MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Katalogový list služby

Centrální místo služeb (CMS)

CMS2-08-2 – Přístup do CMS přes IPsec

Dokument popisuje vlastnosti, technické a volitelné parametry, SLA a postup zřízení služby CMS2-08-2 – Přístup do CMS přes IPsec. Služba je poskytována na základě Provozních podmínek Centrálního místa služeb.

Verze	2.0.5
Datum vytvoření	1. 6. 2017
Datum aktualizace	23. 5. 2019
Počet stran	10

Změny v dokumentu

Dokumentu bude verzován následujícím způsobem: **Verze A.B.C**

A – majoritní verze (2 – CMS 2. generace)

B – minoritní verze (schválené MV)

C – následující úpravy dokumentu před schválením MV

Verze	Datum	Popis změny
1.0.0	1. 6. 2017	Založení dokumentu
1.0.1	7. 2. 2018	Revize parametrů služby, interní revize dokumentu.
1.0.2	28. 3. 2018	Revize parametrů certifikátu.
1.0.3	28. 3. 2018	Revize parametrů IPsec.
2.0.0	9. 4. 2018	Publikace do PDF
2.0.1	24. 4. 2018	Revize žádosti o certifikát a technických parametrů služby.
2.0.2	26. 4. 2018	Kapitola 5. - Směrování sítě EU TESTA-ng do CMS
2.0.3	30. 8. 2018	Přidání bodu do Kontroly služby v kapitole 3.2 a v kapitole 8. změna formulace
2.0.4	13. 12. 2018	Revize kořenových autorit a parametrů IKE.
2.0.5	23. 5. 2019	Změna délky realizace služby v kap. 3.1

1 Obsah

Služba CMS2-08-2 – Přístup do CMS přes IPsec

1 Definice služby

Identifikátor	CMS2-08-2
Verze	1.0
Stav	V provozu
Datum spuštění	30. 6. 2017
Datum ukončení	Není stanoveno
Uživatelé	Registrovaní uživatelé CMS

Služba umožňuje připojení koncové lokality pomocí šifrovaného spojení (IPsec) přes síť Internet. Autentizace připojovaných zařízení probíhá pomocí certifikátů, vydaných neveřejnou certifikační autoritou CMS. Varianta je vhodná pro lokality, kde není možné přivést standardní přípojku KIVS. Přípojka slouží jen ke konzumaci přístupových služeb, tzn. není možné ji využít pro služby zveřejňování.

Pro každou připojovanou lokalitu musí Subjekt disponovat zařízením, které splňuje níže uvedené parametry. Z každé připojované lokality se sestavují dva souběžné IPsec tunely, zakončené v CMS v geograficky oddělených lokalitách. Pro zvýšení redundance přípojky je možné na straně Subjektu využít 2 zařízení v clusteru. Služba se zřizuje pro připojení právě jedné lokality, připojení další lokality znamená zřízení další služby.

2 Podmínky realizace služby

- Subjekt musí mít zřízenu službu „CMS2-01-1 – Akceptace provozních podmínek CMS“.
- Subjekt musí mít internetovou konektivitu na IPsec VPN koncentrátory CMS.
- Pro každou připojovanou lokalitu musí Subjekt disponovat zařízením, které splňuje následující parametry:
    - Zařízení musí umožňovat nastavení minimálně 2 peerů pro jednu VPN (primárního a záložního peeru CMS)
    - Technické parametry pro navázání Internet Key Exchange (IKE) spojení:
        - Auth metoda: Certifikát
        - Auth algoritmus: SHA2
        - Encryption: AES256-CBC
        - Diffie Hellman group 14
        - Lifetime: 28800 sec
        - IKE mode: main

        - IKE verze: 1
    - Technické parametry pro navázání IPsec tunelu:
        - Protokol: ESP
        - Auth algoritmus: SHA2
        - Encryption: AES256-CBC
        - Perfect forward secrecy: Group14
        - Lifetime: 3600 sec
- Pro každou připojovanou lokalitu musí Subjekt vygenerovat žádost o vydání certifikátu (Certificate signing request), splňující následující náležitosti:
    - Délka klíče: 2048 bitů
    - Hash: SHA-256
    - CN = FQDN zařízení – např. „hostname.domena.cz“
    - OU = zkratka subjektu uvedená v žádosti o službu
    - L = lokalita zařízení ve formátu „město-ulice-čp“
    - ST = CZ
    - C = CZ
    - zbývající pole budou do certifikátu doplněna automaticky

3 Zřízení služby

3.1 Délka realizace služby

Na požadavek realizace služby je reagováno do 5 pracovních dní od přijetí žádosti, doba vyřešení požadavku je 20 pracovních dní nebo dle domluvy se Subjektem.

3.2 Postup zřízení služby

Krok	Popis	Odpovědnost
1	**Sběr podkladů od Subjektu.**	
	Subjekt si zažádá o zřízení této služby a musí vyplnit požadavek na zřízení služby.	Subjekt
	Subjekt musí předat pro každou požadovanou VPN následující požadavky: • Popis využití a uživatelský název VPN. • Identifikaci Propojovacího bodu, kde bude VPN zakončena. • Veřejné IP adresy a typ připojovaných zařízení. • IP rozsahy sítí připojovaných IPsec tunelem do CMS. • Nastavení volitelných parametrů služby. • Žádost o vydání certifikátu (Certificate signing request)	Subjekt
2	**Zřízení služby**	
	Zřizovatel doplní následující informace:	Zřizovatel

	• Přidělený název VPN. • Veřejné IP adresy IPsec VPN koncentrátorů CMS. • IKE hostname IPsec VPN koncentrátorů CMS. • IKE hostname zařízení Subjektu. • Rozsahy směrované do CMS. • Vygenerovaný certifikát.	
	Zřizovatel provede konfiguraci služby ve stanovém čase.	Zřizovatel
3	**Předání služby**	
	Zřizovatel vystavuje protokol se všemi výše uvedenými informacemi a předává ho Subjektu. Parametry služby jsou zároveň dostupné na Portálu CMS.	Zřizovatel
	Subjekt zabezpečí následující změny: • Konfiguraci parametrů IPsec na svých zařízeních. • Nastavení směrování uvedených rozsahů do CMS.	Subjekt
4	**Kontrola služby**	
	• Kontrola sestavení IPsec tunelu na koncových zařízeních Subjektu. • Po připojení do IPsec VPN Subjekt ověří konektivitu k Propojovacímu bodu pomocí ping na IP adresu pro testování služby, uvedenou v předávacím protokolu služby. • Kontrola možnosti sestavit tunel ze strany koncového zařízení Subjektu.	Subjekt
	• Ze stavu „Testovací režim“ na Portálu CMS se služba dostane do stavu „Bez problémů“ zasláním emailu s potvrzením o správné funkčnosti služby na pozadavky.cms@nakit.cz.	Subjekt

4 Volitelné parametry

Služba nemá volitelné parametry.

5 Technické parametry služby

- Připojení je realizováno prostřednictvím IPsec tunelů ze zařízení Subjektu na VPN koncentrátory CMS, umístěné v geograficky oddělených lokalitách.
- Adresní rozsah použitý v CMS je 10.240.0.0/12, tento rozsah Subjekt směruje do IPsec tunelu do CMS.
- Pokud Subjekt chce přes IPsec přistupovat do sítě Evropské unie TESTA-ng, musí do IPsec tunelu do CMS směrovat i rozsah 62.62.0.0/17.
- Maximální velikost IP paketu přenášeného prostředím CMS je 1400 bytů.

- VPN koncentrátory CMS podporují NAT traversal (NAT-T).
- IKE tunel (fáze 1) je sestaven do obou lokalit CMS současně.
- IPsec tunel (fáze 2) je sestaven pouze do datového centra 2 (DC2), v případě výpadku se vyjedná IPsec tunel do datového centra 1 (DC1).
- Směrování skrz IPsec tunel je statické.
- Pro každou připojovanou lokalitu musí Subjekt disponovat zařízením, které splňuje následující parametry:
    - Zařízení musí umožňovat nastavení minimálně 2 peerů pro jednu VPN (primárního a záložního peeru CMS)
    - Technické parametry pro navázání Internet Key Exchange (IKE) spojení:
        - Auth metoda: Certifikát
        - Auth algoritmus: SHA2
        - Encryption: AES256-CBC
        - Diffie Hellman group 14
        - Lifetime: 28800 sec
        - IKE mode: main
        - IKE verze: 1
    - Technické parametry pro navázání IPsec tunelu:
        - Protokol: ESP
        - Auth algoritmus: SHA2
        - Encryption: AES256-CBC
        - Perfect forward secrecy: Group14
        - Lifetime: 3600 sec
- Pro každou připojovanou lokalitu musí Subjekt vygenerovat žádost o vydání certifikátu (Certificate signing request), splňující následující náležitosti:
    - Délka klíče: 2048 bitů
    - Hash: SHA-256
    - CN = FQDN zařízení – např. „hostname.domena.cz“
    - OU = zkratka subjektu uvedená v žádosti o službu
    - L = lokalita zařízení ve formátu „město-ulice-čp“
    - ST = CZ
    - C = CZ
    - zbývající pole budou do certifikátu doplněna automaticky
- Vygenerovaný certifikát je odeslán emailem na kontakty uvedené v žádosti o zřízení služby.
- Kořenové certifikáty autorit pro **služby realizované od 1.12.2018**

  DigiCert Global Root G2
  Platnost do: 15.1.2038
  Sériové číslo: 03 3a f1 e6 a7 11 a9 a0 bb 28 64 b1 1d 09 fa e5

  Thawte TLS RSA CA G1
  Platnost do: 2.11.2027
  Sériové číslo: 09 0e e8 c5 de 5b fa 62 d2 ae 2f f7 09 7c 48 57

- Kořenové certifikáty autorit pro **služby realizované do 30.11.2018**
  thawte Primary Root CA - G3
  Platnost do: 01.12.2037
  Sériové číslo: 60 01 97 b7 46 a7 ea b4 b4 9a d6 4b 2f f7 90 fb

  thawte SHA256 SSL CA
  Platnost do: 22.5.2023
  Sériové číslo: 36 34 9e 18 c9 9c 26 69 b6 56 2e 6c e5 ad 71 32

6 Monitoring služby

6.1 Monitoring služby subjektem

Službu je možné monitorovat pomocí sledování stavu IPsec tunelu na zařízení Subjektu.

6.2 Monitoring služby z CMS

Služba je monitorována globálně stavem a dostupností IPSec VPN koncentrátorů.

Typ testu	Interval testu	Název parametru	Hodnota	Status služby
SNMP GET	2 min	Administrativní stav	Stav v obou DC je OK	Bez problémů
			Stav v jednom DC je OK a druhém DC je NOK	Odstávka
			Stav v obou DC je NOK	Odstávka
		Provozní stav	Stav v obou DC je OK	Bez problémů
			Stav v jednom DC je OK a druhém DC je NOK	Snížená dostupnost
			Stav v obou DC je NOK	Porucha

7 SLA služby

Provozní doba služby	24 x 7 x 365
Provozní doba řešení incidentů	24 x 7 x 365
Provozní doba podpory služby	5 x 8 (v pracovních dnech)
SLA v %	---
Maximální reakční doba	---
Maximální doba obnovy	---

8 Hlášení nefunkčnosti služby

Byla-li zákaznická služba schválena Subjektem jako funkční, je možné nahlásit nefunkčnost služby cestou ServiceDesku v souladu s Provozními podmínkami CMS, kde jsou zároveň uvedeny i příslušné kontakty. V případě zřizování služby se zadávají požadavky na testování na email pozadavky.cms@nakit.cz.

Při hlášení nefunkčnosti služby na ServiceDesk je nutné uvést níže uvedené povinné údaje. Bez jejich uvedení není možné nefunkčnost služby prověřit. Incident nemusí být, v souladu s Provozními podmínkami, ServiceDeskem přijat.

- Identifikátor služby ve formátu „GOVxxxxxx“
- Kontakt na technika Subjektu, který nefunkčnost řeší
- Na základě čeho se služba jeví jako nefunkční
- Datum a čas, od kdy je služba nepřístupná
- Datum a čas, kdy byla služba prokazatelně naposledy funkční
- Veřejná IP adresa koncového zařízení Subjektu (IPsec koncentrátoru).
- Výpis traceroute na veřejnou IP adresu IPsec VPN koncentrátoru CMS.