Příloha č. 2

Kompletní technické specifikace informačního systému provozování hazardních her

Produkční prostředí – přístupové a provozní informace

Verze 1.0.0
19. 12. 2019

Ministerstvo financí, Letenská 15, 118 10, Praha 1

ID datové schránky: xzeaauv
e-mail: podatelna@mfcr.cz
Telefon: +420 257 041 111
Fax: +420 257 042 788

Obsah

1 Úvodní informace

Dokument je součástí "Kompletní technické specifikace informačního systému provozování hazardních her" a obsahuje doplňující informace provozního charakteru. Dokument obsahuje informace potřebné pro použití produkčního prostředí datového rozhraní, informace o použitých certifikátech a další důležité provozní informace.

Tento dokument se vztahuje vždy k aktuální zveřejněné verzi dokumentu "Kompletní technická specifikace informačního systému provozování hazardních her". Aktuální verze je 1.0.0.

Produkční prostředí je určeno pro provozovatele a slouží pro běžný provoz datového rozhraní, které zajišťuje ověření totožnosti a věku osob žádajících o registraci a sděluje informaci, zda konkrétní osoba je nebo není zapsána v rejstříku fyzických osob vyloučených z účasti na hazardních hrách. Rovněž jeho prostřednictvím dochází ke sdělení informace o přiděleném HID ověřované osobě.

1.1 Přehled zkratek a základních pojmů

Níže uvádíme definice zkratek a základních pojmů, které jsou používány v rámci textu tohoto dokumentu.

Zkratka	Definice
CA	Certifikační autorita
CRL	Certificate Revocation List
DNS	Domain Name Service
HTTP	Hypertext Transfer Protocol
Ministerstvo	Ministerstvo financí České republiky
Provozovatel	Provozovatel hazardních her ve smyslu ustanovení § 6 zákona o hazardních hrách
Služba	Umožňuje automatizované zpracování požadavku zaslaného z informačního systému provozovatele předepsaným způsobem a poskytuje odpověď na tento požadavek
Technická specifikace	Kompletní technická specifikace informačního systému provozování hazardních her týkající se rejstříku fyzických osob vyloučených z účasti na hazardních hrách podle ustanovení § 16 zákona o hazardních hrách a ověření totožnosti a věku osoby podle § 46 odst. 1 a § 77 odst. 6 zákona o hazardních hrách, a to v souladu s přechodným ustanovením § 137 zákona o hazardních hrách
TLS	Transport Layer Security
URL	Uniform Resource Locator
Zákon o hazardních hrách	Zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů
Zákon č. 297/2016 Sb.	Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů

2 Přístupové informace

2.1 URL a DNS jméno

Produkční prostředí je přístupné na URL https://api.hazard.mfcr.cz/rovo/v1, použit je standardní TCP port 443.

IP adresa odpovídající DNS jménu api.hazard.mfcr.cz se může v průběhu provozu produkčního prostředí měnit, a to jak při případných změnách vnitřní architektury serverového řešení, tak i v rámci DNS balancování (DNS záznam může vracet více IP adres podle aktuální dostupnosti částí neprodukčního prostředí). Informační systém provozovatele musí používat DNS jméno a respektovat TTL DNS záznamů. Při navazování nových spojení musí informační systém provozovatele vždy znovu pokládat dotaz na DNS záznam.

2.2 HTTP a TLS protokoly

Podporován je protokol HTTP/1.1, zabezpečený protokolem TLS verze 1.2 s omezenou sadou šifrovacích algoritmů nebo TLS verze 1.3.

Podporovaná sada šifrovacích algoritmů pro verzi TLS 1.2:

- ECDHE-RSA-AES128-GCM-SHA256 (0xc02f)
- ECDHE-RSA-AES256-GCM-SHA384 (0xc030)
- ECDHE-RSA-CHACHA20-POLY1305-SHA256 (0xcca8)

Podporovaná sada šifrovacích algoritmů pro verzi TLS 1.3 (pouze RSA verze):

- AES128-GCM-SHA256 (0x1301)
- AES256-GCM-SHA384 (0x1302)
- CHACHA20-POLY1305-SHA256 (0x1303)

Verze protokolu TLS a sady šifrovacích algoritmů se mohou v budoucnu z důvodů udržení vysoké úrovně zabezpečení měnit. Oznamování a nasazování verze protokolu TLS nebo sady šifrovacích algoritmů podléhá stejným pravidlům jako u nové verze rozhraní.

Persistentní HTTP spojení a více paralelních spojení od jednoho provozovatele jsou podporovány. Ministerstvo si vyhrazuje možnost ukončovat persistentní spojení ze strany serveru, např. po určitém čase nebo počtu přenesených HTTP požadavků, a to z důvodů optimalizace výkonu serverové platformy nebo z bezpečnostních důvodů.

2.3 Implementovaná verze datového rozhraní

Implementovaná verze datového rozhraní aktuální k momentu zveřejnění tohoto dokumentu je verze **1.0**.

Informace o nasazení a platnosti nových verzí datového rozhraní budou vždy zveřejněny na internetových stránkách ministerstva.

3 Certifikáty

3.1 TLS certifikát

TLS certifikát serveru bude vystaven některou z veřejných internetových certifikačních autorit, podporovaných v aktuálních verzích prohlížečů a operačních systémů, nebo některým z poskytovatelů služeb vytvářejících důvěru, který je zároveň kvalifikovaným poskytovatelem služeb vytvářejících důvěru podle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů (dále jen „zákon č. 297/2016 Sb.“).

Výměna TLS certifikátu serveru bude oznamována vždy minimálně 1 měsíc před vypršením jeho platnosti.

3.2 Podpisový certifikát ministerstva

Odpovědi ministerstva jsou opatřeny uznávanou elektronickou pečetí, vytvořenou na základě kvalifikovaného certifikátu pro elektronickou pečeť, vydaného kvalifikovaným poskytovatelem služeb vytvářejících důvěru ve smyslu zákona č. 297/2016 Sb.

Výměna podpisového certifikátu ministerstva bude oznamována vždy minimálně 1 měsíc před vypršením jeho platnosti.

3.3 Podpisový certifikát provozovatele

Certifikáty provozovatelů pro produkční prostředí jsou vydávány certifikační autoritou (dále jen „CA“) podle volby provozovatele, může jít o veřejnou i interní CA. Certifikáty musí být nahlášeny a zaevidovány postupem uvedeným v dokumentu "Kompletní technická specifikace informačního systému provozování hazardních her" včetně kompletního certifikačního řetězce. Kompletním certifikačním řetězcem (certificate chain) se rozumí kromě předmětného certifikátu i kořenový certifikát příslušné certifikační autority (root CA) a případných mezilehlých certifikačních autorit (intermediate CA) tak, aby bylo možné validovat platnost certifikátu a celý řetězec důvěry až ke kořenovému certifikátu CA.

Důvěryhodnost a bezpečnost zvolené CA a ochrana soukromých klíčů jsou v odpovědnosti provozovatele.

CRL příslušné certifikační autority a distribuční body CRL uvedené v certifikátech nebudou ze strany ministerstva aktivně využívány. V případě zneplatnění certifikátu musí provozovatel zároveň požádat o ukončení používání certifikátu způsobem popsaným v dokumentu "Kompletní technická specifikace informačního systému provozování hazardních her".

Certifikáty musí splňovat minimálně následující požadavky:

1) Algoritmy certifikátů vycházejí z doporučení Národního úřadu pro kybernetickou a informační bezpečnost (https://www.govcert.cz/download/doporuceni/Kryptograficke_prostredky_doporuceni_v1.0.pdf)
    - Algoritmy pro elektronický popis
        - Digital Signature Algorithm (DSA)
        - Rivest-Shamir-Adleman (RSA)
        - Elliptic Curve Schnorr Signature Algorithm (EC-Schnorr)
    - Algoritmy hashovacích funkcí
        - SHA-256

- SHA-384
- SHA-512
- SHA-512/256
- SHA3-256
- SHA3-384
- SHA3-512

2) Platnost certifikátu musí být podle jeho délky maximálně:

Délka certifikátu (bit)	**Platnost**
2048	<= 1 rok
3072	<= 2 roky
4096	<= 3 roky

Nahlášené a evidované certifikáty provozovatele jsou na produkčním prostředí primární a autoritativní identifikací provozovatele v zaslaných datových zprávách, atribut IČO/VČP je pouze informativní, pokud nebude odpovídat nahlášenému certifikátu, nebude se k němu přihlížet.

4 Provozní parametry

4.1 Provozní doba

Provozní doba produkčního prostředí je 7 dní v týdnu 24 hodin denně.

4.2 Dostupnost služby

V případě, že se nepodaří dovolat službě, je nejdříve doporučeno s ohledem na koncepci rozhraní jako vysoce dostupného:

1. Zavolat službu opakovaně s navázáním nových HTTPS spojení.
2. Zkontrolovat síťovou konektivitu

Pokud se i přesto nepodaří dovolat službě, kontaktujte podporu ministerstva.

5 Podpora

5.1 Service Desk ministerstva

Podpora provozu produkčního prostředí je poskytována prostřednictvím Service Desku ministerstva. Aktuální přístupové údaje Service Desku ministerstva (web, e-mail, telefon) budou od zahájení provozu PG vždy zveřejněny na internetových stránkách ministerstva.

5.2 Kontaktní osoby

Pro komunikaci prostřednictvím Service Desku ministerstva musí být provozovatelem vždy nahlášena kontaktní osoba pro Service Desk. Provozovatel kontaktní osoby pro Service Desk nahlásí podáním zaslaným ministerstvu způsobem podle § 12 odst. 2 vyhlášky č. 10/2019 Sb. V tomto podání je nutné ke každé kontaktní osobě pro Service Desk uvést jméno, příjmení, telefonní číslo, e-mailovou adresu a provozovatele, za kterého bude tato kontaktní osoba jednat. Kontaktní osoba pro Service Desk bude moci za provozovatele pokládat dotazy v případě, že bude nutné poskytnout ze strany ministerstva podporu v rámci produkčního prostředí, neprodukčního prostředí nebo vznášet související dotazy.

V případě, že provozovatel chce využít možnost nahlásit kontaktní osobu pro certifikáty, postupuje způsobem uvedeným v předchozím odstavci, u těchto kontaktních osob pro certifikáty však navíc nutné uvést, že tyto osoby jsou oprávněny jednat za provozovatele prostřednictvím Service Desku ministerstva ve věcech týkající se certifikátů. Kontaktní osoby pro certifikáty může provozovatel rovněž nahlásit v žádosti o zaevidování certifikátů, tedy současně se zasláním certifikátů. Takto nahlášené osoby mají nad rámec oprávnění uvedených v předchozím odstavci také oprávnění za provozovatele jednat a komunikovat v rámci všech jeho nahlášených certifikátů.

Nově nahlášené kontaktní osoby budou kontaktovány ze strany Service Desku ministerstva a budou nastavena přístupová hesla pro autentizované kanály podpory (zejména web).

Kontaktní osoby lze opakovaným použitím této procedury doplňovat a/nebo ukončovat jejich oprávnění. Jedna osoba může být kontaktní osobou pro více provozovatelů, musí být ale nahlášena každým z těchto provozovatelů samostatně.

Vzory žádosti o nahlášení kontaktní osoby pro Service Desk a o ukončení oprávnění kontaktní osoby pro Service Desk budou dostupné na internetových stránkách ministerstva.