**PŘÍLOHA Č. 7 Smlouvy – Pravidla a předpisy VPN přístupů do sítě VZP ČR pro Kontraktory**

**Pravidla a předpisy VPN přístupů do sítě VZP ČR pro Kontraktory**

Obsah

1 Úvod 4

1.1 Použité zkratky 4

2 Základní pojmy 4

2.1 VPN přístup 4

2.2 Kontraktor 4

2.3 Uživatel VPN přístupu 4

2.4 Služba VPN 4

2.5 Kontaktní osoba VZP ČR 4

2.6 Kontaktní osoba Kontraktora 5

2.7 Koncové zařízení 5

3 Procesní postupy 5

3.1 Prvotní registrace VPN přístupu 5

3.2 Pozastavení VPN přístupu 5

3.3 Ukončení VPN přístupu 5

3.4 Žádost o ukončení VPN přístupu 6

3.5 Obnovení VPN přístupu 6

4 Provozní požadavky 6

5 Bezpečnostní pravidla 6

6 Důvěrnost – klasifikace informací 7

6.1 Informace považované za neveřejné 7

6.2 Informace považované za veřejné 7

7 Ochrana intelektuálního vlastnictví 7

8 Výklad a platnost 7

9 Formulář číslo 1 1

10 Formulář číslo 2 2

# Úvod

Tento dokument stanoví pro účely Smlouvy o podmínkách VPN přístupů do sítě IS VZP ČR procesy a postupy směřující k zajištění ochrany informačního systému VZP ČR při přístupu externích subjektů do vnitřní sítě VZP ČR prostřednictvím Internetu (Uživatelů). Tento dokument dále stanoví minimální rozsah povinností jednotlivých Uživatelů při používání VPN přístupů.

## Použité zkratky

|  |  |
| --- | --- |
| Zkratka | Význam |
| VZP ČR | Všeobecná zdravotní pojišťovna České Republiky |
| CA | Certifikační autorita – vydává a řídí životní cyklus digitálních certifikátů |
| CRL | Revokační list - seznam zneplatněných digitálních certifikátů (udržuje CA) |
| IPSec | [Bezpečnostní](http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_bezpe%C4%8Dnost) rozšíření [IP protokolu](http://cs.wikipedia.org/wiki/Internet_Protocol) založené na [autentizaci](http://cs.wikipedia.org/wiki/Autentizace) a [šifrování](http://cs.wikipedia.org/wiki/Kryptografie) |
| SSL | Secure Sockets Layer, (SSL) je protokol vložený mezi vrstvu transportní (např. TCP/IP) a aplikační (např. HTTP), který poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran |
| TLS | Protokol Transport Layer Security (TLS) je vývojový následovník SSL. Využívá kryptografické protokoly pro možnost zabezpečené komunikace, většinou v Internetu |
| VPN | Virtuální privátní síť (anglicky virtual private network) je v informatice prostředek k propojení několika počítačů prostřednictvím (veřejné – většinou Internet) nedůvěryhodné počítačové sítě. Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní (důvěryhodné) sítě |

# Základní pojmy

## VPN přístup

VPN přístup je vzdálený přístup do sítě VZP ČR, realizovaný mezi vzdáleným počítačem Uživatele a přístupovým bodem VZP ČR prostřednictvím Internetu, zabezpečený podle požadavků VZP ČR.

## Kontraktor

Je externí subjekt, který k řádnému splnění svých závazků vyplývajících ze smlouvy uzavřené mezi ním a VZP ČR (dále jen „Příslušná smlouva“), potřebuje umožnit některým osobám, které se na plnění jeho závazku přímo podílejí, vzdálený VPN přístup do sítě VZP ČR. Kontraktor musí mít uzavřenou a platnou Smlouvu o VPN přístupu. Bez této smlouvy nelze o VPN přístup žádat.

## Uživatel VPN přístupu

Uživatelem VPN přístupu je osoba, která se na základě smluvního vztahu s Kontraktorem (např. pracovně právní vztah) podílí na plnění závazků Kontraktora vyplývajících z Příslušné Smlouvy, a k tomuto účelu potřebuje mít vzdálený VPN přístup do sítě VZP ČR. Uživatel VPN přístupu není ve smluvním vztahu s VZP ČR a komunikuje s VZP ČR pouze prostřednictvím Kontraktora.

## Služba VPN

VPN přístup pro Kontraktora, resp. pro jednotlivé Uživatele VPN přístupu, zajišťují a udržují určení zaměstnanci VZP ČR (dále jen „Služba VPN“). Služba VPN zodpovídá za to, že VPN přístup bude poskytnut pouze Uživatelům, kterým byl VPN přístup ve Schvalovacím procesu povolen a pouze v rozsahu stanoveném Schvalovacím procesem, a to maximálně po dobu 1 roku.

Služba VPN přístupu zejména zajišťuje, že VPN přístup bude znemožněn uživateli, jehož certifikát není platný nebo jehož certifikát je na seznamu CRL příslušné CA. Služba VPN přístupu zodpovídá za vyřizování připomínek a stížností.

## Kontaktní osoba VZP ČR

Kontaktní osobou je pracovník VZP ČR, který je zodpovědný za komunikaci s  Kontraktorem a podílí se na řízení jeho činnosti, typicky projektový manažer (projektový vedoucí) nebo garant smlouvy o podpoře (supportové smlouvy). Kontaktní osoba je zodpovědná za řádné vyřízení požadavku Kontraktora na zřízení VPN přístupu do sítě VZP ČR.

## Kontaktní osoba Kontraktora

Kontaktní osobou je osoba zmocněná Kontraktorem k jednání ve věci plnění Smlouvy. Zajišťuje zejména komunikaci s Kontaktní osobou VZP ČR, řeší technické a jiné běžné záležitosti související VPN přístupy Uživatelů Kontraktora.

## Koncové zařízení

Koncové zařízení je technické zařízení, z něhož je/bude VPN přístup realizován (PC, notebook, tablet, mobilní telefon, atd.).

## Příslušná smlouva

Příslušnou smlouvou je smlouva uzavřená mezi VZP ČR a Kontraktorem, k jejímuž splnění je v rámci součinnosti ze strany VZP ČR nezbytné umožnit Kontraktorovi, resp. osobám, které se na plnění závazků Kontraktora podílejí, vzdálený VPN přístup do sítě VZP ČR.

## Smlouva

Smlouvou se pro účely tohoto dokumentu rozumí Smlouva o podmínkách VPN přístupů do sítě VZP ČR uzavřená mezi VZP ČR a Kontraktorem, jejíž přílohou je tento dokument.

# Procesní postupy

Tato část definuje proces vyřizování požadavků na zřízení VPN přístupu do sítě VZP ČR. Požadavek na zřízení VPN přístupu může být ze strany VZP ČR zamítnut, schválen v plném rozsahu, či s omezením požadovaných oprávnění přístupů ke zdrojům v síti VZP ČR.

## Prvotní registrace VPN přístupu

Prvotní registrace VPN přístupu začíná podáním žádosti Kontraktora Kontaktní osobě VZP ČR.

Žádost se podává elektronicky formou e-mailu, podepsaného uznávaným elektronickým podpisem Kontraktora na adresu uvedenou ve Smlouvě.

Žádost musí obsahovat:

1. specifikaci Příslušné smlouvy vč. jejího čísla
2. důvod / účel požadavku na zřízení VPN přístupu
3. řádně vyplněný „Formulář číslo 1“.

Pro více Uživatelů jednoho Kontraktora musí být Formulář číslo 1 vyplněn jednotlivě pro každého Uživatele zvlášť.

Kontraktor je informován ze strany VZP ČR o stavu nebo o vyřízení/zamítnutí jeho žádosti v době stanovené ve Smlouvě.

## Pozastavení VPN přístupu

VPN přístup může být ze strany VZP ČR pozastaven při zjištění bezpečnostního incidentu nebo při porušení pravidel pro práci s VPN.

VZP ČR si vyhrazuje právo pozastavit přístup z provozních a technických důvodů. O pozastavení bude Kontraktor informován e-mailem.

 Obnovení přístupu bude provedeno až po vyřešení zjištěného incidentu.

Na žádost není poskytována služba pozastavení VPN přístupu, pouze ukončení VPN přístupu.

## Ukončení VPN přístupu

Automaticky je VPN přístup ukončen:

* vypršením platnosti certifikátu Uživatele VPN přístupu,
* po ukončení platnosti VPN přístupu uvedeném na formuláři č. 1,
* ukončením účinnosti Smlouvy o podmínkách VPN přístupů do sítě VZP ČR.

VZP ČR není povinna před vypršením doby platnosti VPN přístupu z výše uvedených důvodů informovat Kontraktora ani Uživatele VPN přístupu o Ukončení VPN přístupu. O obnovení VPN přístupu musí Kontraktor znovu požádat, shodně jako u Prvotní registrace VPN přístupu.

Kontraktor, resp. osoby zmocněné Kontraktorem k jednání ve věci plnění Smlouvy musí neprodleně zažádat o ukončení VPN přístupu konkrétního Uživatele, jestliže:

* dojde ke ztrátě, nebo poškození privátního klíče,
* je podezření na kompromitaci privátního klíče třetí osobou,
* dojde k ukončení smluvního vztahu mezi Uživatelem (majitelem certifikátu), dodavatelskou společností a Kontraktorem

## Žádost o ukončení VPN přístupu

O ukončení VPN přístupu konkrétního Uživatele žádá Kontraktor. Na základě žádosti o ukončení VPN přístupu musí být příslušný VPN přístup ze strany VZP ČR ukončen.

Žádost podává Kontraktor elektronicky formou e-mailu podepsaného uznávaným elektronickým podpisem Kontraktora Kontaktní osobě.

Žádost musí obsahovat řádně vyplněný a schválený Formulář číslo 2.

## Obnovení VPN přístupu

Pokud nastanou skutečnosti vedoucí k revokaci (zneplatnění) certifikátu Uživatele, na základě kterého byl povolen VPN přístup, řídí se obnova VPN přístupu podmínkami Prvotní registrace VPN přístupu.

# Provozní požadavky

**Použitá technologie**

VPN přístup je realizován sestavením zabezpečeného SSL/TLS/IPSec mezi VPN klientem koncové entity a VPN koncentrátorem s využitím certifikátu. VPN klient ověřuje identitu VPN koncentrátoru certifikátem VPN koncentrátoru s digitálním podpisem CA, která vydala certifikát VPN koncentrátoru. Digitální podpis CA se ověřuje oproti certifikátu CA.

# Bezpečnostní pravidla

Kontraktor je povinen zajistit dodržování následujících bezpečnostních pravidel, která jsou platná pro Kontraktora i pro Uživatele VPN přístupu. Kontraktor (Uživatel):

* Odpovídá za svá „párová data“ – tzn. musí je chránit před zneužitím neoprávněnými osobami. Za „párová data“ se považují informace a data VZP ČR získaná pomocí VPN přístupu a dočasně uložena na HW Uživatele VPN přístupu Kontraktora za účelem výkonu pracovní činnosti.
* Neprodleně informuje Kontaktní osobu v případě podezření na zneužití svých párových dat.
* Bez prodlení vyrozumí příslušnou certifikační autoritu, která mu vydala osobní certifikát, o jakémkoli podezření z kompromitace svého soukromého klíče a zároveň požádat o ukončení platnosti příslušného certifikátu.
* Neprodleně informuje Kontaktní osobu, pokud hrozí nebezpečí zneužití dat VZP ČR, např. v případě odcizení koncového zařízení, výskytu spyware a podobných hrozeb na koncovém zařízení, apod.
* Neponechává koncové zařízení bez dozoru, pokud je sestaveno VPN spojení.
* Používá pro vytvoření VPN spojení pouze schválenou verzi VPN klienta.
* Udržuje aktivní VPN přístup (připojení) jen po nezbytně nutnou dobu.
* Odpovídá za koncové zařízení, které je použito pro VPN přístup do VZP ČR – tzn. zejména za to, že na koncovém zařízení je nainstalována odpovídající „ENDPOINT“ ochrana (Antivirus, Firewall, případně HIDS/HIPS) a jednotlivé komponenty mají aktuální definice. Za to že operační systém stanice má nainstalovány aktuální bezpečnostní opravy.
* Je povinen zajistit, že při navázaném VPN spojení do VZP  ČR nebude z koncového zařízení možný přístup do internetu vyjma komunikace s VPN bránou VZP  ČR.
* Uživatel VPN přístupu je oprávněn využívat VPN přístupu pouze k účelu, který je uveden v žádosti o VPN přístup a který byl ze strany VZP  ČR schválen.
* Uživatel VPN přístupu je oprávněn využívat VPN přístupu pouze v rozsahu, který je uveden v žádosti o VPN přístup a který byl ze strany VZP  ČR schválen.
* Uživatel je povinen užívat poskytnuté VPN spojení v souladu s  příslušnými obecně závaznými právními předpisy, zejména:
* zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů,
* zákonem č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů,
* zákonem č. 551/1991 Sb., o Všeobecné zdravotní pojišťovně České republiky, ve znění pozdějších předpisů,
* zákonem č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů.
* Uživatel VPN přístupu nesmí sdílet sestavené VPN spojení do VZP  ČR s dalšími počítači v síti Kontraktora. Kontraktor je povinen toto zajistit.
* Je zakázáno zasahovat do konfiguračních souborů a nastavení VPN klienta dodaných ze strany VZP  ČR.
* VZP ČR si vyhrazuje právo pořizovat auditní data z VPN připojení.

# Důvěrnost – klasifikace informací

## Informace považované za neveřejné

* Veškerá „párová data“ viz část „Bezpečnostní pravidla“;
* Neveřejnou informací jsou též obsahy auditních záznamů.

## Informace považované za veřejné

* Certifikáty Uživatelů;
* Certifikát VPN koncentrátoru;
* Certifikáty kořenové CA VZP ČR;
* Certifikáty zprostředkující CA VZP ČR;
* Informace obsažené v certifikátech a revokačních seznamech;
* Obsah této Přílohy č. 1 za podmínky dodržení odst. č. 5.2. „Ochrana intelektuálního vlastnictví“.

# Ochrana intelektuálního vlastnictví

Tato příloha je vlastnictvím VZP ČR. Žádná její část nesmí být bez výslovného souhlasu použita jako reference, kopírována ani šířena jinak, než je zde stanoveno.

# Výklad a platnost

Pokud některé z ustanovení tohoto dokumentu je nebo se stane neplatným, neúčinným či zdánlivým, neplatnost, neúčinnost či zdánlivost tohoto ustanovení nebude mít za následek neplatnost dokumentu jako celku ani jiných ustanovení tohoto dokumentu, pokud je takovéto ustanovení oddělitelné od jeho zbytku. Kontraktor a VZP ČR se zavazují takovéto neplatné, neúčinné či zdánlivé ustanovení nahradit novým platným a účinným ustanovením, které svým obsahem bude co nejvěrněji odpovídat podstatě a smyslu původního ustanovení.

Postupy řešení možných rozporů nebo neshod operací při VPN přístupu do sítě VZP ČR musí být v souladu s platnou legislativou ČR. Nedojde-li k dohodě při řešení rozporů nebo neshod smírnou cestou, budou tyto spory a neshody řešeny věcně a místně příslušnými soudy České republiky.

# Formulář číslo 1

|  |
| --- |
| **Formulář pro zřízení VPN přístupu (Prvotní registrace VPN přístupu)** |
| **Kontraktor**  | \* Název / obchodní firma  |  |
| \* IČO  |  |
| \* Jméno, příjmení (Kontaktní osoba) |  |
| \* E-mail |  |
| \* Telefon |  |
| \* Datum podání |  |
| \* Číslo Příslušné Smlouvy (tj. smlouvy, pro jejíž plnění je přístup VPN požadován)  |  |
| \* Důvod/Účel zřízení  |  |
| **Uživatel** | \* Jméno a příjmení  |  |
|  | \* E-mail  |  |
|  | \* Telefon  |  |
|  | \* Hodnota SERIALNUMBER v poli SUBJECT certifikátu vydaného koncové entitě CA |  |
|  | \* Datum ukončení platnosti VPN přístupu (maximálně 1 rok) |  |
|  | \* Výrobce antivir. programu  |  |
|  | \* Výrobce firewallu |  |
|  | \* Operační systém a verze  |  |
| **VZP ČR** | Jméno a příjmení Kontaktní osoby VZP ČR |  |
|  | Telefon a email |  |
|  | Za VZP ČR schválil (jméno, příjmení, email) |  |
|  |  |  |
| **Požadované cíle VPN přístupu na zařízení v VZP ČR** |
|  | \* Koncová zařízení(DNS jména/IP adresy)(protocol/dst port) |  |

# Formulář číslo 2

|  |
| --- |
| **Formulář pro Žádost o ukončení VPN přístupu** |
| **Kontraktor** | \* Název / obchodní firma |  |
|  \* IČO |  |
| \* Jméno a příjmení Uživatele |  |
| \* SERIALNUMBER Hodnota v poli SUBJECT certifikátu vydaného Uživateli |  |
| \* E-mail adresa Uživatele z certifikátu |  |
| \* Důvod ukončení VPN přístupu |  |
| \* Požadované datum ukončení platnosti VPN přístupu |  |
| \* Datum |  |

\* označené položky doplní Kontraktor a Uživatel