**Popis IS Registr CITES**

# **Základní informace**

Informační systém Registr CITES je součástí mezinárodního kontextu signatářů Úmluvy o  mezinárodním obchodu s ohroženými druhy volně žijících živočichů a planě rostoucích rostlin. Nejedná se o izolovaný projekt veřejné správy České republiky, vstupují do něj i zahraniční subjekty a jeho prostřednictvím probíhá mezinárodní (i mimounijní) výměna dat, takže není vhodné jej uzavírat do výlučně národních platforem. Systém musí zůstat zcela otevřený i v mezinárodním kontextu.

Bližší informace o agendě CITES jsou na webových stránkách Zadavatele <https://www.mzp.cz/cz/cites_obchod_ohrozenymi_druhy>.

Domovská stránka informačního systému Registr CITES je na adrese <http://cites.env.cz/>

Informační systém Registr CITES je dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů veden jako informační systém veřejné správy (ISVS): <https://rpp-ais.egon.gov.cz/AISP/verejne/isvs/zobrazeni-isvs/9409>.

Informační systém Registr CITES je dle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích veden jako významný informační systém.

Definice agendy CITES – obchodování s ohroženými druhy (včetně činností, rolí a úkonů) je k dispozici v registru práv a povinností na následující adrese: <https://rpp-ais.egon.gov.cz/gen/agendy-detail/A694_03072019.xlsx>.

# **Provozní prostředí**

Registr CITES je provozován na HW a v datových centrech Zadavatele nebo zajištěných Zadavatelem.

**Datové (LAN/WAN) sítě a komunikace**

* Servery připojeny rychlostí 1 Gb/s.
* Konektivita do sítě Internet rychlostí 1 Gb/s.
* Je nasazen systém firewallů.
* Pro komunikaci ve směru LAN->Internet povoleny pouze definované porty.
* Je nasazen systém bezpečnostních sond.
* Webový provoz ve směru Internet->LAN je směrován přes reverzní proxy (load balancer).
* VPN klient s dvoufaktorovým ověřením za pomocí SMS zpráv.

**Servery a diskové platformy**

* Výpočetní výkon: blade center technologie, takt procesorů min. 2,3 GHz
* Enterprise diskové pole min. 2000 IOPS
* FC SAN min. 10 Gb/s.
* Virtualizační platforma VMware vSphere 6, včetně funkce VMware HA (ochrana proti HW výpadku).
* Platforma pro běh aplikačních kontejnerů kompatibilní s Docker – vSphere Integrated Containers.

Zadavatel bude spravovat HW infrastrukturu a řešit incidenty na HW infrastruktuře. Zadavatel bude spravovat virtualizační prostředí a zajišťovat jeho licence (VMware), řešit incidenty na virtualizační platformě.

# **Popis stávajícího stavu**

Uplynutím času skončila servisní smlouva na podporu a rozvoj předmětného systému. Systém, jeho vlastnosti a služby jsou v rutinním provozu a vyhovují potřebám Zadavatele. Není potřeba je zásadně měnit. Je nutno zajistit trvale udržitelné poskytování a průběžné zlepšování a rozšiřování IT služeb poskytovaných Registrem CITES. Do budoucna pak postupný přechod do cloudové architektury.



**Schéma 1: Procesní architektonický diagram systému Registr CITES**

Agenda CITES sestává z celé řady procesů. V tomto diagramu jsou identifikovány všechny procesy a procesní role dané legislativou CITES včetně aktuální i budoucí možné interakce s okolím.

Procesy a procesní role označené světle žlutou barvou jsou nedílnou součástí aktuální implementace informačního systému Registr CITES.

Služby označené tmavší žlutou barvou reprezentují aktuálně využívané externí služby.

Konečně služby označené tmavou žlutooranžovou barvou jsou externí služby, jejich využití je plánováno v budoucnu v rámci běžného rozvoje systému Registr CITES.



**Schéma 2: Aplikační architektonický diagram systému Registr CITES**

Z diagramu je patrná aplikační architektura stávajícího systému s vazbami na okolí a procesní architekturu. Ke každé procesní skupině existuje jeden aplikační modul. Tyto moduly tvoří obchodní jádro Registru CITES.

Jádro používá vrstvu společných služeb sestávající se ze Správy, Autorizace, Registrace osob CITES a Výměny dat.

* Správa systému zajištuje veškerou administraci obsahu a nastavení systému
* Autorizace zajišťuje přístup kompetentním uživatelům ke službám systému
* Registrace osob CITES – zajišťuje registraci účastníků procesů CITES. Těmito účastníky mohou být jak uživatelé systému, tak i externí osoby – žadatelé o doklady CITES (například držitelé exemplářů, obchodníci, atd.). Osoby mohou být tuzemské i zahraniční. Je plánováno rozšíření funkcionality této služby o kontrolu identifikačních údajů tuzemských osob vůči Základním registrům.
* Výměna dat je služba umožňující autorizované přenosy dat mezi různými autoritami účastnícími se procesů CITES. V produkčním režimu probíhá výměna dat se Sekretariátem CITES, švýcarskou vydávací autoritou, celním systémem Single Window a EU-Twix. Služba je otevřená, takže lze připojovat i další autority a systémy. Do budoucna se počítá s napojením Registru CITES na připravovaný celounijní systém EU CITES.

Pomocí standardního otevřeného rozhraní odpovídajícího doporučení CITES e-Permitting Toolkit v2 mohou data CITES získávat i obecné autorizované systémy třetích stran.

Rozhraní CMS umožňuje interakci se službami umístěnými v CMS. Samotné služby Registru CITES mají mezinárodní charakter, musí být dostupné zahraničním autoritám, a proto nemohou být umístěny v CMS.

Obchodní jádro systému poskytuje své služby pomocí portálu prostřednictvím webového rozhraní.

Služby správy systému jsou poskytovány prostřednictvím rozhraní NRPC (Notes Remote Procedure Call).



**Schéma 3: Technologický architektonický diagram systému Registr CITES**

Informační systém Registr CITES prošel v posledních pěti letech zásadní modernizací, kdy byly provedeny změny vedoucí k přeměně původně sice modulárního, avšak monolitického systému na systém odpovídající architektuře orientované na služby (SOA). Z výše uvedených schémat je to jasně patrné.

1. Po procesní stránce Systém pokrývá veškeré agendy vyplývající z Úmluvy o mezinárodním obchodu ohroženými druhy volně žijících živočichů a planě rostoucích rostlin (Convention on International Trade in Endangered Species of Wild Fauna and Flora, CITES, Washingtonská úmluva) a související legislativy a to především nařízení EU v oblasti obchodování s ohroženými druhy a zákona č. 100/2004 Sb., o obchodování s ohroženými druhy, v platném znění. Česká republika je signatářem této Úmluvy. Součástí systému jsou i komunikační rozhraní se spolupracujícími orgány v mezinárodním kontextu. Komunikace probíhá na základě standardů stanovených Sekretariátem CITES. Součástí systému je i tvorba požadovaných reportingů.
2. Po aplikační stránce je systém dekomponován na samostatné aplikační moduly využívající několik společných služeb. Přístup ke službám je řízen na základě procesních rolí. Systém v současnosti poloautomaticky využívá služby základního registru RUIAN k obohacování dat. Po vyjasnění procesních omezení vyplývajících z legislativy (interakce národní legislativy s dohodou CITES) se počítá i s využitím služeb ROB a ROS pro ověřování tuzemských účastníků procesů CITES.
3. Technologicky se v posledních několika letech podařilo systém virtualizovat a dekomponovat na samostatné spolupracující uzly, které postupně dostávají charakter mikroslužeb. SW platforma použitá pro realizaci je hybridní. Používá se jak Open source software, jako zejména Linux, Apache Tomcat, NGINX, PostGIS, Pure Java, Python, Elastic search, Kibana atd., tak i komerční software, jím je platforma HCL Domino/Notes, která s výhodou umožňuje efektivní práci s NoSQL datovými objekty a poskytuje pokročilé messagingové služby.

Systém nevykazuje žádné závažné nedostatky a plní dobře svůj účel. Je však třeba zabránit jeho zastarávání, protože technologický vývoj přináší stále nové poznatky, které je třeba neustále do systému začleňovat, aby po čase nenastala potřeba nákladné modernizace nebo dokonce přestavby celého systému.

# **Aplikační architektura**

| Katalog všech aplikačních komponent řešení a klíčových aplikačních funkcí: |
| --- |
| Typ prvku | Název prvku | Vysvětlení významu aplikačních komponent, funkcí a služeb |
| **Komponenty, funkce a aplikační služby vytvářené nebo významně měněné v rámci záměru** (žádosti) |
| **komponenta** | Portál (GUI) | Jednotná ergonomie všechny uživatele Registru CITES v responzivním prostředí. Slouží pro přístup ke všem agendovým službám Registru CITES pro lidi i pro stroje. |
| **Komponenta** | Registr osob CITES | Registr všech osob vstupujících do procesů CITES. |
| **Komponenta** | Výjimky a registrační listy | Agenda vydávání a správy výjimek z obchodování a registračních listů.  |
| **komponenta** | Permity | Agenda vydávání permitů. |
| **komponenta** | Stanoviska vědeckého orgánu | Podpůrná agenda vydávání stanovisek vědeckého orgánu (AOPK).  |
| **komponenta** | Zadržené a zabavené exempláře | Agenda evidence zadržených a zabavených exemplářů, přestupků a Registr přestupců. |
| **komponenta** | Ostatní dokumenty CITES | Agenda vydávání ostatních dokumentů CITES.  |
| **komponenta** | Taxony | Komponenta pro vedení řízeného slovníku taxonů.  |
| **komponenta** | Analýza dat a reporting | Subsystém pro analýzu dat CITES vytváření požadovaných reportů a exportních datasetů. Subsystém využívá resortní Environmentální analytickou platformu (EAP) a je při vhodném použití je schopen generovat datasety pro OpenData. |
| **komponenta** | Single Window | Single Window je informační systém GŘC, se kterým probíhá komplexní dvoucestná výměna dat o vydání a použití povolení CITES k dovozu či vývozu exemplářů ohrožených druhů v rámci mezinárodního obchodu |
| **komponenta** | Informační systém třetí strany | Komponenta „Informační systém třetí strany“ představuje zejména informační systém cizí autority CITES (například probíhá výměna dat se švýcarskou autoritou) nebo systém nadnárodní autority. Ke standardizovanému rozhraní lze připojit i libovolný jiný systém.  |
| **služba** | Správa | Služba dostupná všem komponentám. Je určená k provádění správy celého systému Registr CITES a všech jeho komponent. |
| **služba** | Registrace osob | Služba dostupná relevantním komponentám. Realizuje proces Registrace osob. |
| **služba** | Autorizace | Služba vyhodnocující oprávnění uživatelů provádět konkrétní operace. Je dostupná relevantním komponentám. |

| Katalog aplikačních rozhraní (mezi dvěma různými komponentami A, B): |
| --- |
| Název aplikačního rozhraní | Komponenta A | Komponenta B | Vysvětlení obsahu a významu rozhraní aplikačních komponent |
| **Interní rozhraní** (aplikací řešení mezi sebou, na aplikace uvnitř úřadu, případně resortu, krajské korporace, apod.) |
| REST API | Obchodní jádro Registru CITES | Obchodní jádro Registru CITES | Preferované rozhraní používané jak pro vzájemnou komunikaci mezi komponentami Registru CITES a jednak pro komunikaci se systémy třetích stran.  |
| REST API | Obchodní jádro Registru CITES | Informační systém třetí strany | Preferované rozhraní používané jak pro vzájemnou komunikaci mezi komponentami Registru CITES a jednak pro komunikaci se systémy třetích stran. |
| NRPC | Obchodní jádro Registru CITES | Obchodní jádro Registru CITES | Některé komponenty obchodního jádra Registru CITES mezi sebou komunikují pomocí proprietárního rozhraní NRPR (Notes Remote Procedure Call). Toto rozhraní je postupně nahrazováno REST API. |
| CMS rozhraní | Obchodní jádro Registru CITES | Single Window | Standardní rozhraní Registru CITES nemůže být vzhledem k jeho charakteru mezinárodního informačního systému implementováno v rámci CMS. Systém GŘC Single Window však své služby poskytuje v rámci CMS, proto bylo třeba vytvořit rozhraní do CMS.  |
| Webová služba SOAP | Obchodní jádro Registru CITES | Informační systém třetí strany | Alternativní rozhraní pro datovou výměnu mezi Registrem CITES a systémy třetích stran. Aktuálně je jeho prostřednictvím připojen systém UNE-WCMC a švýcarská autorita CITES. Připojení švýcarské autority je v současné době v rekonstrukci kvůli přechodu Švýcarska na novou komunikační koncepci |
| **Externí rozhraní** (na aplikace eGovernmentu a jiných úřadů, případně jiná rozhraní) |
| Napojení na základní registry | Registr CITES | ISZR | Vazba na základní registry (4 základní registry):• ROB - Registr obyvatel;• RPP - Registr práv a povinností;• ROS - Registr osob;• RUIAN - Registr územní identifikace, adres a nemovitostí.  |

| Katalog aplikacemi podporovaných agend: |
| --- |
| Realizovaný systém | Agenda |
| Registr CITES | Vydávání permitů |
| Registr CITES | Vydávání výjimek z obchodování a registrace exemplářů |
| Registr CITES | Zadržené a zabavené exempláře |
| Registr CITES | Vydávání ostatních dokumentů CITES |
| Registr CITES | Výměna dat Single Window |
| Registr CITES | Poskytování dat a informací |
| Registr CITES | Analytické zpracování dat CITES a reporting |
| Registr CITES | Mezinárodní výměna dat |

# **Technologická architektura – IT technologie**

Fyzická infrastruktura je umístěna ve vlastním datacentru resortu MŽP. Rezortní datové centrum zabezpečuje jednotný centrální přístup všech organizací rezortu k aplikacím a jejích správě. Registr CITES je provozován v datacentru MŽP.

Dvě samostatné služby Servisní proxy a Exportní proxy EAP mají charakter bezstavové výměny dat, přičemž se v nich data neukládají a jsou umístěny v privátním cloudu a zahrnuty do celkového monitoringu Registru CITES.

Do budoucna je technicky možné provozovat celý systém Registr CITES jako SaaS. Návrh architektury s tím počítá a není jej třeba nijak měnit.

| Katalog uzlů a klíčových funkcí nebo služeb: |
| --- |
| Typ prvku | Název prvku  | Vysvětlení významu uzlu, funkce nebo služby |
| **Technologické zařízení** | Klientský informační systém | IS využívající IT služby Registru CITES |
| **Technologické zařízení** | Klientské zařízení | Uživatelské zařízení, pomocí kterého přistupují uživatelé k IT službám Registru CITES |
| **Technologická služba** | Produkční služby Registru CITES | Soubor služeb tvořících jádro Registru CITES |
| **Technologická služba** | Zálohování | Zálohovací služba Datacentra MŽP |
| **Technologická služba**  | Reverzní proxy | Vysvětlení je zřejmé z názvu prvku |
| **Technologický software** | Objektové úložiště | NoSQL úložiště datových objektů. Realizováno hybridně na HCL Domino a Elasticsearch.  |
| **Technologický software** | Messaging | Systém zasílání zpráv. Realizován hybridně na HCL Domino a Postfix.  |
| **Technologický uzel** | Portál a řadič | Uzel sdružující společné prezentační služby a autorizační část obchodní logiky.  |
| **Technologický uzel** | Notifikace | Vysvětlení je zřejmé z názvu prvku |
| **Technologický uzel** | Správa | Uzel poskytující služby správy systému |
| **Technologický uzel** | NGINX | Uzel realizující reverzní proxy |
| **Technologický uzel** | Permity | Vysvětlení je zřejmé z názvu prvku |
| **Technologický uzel** | Výjimky a registrační listy | Vysvětlení je zřejmé z názvu prvku |
| **Technologický uzel** | Ostatní dokumenty CITES | Vysvětlení je zřejmé z názvu prvku |
| **Technologický uzel** | Zadržené a zabavené exempláře | Vysvětlení je zřejmé z názvu prvku |
| **Technologický uzel** | Stanoviska AOPK | Vysvětlení je zřejmé z názvu prvku |
| **Technologický uzel** | Registr osob | Vysvětlení je zřejmé z názvu prvku |
| **Technologický uzel** | Taxony | Vysvětlení je zřejmé z názvu prvku |
| **Technologický uzel** | Analytika a reporting | Vysvětlení je zřejmé z názvu prvku |
| **Technologický uzel** | Servisní proxy | Uzel realizující služby zprostředkování a transformace služeb  |
| **Technologický uzel** | Exportní proxy EAP  | Uzel realizující synchronizaci datového jezera EAP s datovou základnou CITES. |

# **Technologická architektura – komunikační infrastruktura**

Komunikační infrastruktura pracuje s pěti základními lokalitami propojenými buď prostřednictvím veřejné sítě internet nebo privátní sítě veřejné správy KIVS.

* Lokalita MŽP – zde je provozován vlastní Registr CITES. Orgány veřejné správy využívají jeho služby prostřednictvím sítě KIVS nebo internet. Registr CITES se připojuje ke službám jiných orgánů veřejné správy prostřednictvím sítě KIVS nebo internet
* Lokalita GŘC (nebo jiného orgánu veřejné správy) – orgán poskytuje své služby (např. Single Window) prostřednictvím KIVS nebo internetu
* Lokalita servisní proxy – zajišťuje kompatibilitu poskytovaných a konzumovaných služeb a odolnost proti výpadkům komunikace. Služby poskytovány na internetu
* Lokalita exportní proxy EAP – zajišťuje poskytování služeb helperu, který předává data registru CITES k analytickým účelům platformě EAP. Služby poskytovány na internetu

Lokalita systému třetí strany – třetí strana (typicky zahraniční autorita) poskytuje své služby a/nebo konzumuje služby Registru CITES (typicky prostřednictvím servisní proxy) na internetu.

| Katalog infrastrukturních komunikačních funkcí, sítí, cest a klíčových služeb: |
| --- |
| Typ prvku | Název prvku | Vysvětlení významu infrastrukturních funkcí, sítí, cest a služeb |
| **Uzel**  | Komunikační prvky datového centra | Komunikační infrastruktura datového centra |
| **Komunikační funkce**  | Komunikační funkce lokality | Úplný souhrn komunikačních funkcionalit dané lokality |
| **Cesta**  | Routery | Vysvětlení je zřejmé z názvu prvku |
| **Cesta**  | Bezpečnostní brána - firewall | Vysvětlení je zřejmé z názvu prvku |
| **Komunikační síť**  | Internet | Vysvětlení je zřejmé z názvu prvku |
| **Komunikační síť**  | KIVS | Vysvětlení je zřejmé z názvu prvku |
| **Komunikační funkce**  | Rozhraní vzdálené správy | Rozhraní umožňující bezpečný vzdálený přístup správce.  |
| **Komunikační funkce**  | CMS připojení | Vysvětlení je zřejmé z názvu prvku |
| **Lokace** | Lokalita MŽP | Vysvětlení je zřejmé z názvu prvku |
| **Lokace** | Lokalita GŘC nebo jiného orgánu veřejné správy | Vysvětlení je zřejmé z názvu prvku |
| **Lokace** | Lokalita servisní proxy | Vysvětlení je zřejmé z názvu prvku |
| **Lokace** | Lokalita exportní proxy EAP | Vysvětlení je zřejmé z názvu prvku |
| **Lokace** | Lokalita systému třetí strany | Vysvětlení je zřejmé z názvu prvku |