



Příloha č. 2

Kompletní technické specifikace/dokumentace informačního systému provozování hazardních her

Produkční prostředí – přístupové a provozní informace

Verze 2.0.0

Platnost: 30. 1. 2024

Účinnost: 1. 7. 2024



Historie dokumentu

Verze	Název dokumentu	Datum platnosti/účinnosti	Popis změn
1.0.0	Příloha č. 2 Kompletní technické specifikace informačního systému provozování hazardních her Produkční prostředí – přístupové a provozní informace	Platnost: 19. 12. 2019 Účinnost: od 20. 12. 2020 do 30. 6. 2024	První verze
2.0.0	Příloha č. 2 Kompletní technické specifikace/dokumentace informačního systému provozování hazardních her Produkční prostředí – přístupové a provozní informace	Platnost: 30. 1. 2024 Účinnost: od 1. 7. 2024	<ol style="list-style-type: none">1) Úprava textu kapitoly „1 Úvodní informace“ zohledňující rozšíření služeb daného rozhraní.2) Úprava/doplnění zkratk a definic – viz kapitola 1.1.3) Změna URL produkčního prostředí – viz kapitola 2.14) Doplnění informací k implementaci nové verze datového rozhraní a souběhu s verzí 1.0 – viz kapitola 2.35) Změna lhůty pro oznamování výměny TLS certifikátu serveru a podpisového certifikátu ministerstva – viz kapitola 3.1 a 3.2.6) Drobné formální úpravy – celý dokument



Obsah

1	Úvodní informace	4
1.1	Přehled zkratk a základních pojmů.....	5
2	Přístupové informace	6
2.1	URL a DNS jméno.....	6
2.2	HTTP a TLS protokoly.....	6
2.3	Implementovaná verze datového rozhraní	6
3	Certifikáty	7
3.1	TLS certifikát	7
3.2	Podpisový certifikát ministerstva	7
3.3	Podpisový certifikát provozovatele.....	7
4	Provozní parametry	9
4.1	Provozní doba	9
4.2	Dostupnost služby	9
5	Podpora	9
5.1	Service Desk ministerstva	9
5.2	Kontaktní osoby	9



1 Úvodní informace

Dokument je součástí "Kompletní technické specifikace/dokumentace 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 k dokumentu "Kompletní technická specifikace/dokumentace informačního systému provozování hazardních her", verze 2.0.0, který je účinný od 1. 7. 2024.

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

Dále zajišťuje přijetí oznámení o využití prostředku pro zamezení účasti na hazardní hře (resp. na zápis osoby do rejstříku) na 48 hodin včetně odeslání zprávy o jeho zpracování (příp. nezpracování) a přijetí podání žádosti o vyloučení z účasti na hazardní hře (resp. žádosti o zápis osoby do rejstříku) prostřednictvím provozovatele. Komunikace probíhá s využitím HID osoby, již se informace nebo žádost týká.



1.1 Přehled zkratk a základních pojmů

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

Zkratka	Definice
CA	Certifikační autorita
CRL	Certificate Revocation List
DNS	Domain Name Service
HID	Herní identifikátor osoby
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 zaslání z informačního systému provozovatele předepsaným způsobem a poskytuje odpověď na tento požadavek
Technická specifikace/dokumentace	Kompletní technická specifikace/dokumentace informačního systému provozování hazardních her zahrnující jak technickou specifikaci dle ustanovení § 137 odst. 1 zákona o hazardních hrách, tak technickou dokumentaci dle ČÁSTI PADESÁTÉ TŘETÍ, Čl. XCIV, bodu 7 přechodných ustanovení zákona č. 349/2023 Sb., kterým se mění některé zákony v souvislosti s konsolidací veřejných rozpočtů
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
§ 12 odst. 2 vyhlášky č. 10/2019 Sb.	§ 12 odst. 2 vyhlášky č. 10/2019 Sb. ve znění účinném do 31. 12. 2023 (v souladu s přechodným ustanovením § 14 odst. 5 vyhlášky č. 466/2023 Sb., o podmínkách provozování hazardních her). V § 12 odst. 2 vyhlášky č. 10/2019 Sb. je uvedeno, že Plní-li provozovatel povinnost spočívající v oznámení nebo zasílání jiných informací ministerstvu, činí se podání v elektronické podobě podepsané způsobem, se kterým jiný právní předpis spojuje účinky vlastnoručního podpisu.



2 Přístupové informace

2.1 URL a DNS jméno

Produkční prostředí verze 2.0.0 bude po zveřejnění přístupné na URL <https://api.hazard.mfcr.cz/rovo/v2>, 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 datového 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

Datové rozhraní verze **1.0** v nezměněné podobě bude na produkčním prostředí dostupné do 30. 6. 2024 (včetně). Nové datové rozhraní verze **2.0** bude dostupné před datem 1. 7. 2024, přičemž konkrétní datum publikace verze 2.0 bude zveřejněno na webových stránkách ministerstva v dostatečném předstihu. Souběh verzí umožní integraci na nové datové rozhraní verze 2.0 na straně provozovatelů v čase (po spuštění nové verze produkčního prostředí), který si sami zvolí, avšak nejpozději do 1. 7. 2024.



3 Certifikáty

3.1 TLS certifikát

TLS certifikát serveru bude vždy 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.

Výměna TLS certifikátu serveru bude oznamována vždy minimálně 14 kalendářních dnů před vypršením jeho platnosti.

3.2 Podpisový certifikát ministerstva

Odpovědi ministerstva budou vždy 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 14 kalendářních dnů před vypršením jeho platnosti.

3.3 Podpisový certifikát provozovatele

Certifikáty provozovatelů pro produkční prostředí jsou vydávány CA podle volby provozovatele, může jít o veřejnou i interní CA. Certifikáty musí být nahlášeny a zaevidovány postupem uvedeným v dokumentu Kompletní technická specifikace/dokumentace 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 popsáním v dokumentu "Kompletní technická specifikace/dokumentace 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/doporuzeni/Kryptograficke_prostredky_doporuce_ni_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) jsou 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 jsou dostupné na [internetových stránkách ministerstva](#).