednatel s dodavatelem jinak, budou zákaznická data dodavatelem předána ve strukturovaném, běžně používaném, strojově čitelném a interoperabilním formátu. Objednatel určí lhůty k předání nebo zpřístupnění zákaznických dat a také dobu, po kterou budou případně data uschovaná dodavatelem po ukončení smlouvy.
P07 Politika řízení přístupu		
6.1.	Dodavatel bere na vědomí, že přístup k jednotlivým aplikacím a datům systému ICT smí být povolen pouze na základě úspěšné autentizace a autorizace uživatele.	Dodavatel bere na vědomí, že přidělení oprávnění zaměstnanci dodavatele musí být řízeno zásadou tzv. „potřeba vědět“ (need to know) a není nárokové.
6.2.	Přístupy musí být přidělovány identitě uživatele identifikované uživatelským jménem; identifikátory identity uživatele musí být jednoznačné a vždy spojitelné s konkrétní fyzickou osobou.	Dodavatel bere na vědomí, že přístup k datům, informacím či zařízením souvisejícím s předmětem smlouvy je možné povolit pouze fyzické identitě zaměstnance dodavatele nebo poddodavatele dodavatele zaevidované v seznamu oprávněných osob, a to na základě požadavku dodavatele na přístup. Dodavatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci dodavatele nebo poddodavatele dodavatele.
6.3.	Identita a její platnost musí být zavedena/měněna/rušena během procesu vzniku/změny/ukončení pracovního vztahu zaměstnance nebo na základě smluvního vztahu s dodavatelem.	
P22 Politika zvládání kybernetických bezpečnostních incidentů		

7.1.	Dodavatel bere na vědomí, že zhotovitel je oprávněn při přípravě a provedení testů Za přípravu a zvládání kybernetických bezpečnostních incidentů provedení testů součinnost potřebných zaměstnanců CS i dotčených dodavatelů externích služeb.

Ostatní bezpečnostní dokumentace objednatele	
8.1.	Dodavatel má povinnost se seznámit s pravidly objednatele, která jsou obsažena v níže uvedeném seznamu ostatní bezpečnostní dokumentace objednatele, a která zohledňují jeho požadavky systému řízení bezpečnosti informací a plnit je: a) P00 Politika kybernetické bezpečnosti ISCS b) P03 Politika organizační bezpečnosti c) P04 Politika řízení dodavatelů d) P05 Politika bezpečnosti lidských zdrojů e) P07 Politika řízení přístupu f) P22 Politika zvládání kybernetických bezpečnostních incidentů

Minimální bezpečnostní standard, NÚKIB, (ve vztahu k dodavatelům)		
9.1.	Dodavatel bere na vědomí, že objednatel je povinen poučit relevantní osoby dodavatele o jejich povinnostech, teoreticky a prakticky je školit, seznámit je s platnými bezpečnostními politikami a kontrolovat jejich dodržování.	
9.2.	V případě vyvíjeného informačního nebo komunikačního systému dodavatelem musí být definovány a dokumentovány následující požadavky: a) požadavky na licenční ujednání, vlastnictví kódu a práv duševního vlastnictví, b) požadavky na osvědčení kvality a správnosti provedených prací, c) požadavky na uložení zdrojového kódu, d) požadavky na právo přístupu k vývoji pro audit bezpečnosti a správnosti provedené práce, e) požadavky na smluvní podmínky na bezpečnost a zabezpečení kódu, f) požadavky na provedení testů zranitelnosti před instalací v produkčním prostředí.	
10.1.	V případě webových aplikací je dodavatel povinen zajistit vývoj dle principů definovaných ve standardu OWASP v aktuálním znění.	
10.2.	Dodavatel bere na vědomí, že má objednatel právo auditu zdrojového kódu a dodržování požadavků na bezpečnost.	V rámci podmínek plnění díla bude vždy předáván i aktuální zdrojový kód.