FAQ

Často kladené dotazy

k vyhlášce č. 10/2019 Sb., o způsobu oznamování a zasílání informací a přenosu dat provozovatelem hazardních her, rozsahu přenášených dat a jiných technických parametrech přenosu dat

TECHNICKÉ DOTAZY A ODPOVĚDI

Ministerstvo financí, odbor 73 – Procesní agendy a regulace hazardu, zveřejňuje v rámci metodické činnosti za účelem snadnější implementace vyhlášky č. 10/2019 Sb., o způsobu oznamování a zasílání informací a přenosu dat provozovatelem hazardních her, rozsahu přenášených dat a jiných technických parametrech přenosu dat (dál jen „reportingová vyhláška“), následující seznam často kladených dotazů.

Seznam často kladených dotazů bude průběžně doplňován a dle potřeby aktualizován.

9. 3. 2020

Verze 3.0

Obsah

Použité zkratky

Reportingová vyhláška - vyhláška Ministerstva financí č. 10/2019 Sb., o způsobu oznamování a zasílání informací a přenosu dat provozovatelem hazardních her, rozsahu přenášených dat a jiných technických parametrech přenosu dat

ZHH nebo **zákon o hazardních hrách** - zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů

MF, Ministerstvo – Ministerstvo financí ČR

CS - Celní správa

Poznámka k verzi – nově obsažené otázky jsou v rámci kapitoly či podkapitoly odděleny příznakem **NOVÉ**

1. Komunikační parametry a registrace

Kde najdu popis jednotlivých položek registračního formuláře?

V Pokynech k vyplnění, které jsou dostupné přímo z registračního formuláře, odkazem na záložce v pravém horním rohu formuláře https://forms.celnisprava.cz/aforms.php?action=fill&id_form=159.

Co znamenají následující výrazy:

a) **kvalifikovaný certifikát provozovatele pro uznávanou elektronickou pečeť (§ 2 odst. 1, písm. a) reportingové vyhlášky),**
b) **certifikát veřejného klíče provozovatele (§ 2 odst. 1, písm. b) reportingové vyhlášky),**
c) **šifrování souboru (§ 2 odst. 1, písm. b), bod 1 reportingové vyhlášky,**
d) **autentizace při šifrovaném autentizovaném přenosu.**

Výše uvedené prvky obecně slouží pro zabezpečení komunikací a dat při poskytování automatizovaných výstupů, a to jak pro vzájemné ověření identity provozovatele a orgánu vykonávajícího dozor, tak i pro ochranu dat (šifrování).

Ad a) Kvalifikovaný certifikát pro uznávanou elektronickou pečeť v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, vydaný kvalifikovaným poskytovatelem služeb vytvářejících důvěru (např. První certifikační autorita, PostSignum, eIdentity, ale i jiné v EU v souladu s eIDAS). Certifikát ve formátu X.509 spojuje data pro ověřování platnosti elektronických pečetí (veřejné klíče) s určitou právnickou osobou a potvrzuje název této osoby. Elektronická pečeť je obdobou elektronického podpisu, není vázána na konkrétní fyzickou osobu, ale na právnickou osobu a jejím účelem je prokázat původ a integritu dat. Certifikát musí být vydán pro právnickou osobu (IČO) provozovatele - neplatí na Playground (veřejné testovací rozhraní).

Ad b) Certifikát ve formátu X.509 spojuje veřejný klíč se subjektem, který disponuje odpovídajícím soukromým klíčem. Certifikát je vydán certifikační autoritou dle výběru provozovatele (může být i interní), údaje o certifikační autoritě musí být předány spolu s certifikátem. Zvolená délka soukromých klíčů, bezpečná správa soukromých klíčů a výběr důvěryhodné certifikační autority jsou klíčovými prvky zabezpečení poskytování automatizovaných výstupů a jsou v odpovědnosti provozovatele.

Ad c) Kódování přenášené informace pomocí klíče nebo klíčů tak, aby nebyla srozumitelná třetí osobě. Pro šifrování jsou použity formáty CMS (dle RFC 5652) a metody asymetrické kryptografie s využitím X.509 certifikátů. Šifrování provádí vždy původce informace s využitím šifrovacího certifikátu (tj. veřejného klíče) příjemce, příjemce dešifruje pomocí svého soukromého klíče. Formát CMS umožňuje šifrovat stejnou informaci pro více příjemců, často využívanou možností je šifrovat pro příjemce i pro původce (sama sebe), což umožňuje pozdější kontrolu šifrovaného obsahu původcem.

Ad d) Konkrétně jde o využití klientských certifikátů při HTTPS komunikaci za účelem ověření totožnosti strany iniciující HTTPS spojení.

Jaký je význam a správná hodnota pole Datum platnosti při prvotní registraci komunikačních parametrů ostrého prostředí, vzhledem k datu účinnosti vyhlášky 1.6.2019?

Provozovatel musí do 2.5.2019 pro každou hru a kasino registrovat komunikační parametry s datem platnosti odpovídající zahájení jeho povinnosti poskytovat automatizované přístupy v souladu s reportingovou vyhláškou, což je pro většinu případů již povolených her a kasin 1.6.2019. Dřívější datumy budou zpracovány stejně jako by bylo vloženo 1.6.2019. **Musíme mít k 2.5.2019 zaregistrována všechna kasina, za která budeme v malém modelu odesílat data? Nebo stačí mít zaregistrováno 1 a ostatní doplnit nejpozději 5 pracovních dní před účinností reportingové vyhlášky? Pro doplnění dalších kasin máme použít typ podání - oznámení k registraci údajů nebo použít typ podání oznámení o změně?**

K 2. 5. 2019 měly být zaregistrovány komunikační parametry pro všechna kasina, ve kterých bylo zahájeno provozování živé hry.

Co se týká dotazu k registraci nových kasin, je nutné užít formulář Oznámení o registraci údajů, kde uvedete kompletní údaje pro všechna nově registrovaná kasina. Pokud by docházelo ke změně pouze některých komunikačních parametrů u již zaregistrovaných kasin, tak bude užit formulář Oznámení o změně. Blíže viz Pokyny k vyplnění (https://forms.celnisprava.cz/aforms.php?action=fill&id_form=159).

Kdy používat oznámení o změně a kdy oznámení k registraci?

Typ podání „oznámení k registraci“ slouží k nastavení nebo změně kompletní sady konfiguračních parametrů pro sadu automatizovaných výstupů. V případě registrace jiných parametrů s dřívějším datem platnosti dojde k uvedenému Počátečnímu datu platnosti k jejich přepsání.

Oznámení k registraci je možno podávat opakovaně s různými daty platnosti, systém pracuje vždy s nejnovější registrací s nejbližším Počátečním datem platnosti. Pokud má provozovatel k dispozici plnou sadu komunikačních parametrů (například uloženou v XML), je doporučeno používat opakovanou registraci.

Typ podání „oznámení o změně“ slouží ke změně pouze některých komunikačních parametrů, ve formuláři nemusí být vyplněna kompletní sada parametrů. K uvedenému Počátečnímu datu platnosti dojde ke změně uvedených komunikačních parametrů, ostatní zůstávají v platnosti z předchozí konfigurace.

Oznámení o změně je určeno primárně pro případy, kdy provozovatel nemá k dispozici plnou sadu komunikačních parametrů (certifikátů) a chce změnit pouze některé, např. pouze autentizační certifikát.

Podmínkou přijetí oznámení o změně je předchozí úspěšné zpracování alespoň jedné registrace pro uvedené řady automatizovaných výstupů.

Je přidání nového kasina oznámením o změně nebo oznámením o registraci?

Jde o registraci nové řady automatizovaných výstupů, nelze použít oznámení o změně. Je možno zopakovat původní registraci (např. pokud ji má provozovatel uloženou v XML) s

doplněným kasinem a novým datem platnosti, nebo uvést pouze jedno kasino. Jednotlivé registrace se v systému skládají a vždy jsou používány ty nejaktuálnější.

NOVÉ

Jak postupovat při změně údajů nutných k technickému zabezpečení poskytování automatizovaného výstupu orgánu vykonávajícího dozor (např. obnova certifikátů orgánu vykonávajícího dozor)?

Platí pro Playground i ostré prostředí. Orgán vykonávající dozor publikuje své změněné údaje nutné k technickému zabezpečení poskytování automatizovaného výstupu. předem na webu MF https://www.mfcr.cz/cs/soukromy-sektor/hazardni-hry/reportingova-vyhlaska/komunikacni-parametry. Orgán vykonávající dozor oznámí změnu těchto údajů rovněž provozovateli sdělením v souladu s § 2 odst. 4 reportingové vyhlášky. Nejčastěji se bude jednat o změnu certifikátu, přičemž tento proces je přiblížen níže.

Orgán vykonávající dozor zároveň oznámí datum změny certifikátů (v závislosti na platnosti stávajících certifikátů se může měnit jeden nebo více certifikátů).

V případě změny certifikátu pro elektronickou pečeť orgánu vykonávajícího dozor (použitého pečetění potvrzovacích zpráv) je provozovatelům doporučeno nastavit ve svých systémech před datem změny oba pečetící certifikáty (starý i nový) jako důvěryhodné a po termínu výměny certifikátu starý certifikát z konfigurace vyjmout.

V případě změny šifrovacího certifikátu orgánu vykonávajícího dozor (použitého pro šifrování datových balíčků provozovatelem) je provozovatelům doporučeno nastavit ve svých systémech před datem změny oba šifrovací certifikáty (starý i nový) a použít pro zašifrování datových balíčků oba certifikáty a po termínu výměny certifikátu starý certifikát z konfigurace vyjmout. V případě chybného postupu dojde k odmítnutí balíčků z důvodu nemožnosti rozšifrovat.

V případě změny serverového TLS certifikátu orgánu vykonávajícího dozor (pro přístup k administrační aplikaci Komunikačního rozhraní a pro stahování potvrzovacích balíčků uložených na serveru orgánu vykonávajícího dozor) provozovatel pravděpodobně nemusí dělat žádné změny, pokud se zároveň nemění vydávající certifikační autorita. V případě potřeby změn doplní nové certifikáty do příslušných úložišť certifikátů (trust store, keychain,…) ve svých systémech před termínem změny.

V případě změny klientského TLS certifikátu orgánu vykonávajícího dozor (pro autentizaci orgánu vykonávajícího dozor při odesílání notifikací o potvrzovacím balíčku provozovateli) je provozovateli doporučeno doplnit před termínem změny nové autentizační certifikáty do konfigurace svého web serveru nebo aplikace.

Jak postupovat při změně údajů nutných k technickému zabezpečení poskytování automatizovaného výstupu provozovatele (např. při obnově certifikátů) na straně provozovatele?

V případě změny kteréhokoliv certifikátu provozovatele je provozovatel povinen provést registraci změn 5 pracovních dní předem prostřednictvím webového formuláře Celní správy *https://forms.celnisprava.cz/aforms.php?action=fill&id_form=159*. Lhůta 5 pracovních dnů

slouží primárně pro zpracování změny registrace pracovníky Celní správy a vložení změny do systému a je stanovena v reportingové vyhlášce.

Doporučujeme provozovatelům následující postup:

1) Zajistit si nový certifikát v dostatečné předstihu před exspirací stávajícího.
2) Nejpozději 5 pracovních dnů před termínem plánované změny na straně provozovatele (která musí být nejpozději v den exspirace stávajícího certifikátu) provést změnu registrace - přidání nového certifikátu. Jako Počáteční datum platnosti uvede provozovatel den změny certifikátu ve svém systému.
3) Pokud budou v den změny certifikátu zaregistrovány oba certifikáty (starý i nový), může provozovatel reálně provést výměnu kdykoliv během dne, orgán vykonávající dozor bude používat oba certifikáty. *Pokud by Provozovatel zároveň ke stejnému Počátečnímu datu platnosti zrušil registraci starého certifikátu (nedoporuceno), musí změnu provést přesně v 00:00 hodin daného dne.*
4) Po ověření změny provozovatel provede druhou změnu registrace - odebrání starého certifikátu.

Je nutné měnit certifikát v konkrétní den nebo hodinu?

Nikoli. Při správném časování registrace certifikátů je možné implementovat přechodné období, kdy je bez ztráty funkčnosti možné používat jak starý, tak nový certifikát. Pro využití přechodného období je třeba vytvořit nové certifikáty a registrovat je s dostatečným předstihem před exspirací starých certifikátů. Komunikace bude fungovat v případě, kdy je v aktuálně platných komunikačních parametrech uveden alespoň jeden platný certifikát daného typu. Pro změnu certifikátu vždy využijte dostatečně dlouhé přechodné období, kdy můžete používat oba certifikáty a kdy budete mít možnost provést změnu certifikátu v libovolném okamžiku tohoto přechodného období.

Jaký je doporučený postup registrace změny certifikátů vůči orgánu vykonávajícímu dozor?

Webový formulář Celní správy *https://forms.celnisprava.cz/aforms.php?action=fill&id_form=159* nabízí dvě možnosti pro registraci změny certifikátů.

Typ podání **Oznámení k registraci** - **doporučená varianta** - slouží k nastavení nebo nahrazení kompletní sady konfiguračních parametrů pro všechny řady automatizovaných výstupů uvedené ve spodní části formuláře. Předpokladem použití tohoto mechanismu je schopnost provozovatele kompletně vyplnit všechny položky formuláře novým nastavením - toho lze nejsnáze dosáhnout pomocí systematického ukládání obsahu formuláře do XML souboru pomocí tlačítka "Uložit data formuláře". Každou změnu pak lze provádět pomocí nahrání obsahu formuláře pomocí tlačítka "Načíst data do formuláře", úpravou dat a opětovným uložením do XML před odesláním podání. Výhodou tohoto postupu je nahrazení všech předchozích konfigurací - není třeba řešit vazby na předchozí registrace a změny. Tímto postupem lze provést přidání i odebrání certifikátů.

Typ podání **Oznámení o změně** slouží ke změně pouze některých komunikačních parametrů, což zahrnuje i přidání certifikátů. Ve formuláři nemusí být vyplněna kompletní sada parametrů, stačí pouze nové certifikáty, které jsou doplněny ke stávající registraci. Výhodou tohoto postupu je jednoduchost vyplnění. Nevýhodou je vazba na předchozí

registrace, při opakovaném použití změny mohou vzniknout netriviální kombinace změn a obtížně predikovatelný výsledný stav registrací. Tímto postupem dále není možno provést odebrání certifikátu, takže neplatné certifikáty se budou v registraci hromadit.

V obou případech je nutné ve formuláři uvést všechny řady automatizovaných výstupů (balíčkové řady) provozovatele, včetně identifikace všech kasin malého modelu, pro které je certifikát měněn. V případě opomenutí některé balíčkové řady zůstává pro tuto řadu v platnosti původní registrace.

Typ podání **Oznámení o zrušení** nelze pro změnu certifikátů použít, slouží pouze pro odebrání registrované řady automatizovaných výstupů (balíčkové řady).

Jak postupovat při obnově certifikátů na Playgroundu?

Obnova certifikátů na Playgroundu probíhá nezávisle na ostrém prostředí a stejným postupem, pouze s využitím webového formuláře pro Playground na adrese *https://forms.celnisprava.cz/aforms.php?action=fill&id_form=157*.

Na Playgroundu lze navíc s výhodou využít funkce samoobslužné registrace, která funguje následovně. Místo odeslání formuláře do datové schránky nebo na e-podatelnu s elektronickým podpisem provozovatel uloží podání pomocí tlačítka "Uložit data formuláře dle XSD Hazard" do XML souboru ve speciálním fomátu "XML Hazard" (odlišný od formátu XML pro běžné ukládání a znovunahrání obsahu formuláře). Tento soubor pak provozovatel vloží na stránce *https://reporting-pg.hazard.spcss.cz/apps/reg-db/import-form* do administrační aplikace Komunikačního rozhraní. V případě chyb podání tato stránka vrátí informaci o chybách, jinak okamžitě vloží registraci do registrační databáze. Registrace je platná a použitá systémem od nejbližší půlnoci.

Podmínkou použití samoobslužné registrace je použití platného (neexspirovaného) zaregistrovaného klientského autentizačního certifikátu (certifikát pro autentizaci klienta).

Jak zkontrolovat stav registrace certifikátů?

Provozovatel si může zkontrolovat své registrace v registrační databázi systému na adrese *https://reporting-hazard.celnisprava.cz/apps/reg-db/registration-list* (ostré prostředí) a *https://reporting-pg.hazard.spcss.cz/apps/reg-db/import-form* (Playground).

Jednotlivé řádky výpisu odpovídají registracím pro jednotlivé registrované balíčkové řady. Každou řádku lze rozkliknout a získat detailní přehled registrovaných certifikátů. Seznam lze filtrovat a třídit pomocí různých atributů zobrazených v horní řádce nebo dále zobrazených tlačítkem Filtrovat.

V režimu zobrazení "Vše" (políčko v levém horním rohu) stránka zobrazuje celou historii registrací, ve které se lze orientovat podle data podání a data platnosti. Typ podání je zobrazen ve sloupci Operace.

V režimu zobrazení "Platné k datu" lze zadat datum (aktuální nebo historické) a systém zobrazí pro každou registrovanou balíčkovou řadu jen jeden záznam se všemi certifikáty platnými k danému datu. Tato funkce je užitečná pro odfiltrování historie nebo pro vyjasnění výsledku registrací typu Oznámení o změně.

2. Datové balíčky

Co znamená, že orgán vykonávající dozor přistoupí k adrese …. (§ 3 odst. 2 reportingové vyhlášky)?

Provozovatel umístí datový balíček na svůj web server dostupný na síti Internet (na URL adrese poskytnuté při registraci komunikačních parametrů) a ponechá jej na něm do té doby, než orgán vykonávající dozor potvrdí jeho přijetí potvrzovacím balíčkem. Orgán vykonávající dozor si datový balíček sám "stahuje" z definované URL adresy na web serveru provozovatele.

Jak dlouho máme uchovávat datové balíčky na serveru provozovatele?

Reportingová vyhláška stanoví, že orgán vykonávající dozor dle vyhlášky stáhne aktualizovaný výstup nejpozději do 7 dnů (to neplatí v případě živelné pohromy nebo jiné mimořádné události). Provozovatel by měl automatizovaný výstup ponechat do obdržení potvrzovacího balíčku (viz § 3 odst. 4 reportingové vyhlášky).

Jak často a jak dlouho kontroluje server orgánu vykonávajícího dozor přítomnost datových balíčků na server provozovatele?

Reportingová vyhláška stanoví pro vzdálený přístup povinnost provozovatele vystavit automatizovaný výstup do 8 hodin po ukončení příslušného reportovacího období. Orgán vykonávající dozor dle vyhlášky stáhne aktualizovaný výstup nejpozději do 7 dnů. Reálně bude orgán vykonávající dozor za normálních okolností provádět pokusy o stažení od momentu ukončení reportovacího období v rostoucích intervalech několika minut až několika hodin, a to i po uplynutí 8 hodin.

3. Potvrzovací a chybové balíčky

Jak dlouho bude trvat vystavení potvrzovacího OK/ERR balíčku?

Čas stažení a zpracování automatizovaného výstupu ze strany orgánu vykonávajícího dozor není reportingovou vyhláškou určeno, reportingová vyhláška uvádí, že orgán vykonávající dozor přistoupí k internetové adrese používané k poskytování automatizovaného výstupu nejpozději do 7 dní ode dne, kdy má být automatizovaný výstup poskytnut. V normálním případě ale dojde ke stažení automatizovaného výstupu v řádu jednotek hodin po vystavení. Automatizovaný výstup je poté zpravidla okamžitě zpracován na úrovni komunikačního rozhraní a pokud jsou nalezeny chyby, je vystaven chybový potvrzovací balíček. Pokud nejsou nalezeny chyby na úrovni komunikačního rozhraní, je automatizovaný výstup předán databázové vrstvě, která ho v asynchronním režimu opět v řádu hodin zpracuje a vrátí OK nebo ERR potvrzovací balíček. Celkově by tedy za normálních okolností mělo dojít ke zpracování a vystavení odpovědi v řádu jednotek hodin, nejpozději do 24 hodin.

Jak se o vystavení potvrzovacího balíčku dozvíme a jak ho získáme?

V bodě III oddílu 3 Přílohy k reportingové vyhlášce je uvedeno, že jde o POST notifikaci na URL ve formě
https://<URL OK>?protokol=<Název balíčku>.ok.zip.p7e.p7s nebo

https://<URL chyba>?protokol=<Název balíčku>.err.zip.p7e.p7s.

V rámci implementace Playgroundu jsme upřesnili, že mime-type POST requestu bude application/octet-stream.

Reportingová vyhláška ve stejném bodě dále uvádí, že orgán vykonávající dozor vystaví potvrzovací balíček také na serveru, ke kterému má provozovatel přístup šifrovaným autentizovaným přenosem pomocí protokolu HTTPS. To v praxi znamená, že potvrzovací balíčky si můžete alternativně stáhnout z URL adresy, publikované jako součást komunikačních parametrů orgánu vykonávajícího dozor, konkrétně pro Playground https://reporting-pg.hazard.spcss.cz/data/<Název balíčku>.ok.zip.p7e.p7s nebo https://reporting-pg.hazard.spcss.cz/data/<Název balíčku>.err.zip.p7e.p7s
Pro stažení balíčku je třeba použít jako HTTPS klientský certifikát registrovaný autentizační certifikát.

Jako pomocný nástroj pro provozovatele je dále na URL adrese https://reporting-pg.hazard.spcss.cz/apps/reg-db/processing (pro Playground) aplikace zobrazující stav stahování datových balíčků, opět dostupná při použití registrovaného autentizačního certifikátu.

Jaký je význam souborů v potvrzovacím balíčku?

V případě neúspěchu vstupních kontrol na úrovni komunikačního rozhraní obsahuje potvrzovací balíček jeden nebo více z následujících souborů:

- validation-report.csv - přehled validace jednotlivých CSV souborů balíčku
- validation-errors.csv - seznam nalezených jednotlivých chyb
- validation-processing.txt - detailní výpis zpracování balíčku

Pozn: Tyto soubory jsou stejné, jako výstupy nástroje PackageValidation.exe, který je součástí referenčního klienta.

Dále v případě vyhodnocení databázových validací obsahuje potvrzovací balíček databázových validací jeden nebo více z následujících souborů:

- db-validation-report.csv - přehled validace jednotlivých CSV souborů balíčku
- db-validation-errors.csv - seznam nalezených jednotlivých chyb

Výstupní soubory z jednotlivých vrstev validací jsou pojmenovány odlišně a mají částečně odlišnou strukturu (ve výstupech komunikačního rozhraní jsou odkazovány čísla řádků vstupních souborů, ve výstupech databázových validací primární klíče).

Výstupní soubory jsou obecně určeny pro manuální zpracování, jsou ale částečně strukturovány pro možnost základního třídění a filtrování.

Výstupní soubory validation-errors.csv a db-validation-errors.csv soubory obecně obsahují jeden řádek pro každou nalezenou chybu, při velkém množství stejných chyb je počet chybových hlášení pro danou chybu omezen na 1000 řádků.

Co znamená neprázdný soubor db-validation-errors.csv v OK potvrzovacím balíčku?

Databázové validace podporují přijetí balíčku s určitou mírou nekonzistencí a chyb. V takovém případě je součástí OK potvrzovacího balíčku neprázdný soubor db-validation-errors.csv

V prvotním nasazení na veřejném testovacím prostředí (Playground) je pro usnadnění rozjezdu testování nastavena vyšší míra tolerance k chybám (s výjimkou implicitních validací, tj. zejména validací referenční integrity dat). V průběhu května (termín bude oznámen na stránkách Ministerstva financí) dojde k nastavení parametrů tolerance k chybám na stejnou úroveň, jaká bude nastavena od 1. 6. 2019 na produkčním prostředí.

Proto je při testování na Playgroundu doporučeno sledovat nejen návratový status potvrzovacího balíčku (OK/ERR), ale i obsah souboru db-validation-errors.csv a opravovat chyby uvedené v tomto souboru i pro potvrzovací balíčky se statusem OK.

Jaký je význam chybových kódů v potvrzovacím balíčku?

Přehled vstupních kontrol (validací) a odpovídajících chybových kódů je publikován a na URL adrese https://www.mfcr.cz/cs/soukromy-sektor/hazardni-hry/reportingova-vyhlaska/technicke-informace/2019/seznam-vstupnich-kontrol-validaci-automa-34765.

4. Playground

Jaké jsou URL adresy playgroundu?

Playground (veřejné testovací rozhraní) je provozován pod identitou SPCSS (Státní pokladna Centrum sdílených služeb, s.p.) v roli testovacího "orgánu vykonávajícího dozor".

- URL adresa pro poskytování potvrzovacího balíčku (dle vyhlášky): https://reporting-pg.hazard.spcss.cz/data
- URL adresa aplikace pro přehled stavu zpracování datových balíčků: https://reporting-pg.hazard.spcss.cz/apps/reg-db/processing (zatím nefunkční)
- URL adresa aplikace pro přehled registrací: https://reporting-pg.hazard.spcss.cz/apps/reg-db/registration-list
- URL adresa aplikace samoobslužné registrace: https://reporting-pg.hazard.spcss.cz/apps/reg-db/import-form

Přístup k potvrzovacím balíčkům a aplikacím je možný pouze s použitím registrovaného autentizačního certifikátu provozovatele.

Bude Playground v provozu i po 1.6.2019?

Ano, Playground bude v provozu dlouhodobě pro účely testování změn a nových implementací na straně provozovatelů. Jde o samostatný systém, oddělený od ostrého prostředí.

Jak zrušit registrace do Playgroundu v případě, že ho nyní nepotřebujeme používat?

V registračním formuláři pro Playground použijte typ podání “oznámení o zrušení”. V tomto případě doporučujeme odregistrovat balíčky velkého modelu a ponechat registraci pouze na jeden balíček malého modelu. Tak zůstanou v systému zaregistrované autentizační certifikáty, které vám umožní samoobslužnou registraci při návratu k testování.

5. Ostré (produkční) prostředí

Jaké jsou URL adresy ostrého prostředí?

Ostré prostředí je provozováno pod identitou Celní správy (orgánu vykonávajícího dozor).

- URL adresa pro poskytování potvrzovacího balíčku (dle vyhlášky): https://reporting-hazard.celnisprava.cz/data
- URL adresa aplikace pro přehled stavu zpracování datových balíčků: https://reporting-hazard.celnisprava.cz/apps/reg-db/processing
- URL adresa aplikace pro přehled registrací: https://reporting-hazard.celnisprava.cz/apps/reg-db/registration-list

Přístup k potvrzovacím balíčkům a aplikacím je možný pouze s použitím registrovaného autentizačního certifikátu provozovatele. Tyto URL adresy budou v provozu nejpozději od 25.5.2019.

Jaká je možnost ověření správnosti registrovaných komunikačních parametrů pro produkční prostředí před 1.6.2019?

Pro ověření nastavení komunikačních parametrů produkčního prostředí v systému provozovatele poskytne orgán vykonávající dozor následující podporu - pilotní provoz ostrého prostředí. Pokud si provozovatel zaregistruje nastavení komunikačních parametrů produkčního (ostrého) prostředí pro hazardní hru nebo kasino s datem dřívějším než 1. 6. 2019, nebo shodným, budou jeho automatizované výstupy od 25. 5. 2019 stahovány a validovány. Všechny automatizované výstupy stažené před datem 1.6.2019 pak budou ke dni 1.6.2019 smazány.

Z důvodů zvýšení bezpečnosti (nastavení firewall pravidel) potřebujeme znát IP adresy serverů orgánu vykonávajícího dozor.

Reportingová vyhláška stanovuje kryptografické mechanismy zabezpečení komunikace a přenášených dat mezi provozovatelem a orgánem vykonávajícím dozor prostřednictvím Internetu. Tyto mechanismy zahrnují oboustrannou autentizaci na úrovni HTTPS protokolu a šifrování a elektronické pečetění datových balíčků. Potřebné komunikační parametry obou stran jsou komunikovány důvěryhodným kanálem. Tyto mechanismy jsou z pohledu zákona o kybernetické bezpečnosti dodatečné a jde o silnější mechanismy zabezpečení než filtrování IP adres.

Orgán vykonávající dozor používá fixní sadu IP adres pro odchozí komunikaci, aktuálně jde o IP adresy z veřejného rozsahu Státní pokladny Centra sdílených služeb, s.p., 5.145.105.*. Orgán vykonávající dozor ale může z technických důvodů tyto adresy bez oznámení změnit. Provozovatel může využít filtrování provozu jako dodatečné bezpečnostní opatření na vlastní riziko, v takovém případě musí provoz monitorovat a zajistit soulad s požadavky reportingové vyhlášky.

Jak vyžádat opravu u již přijatého balíčku?

Jde o mechanismus opravy věcných chyb dle § 5 reportingové vyhlášky. Na rozdíl od Playgroundu, kde lze provést tuto akci samoobslužně, je třeba iniciovat podáním do formuláře https://forms.celnisprava.cz/webfiller/formservice/filler.open?DocID=2019032778,

zde zvolit celní úřad příslušný sídlu provozovatele a příslušný typ podání, uvést důvod opravy hodný zřetele a identifikaci balíčku (zadává se bez čísla verze, opravu připravte jako následující vyšší verzi po poslední přijaté verzi). Po přijetí a posouzení podání pracovníky celní správy bude v systému nastaveno stahování nové verze balíčku a zbytek (vlastní stažení a validace datového balíčku) jde standardním způsobem. Upozorňujeme, že jde o mechanismus pro mimořádné situace, není určen pro běžné použití.

Je možná změna komunikačních parametrů pro balíček/balíčky malého modelu v polovině měsíce?

Komunikační parametry musí být platné v okamžiku předání automatizovaného výstupu, resp. v momentě, kdy systém zahajuje jeho stahování. Tzn. u malého modelu se reportuje vždy od 1. dne po uplynutí vykazovaného období. Kompletní balíček za celý měsíc bude vystaven dle nových parametrů, které jsou platné k 1. dni měsíce.

Jak zrušit registrace jednoho kasina (balíčku malého modelu)?

Pro zrušení jednoho kasina použijte v registračním formuláři: https://forms.celnisprava.cz/webfiller/formservice/filler.open?DocID=693323274 typ podání "oznámení o zrušení". V seznamu automatizovaných výstupů vložte identifikátory pouze pro rušené kasino.

Co znamená stav Předběžně validováno?

Jak je podrobně vysvětleno na https://www.mfcr.cz/cs/soukromy-sektor/hazardni-hry/reportingova-vyhlaska/technicke-informace/2019/chybova-hlaska-a-zmena-oznamovani-inform-35598, ode dne 10. 7. byla nasazena funkcionalita "preapprove", a to následujícím způsobem:

Pokud určitý automatizovaný výstup (označme jej X) projde všemi vstupními validacemi, ale všechny předchozí automatizované výstupy v rámci stejné balíčkové řady (řad dříve poskytnutých automatizovaných výstupů) nejsou ve stavu "Přijato", dostane se do nového stavu "Předběžně přijato". Stav "Předběžně přijato" není oznamován potvrzovacím "OK" balíčkem podle reportingové vyhlášky. Informace o tomto stavu je pouze zobrazena ve webové aplikaci na adrese https://reporting-hazard.celnisprava.cz/apps/reg-db/processing za účelem zajištění dostatečné informovanosti provozovatele.

Následně přichází v úvahu dva scénáře:

1) Při opravách formálních chyb předchozích automatizovaných výstupů (zpracování dalších verzí předchozích balíčků) dojde ke stavu, že všechny předchozí automatizované výstupy ve stejné balíčkové řadě jsou ve stavu "Přijato", bude automatizovaný výstup X znovu předmětem validací (roll-back automatizovaného výstupu a validace v kontextu nových přijatých dat předchozích automatizovaných výstupů) a znovu vyhoví validačním kritériím, posune se automatizovaný výstup X rovněž do stavu "Přijato" a je odeslán finální "OK" potvrzovací balíček.

2) Při opravě formálních chyb některého z předchozích automatizovaných výstupů (zpracování další verze předchozího automatizovaného výstupu) dojde při opakovaném zpracování validací automatizovaného výstupu X k chybě vstupních validací, je automatizovaný výstup X odmítnut a je odeslán "ERR" potvrzovací balíček.

Finální informace o úspěšném přijetí automatizovaného výstupu ve formě "OK" potvrzovacího balíčku tedy nemusí být odeslána ihned po zpracování, ale až po přijetí všech předchozích automatizovaných výstupů v tzv. balíčkové řadě (řada automatizovaných výstupů). Místo odeslání potvrzovacího balíčku je v takovém případě ve web aplikaci zobrazen stav "Předběžně přijato". Tento stav se v závislosti na dalším zpracování oprav předchozích automatizovaných výstupů v tzv. balíčkové řadě může změnit buď na "Přijato", nebo na "Odmítnuto" (resp. na čekání na další verzi automatizovaného výstupu).