Technický standard připojení do sítí deklarantů
verze 1.4
15/05/2026

Účelem tohoto dokumentu je definovat technické podmínky pro připojení vybraných zaměstnanců Celní správy ČR do sítí deklarantů (konkrétně k vybraným informačním systémům deklarantů).

Standard přímého přístupu do sítě (elektronického informačního systému; dále jen „IS“) deklaranta souvisí s praktickým prováděním zjednodušeného postupu „zápis do záznamů deklaranta“, v současné době primárně ve formě zahrnující upuštění od povinnosti předkládat zboží. Podmínky tohoto zjednodušení jsou stanoveny zejména v článku 182 nařízení Evropského parlamentu a Rady (EU) č. 952/2013, kterým se stanoví celní kodex Unie, v platném znění (dále jen „UCC“), čl. 150 nařízení Komise v přenesené pravomoci (EU) 2015/2446, 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“) a čl. 233 až 236 prováděcího nařízení Komise (EU) 2015/2447, kterým se stanoví prováděcí pravidla k některým ustanovením nařízení Evropského parlamentu a Rady (EU) č. 952/2013, kterým se stanoví celní kodex Unie, v platném znění (dále jen „IA“). Standard je následující:

1. IS deklaranta musí být přístupný jedním z následujících způsobů:

a) Přímo dostupný ze sítě Celní správy České republiky (dále jen „CS“) zabezpečeným spojením (viz specifikace níže) přes síť Internet. Zabezpečené spojení bude sestaveno pomocí připojení webového prohlížeče klienta v síti CS k IS deklaranta. Přístup k IS deklaranta je možné omezit pomocí bezpečnostního pravidla, které přístup omezí na zdrojový adresní prostor 193.179.220.0/22, přidělený CS společností RIPE NCC.

b) Dostupný zabezpečeným spojením (viz specifikace níže) přes síť Internet, prostřednictvím webového portálu VPN koncentrátoru deklaranta. Zabezpečené spojení mezi klientem v síti CS a VPN koncentrátorem deklaranta bude sestaveno pomocí webového prohlížeče.

2. Data deklaranta musí být plnohodnotně přístupná webovým prohlížečem (Microsoft Edge, Firefox, Chrome) bez nutnosti instalací jakýchkoliv klientských aplikací nebo rozšíření prohlížečů, jako je Java, Silverlight, ActiveX, FlashPlayer a jiné. Rozhraní musí být založeno pouze na bázi standardu HTML5.

3. Autentizace může být řešena:

a) Autentizace uživatelským jménem a heslem. Je doporučeno, aby se heslo k uživatelskému účtu řídilo požadavky vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (viz specifikace v bodě 7). V případě jeho vypršení musí být jasně definovaný způsob jeho obnovy. Deklarant musí v tomto režimu zpřístupnit klientům ze sítě CS i nástroj pro bezpečnou změnu hesla.

b) Autentizace jednorázovým OTP heslem. Možná jsou jak OTP hesla generovaná specializovaným HW tokenem, tak i mobilním tokenem, tj. aplikací pro mobilní telefony. CS doporučuje, aby touto aplikací pro mobilní telefony byla aplikace MS Authenticator, minimální verze 6.2602.0889, a verze aplikace MS Authenticator nesmí být starší než jeden rok. Aplikace musí být dostupná pro operační systém Android verze 13 a vyšší. Oba typy OTP tokenů musí být v užívání CS po dobu existence přístupu. V případě mobilního OTP tokenu je nutné, aby byl deklarant ochoten mobilní aplikaci aktivovat na

mobilním telefonu ve správě a majetku CS nebo aby předal inicializovanou aplikaci včetně kompatibilního mobilního telefonu CS. Pro případ reinstalace mobilního OTP tokenu musí být přesně popsán proces jeho reinicializace. Tento způsob autentizace je podmíněn souhlasem Celní správy ČR s vybraným technickým řešením deklaranta.

4. Deklarant nesmí umožnit současné vícenásobné připojení klientů ze sítě CS pod stejnou identitou. CS zajistí interním procesem řízený přístup k přihlašovacím údajům a bude monitorovat spojení směrem k IS deklaranta.

5. Deklarant musí zajistit, aby klientům v síti CS nebyly zpřístupněny jiné interní IS, než právě a jedině IS „o zápisu do záznamu deklaranta v rozsahu stanoveném v UCC, DA a IA“ v režimu pouze pro čtení a případně nástroj pro změnu hesla.

6. Vlastnictví výše uvedeného adresního prostoru 193.179.220.0/22 lze ověřit zde:

   https://apps.db.ripe.net/db-web-ui/#/query?searchtext=193.179.220.0%2F22#resultsSection

7. Doporučované parametry pro uživatelský účet:
   a) minimální délka hesla 12 znaků,
   b) minimální složitost hesla tak, že heslo bude obsahovat alespoň 3 z následujících 4 požadavků:
      i) nejméně jedno velké písmeno,
      ii) nejméně jedno malé písmeno,
      iii) nejméně jedna číslice,
      iv) nejméně jeden speciální znak odlišný od požadavků v bodech i) až iii),
   c) maximální dobu pro povinnou změnu hesla 180 dnů; tento požadavek není vyžadován pro samostatné identifikátory aplikací.

8. Je nutné prosazovat bezpečné nakládání s kryptografickými prostředky a zohledňovat doporučení vydaná NÚKIB a zveřejněná na jeho internetových stránkách (Minimální požadavky na kryptografické algoritmy, doporučení v oblasti kryptografické bezpečnosti, NÚKIB). Aktuální doporučení NÚKIB je uvedeno na odkazu:
   Minimální požadavky na kryptografické algoritmy | Portál NÚKIB

Za správnost:

1. Ing. Vladimír Cepek, Vladimir.Cepek@celnisprava.gov.cz, za problematiku související s kybernetickou bezpečností.
2. Bc. Milan Mašek, Milan.Masek@celnisprava.gov.cz, tlf. +420 725083572, za provozní realizaci systému přístupů zaměstnanců CS ČR do IS deklaranta na straně celní správy a kontrolu technických podmínek pro připojení IS deklaranta

Schválil:

Ing. Petr Gavlas
ředitel Odboru 12 Informatiky
zástupce ředitelky Sekce 1 ekonomiky a informatiky
Generální ředitelství cel

Digitálně podepsáno
Ing. Petr Gavlas
ředitel Odboru informatiky
18.05.2026 13:16:54