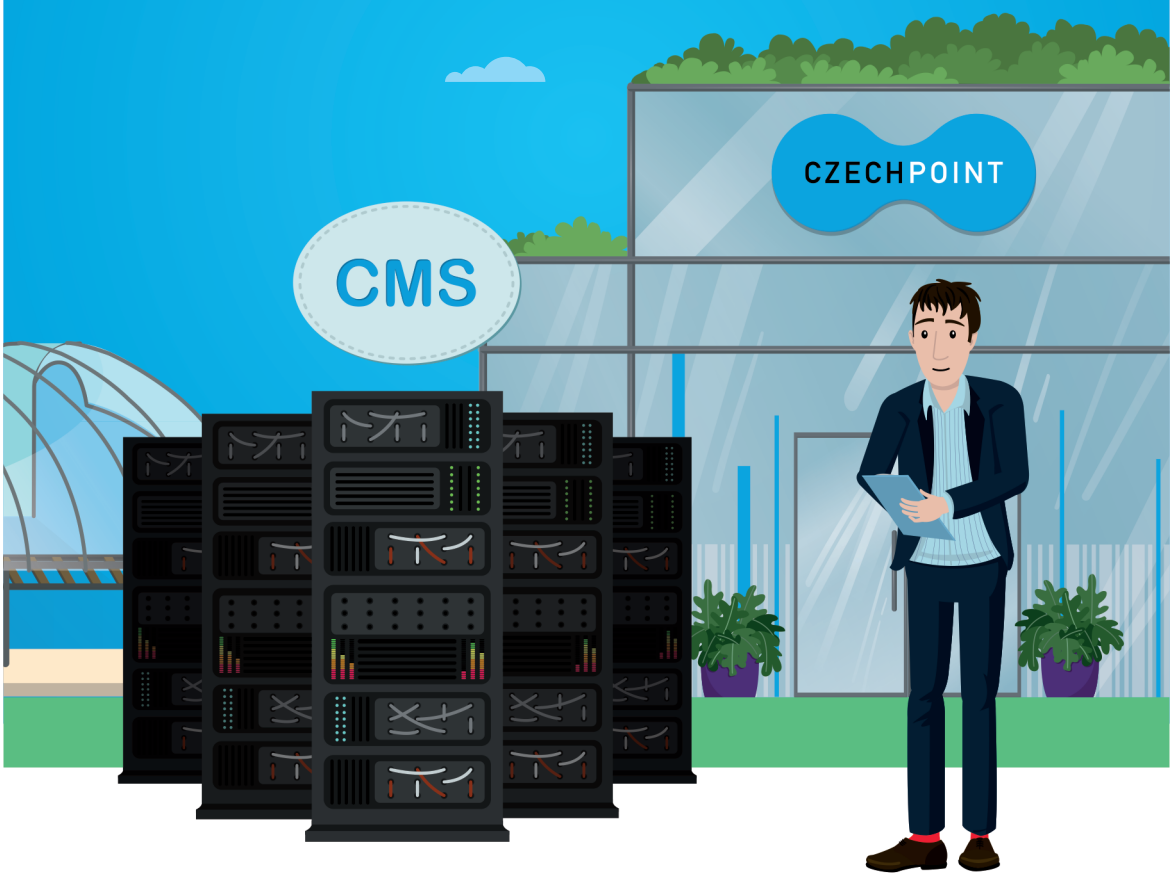
CENTRÁLNÍ MÍSTO SLUŽEB
Manuál CMS 2.0



INTEGROVANÝ OPERAČNÍ PROGRAM

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

INTEGROVANÝ OPERAČNÍ PROGRAM

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

Obsah

INTEGROVANÝ OPERAČNÍ PROGRAM

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

CMS 2.0

CMS 2.0 je druhá generace Centrálního místa služeb (CMS).
Tento dokument popisuje možnosti nového Centrálního místa služeb (dále jen CMS 2.0). Je určen pracovníkům státní správy, krajských úřadů a místní samosprávy, kteří využívají služby CMS 2.0.

V dokumentu se rozlišuje pojem služba ve dvou významech:

- Aplikační služba je služba, kterou poskytuje nějaká aplikace, spravovaná nějakým subjektem.
- Služba CMS 2.0 je služba, kterou poskytuje samotné CMS 2.0, například jednou ze služeb je publikace aplikační služby.

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

VYUŽITÍ SLUŽEB CMS 2.0

Hlavním cílem CMS 2.0 je umožnit pracovníkům státní správy, krajských úřadů a místní samosprávy ČR snadný přístup k informacím a informačním systémům, které potřebují ke své práci a k plnění legislativních nároků. K zajištění tohoto cíle nabízí CMS 2.0 řadu služeb.

Jednou z hlavních služeb CMS 2.0 je zpřístupnění dat a aplikací spravovaných jedním orgánem státní správy pracovníkům jiného orgánu státní správy. CMS 2.0 je v tomto případě bodem, ve kterém jeden subjekt nabízí data a aplikační služby a jiné subjekty tato data a služby využívají. CMS 2.0 nabízí technickou infrastrukturu pro propojení a řídí přístup subjektů k nabízeným datům a službám podle pravidel definovaných správcem dat a služeb. V praxi tedy jeden subjekt státní správy požádá provozovatele CMS 2.0 o připojení svého informačního systému (IS) k CMS 2.0 a o publikaci nějaké aplikační služby tohoto IS prostřednictvím CMS 2.0. A jiné subjekty požádají provozovatele CMS 2.0 o připojení svých IS a správce publikované služby požádají o povolení připojení svého IS k publikované aplikační službě.

Správce aplikační služby může již v žádosti o publikaci služby specifikovat okruh subjektů, kterým má být povolen přístup k publikované aplikační službě. Provozovatel CMS 2.0 zřídí v takovém případě určeným subjektům přístup k aplikační službě, aniž by příslušný subjekt musel o přístup žádat správce aplikační služby. Ostatní subjekty musí o povolení přístupu k aplikační službě požádat.

příklad: Ministerstvo dopravy (MD) publikuje do CMS 2.0 aplikační službu „webový přístup k Centrálnímu registru řidičů (CRŘ)“ a určí, že k této aplikační službě mají mít povolený přístup všechny obce s rozšířenou působností (ORP) a podřízené organizace MD a uvede seznam podřízených organizací. Provozovatel CMS 2.0 publikuje aplikační službu podle požadavků MD a zjistí všechny ORP a jejich přípojky k CMS 2.0 a přípojky podřízených organizací MD. Seznam předloží MD ke schválení a povolí přístup ke službě ze schválených přípojek. Pokud se změní seznam ORP s přístupem k CMS 2.0 nebo seznam přípojek podřízených organizací MD, provozovatel CMS 2.0 požádá MD o schválení příslušných změn. Pokud se změní seznam podřízených organizací MD, MD požádá o příslušnou změnu provozovatele CMS 2.0. Pokud chce k aplikační službě nějaký subjekt, který není v seznamu povolených subjektů, požádá o přístup provozovatele CMS 2.0 a ten nechá MD příslušnou žádost schválit.

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

PŘÍSTUP KE SLUŽBÁM CMS 2.0

Uživateli CMS 2.0 jsou orgány veřejné moci (OVM). Aby nějaký OVM mohl využívat služby CMS 2.0, musí o to požádat provozovatele CMS 2.0. Na Portálu CMS 2.0 si stáhne formulář, který obsahuje souhlas s podmínkami pro využívání služeb CMS 2.0, a pošle ho ze své datové schránky do datové schránky provozovatele CMS 2.0.

Provozovatel CMS 2.0 nechá žádost schválit správce CMS 2.0 (tím je MV), zaeviduje OVM v interní evidenci CMS 2.0 a nastaví v JIP, že OVM může přidělovat role (práva) pro využívání služeb CMS 2.0 konkrétním osobám. Fyzická osoba autorizovaná provádět jménem OVM změny v JIP* přidělí příslušná práva konkrétním fyzickým osobám. OVM má právo delegovat oprávnění na libovolné osoby, ale je odpovědný za jejich požadavky na služby CMS 2.0.

Rolí CMS 2.0 existuje více, ale je možné je rozdělit na dvě skupiny:

A | **role, které mohou žádat o služby CMS 2.0 bez dodatečného schválení OVM a role, které mohou žádat o služby CMS 2.0 s dodatečným schválením OVM**

B | **ve druhém případě CMS 2.0 vyžaduje potvrzení každého požadavku na služby CMS 2.0 datovou schránkou. CMS 2.0 po potvrzení požadavku vygeneruje nemodifikovatelný dokument a umožní jeho stažení osobou, která požadavek zadala. Poté čeká s realizací požadavku na doručení dokumentu datovou schránkou.**

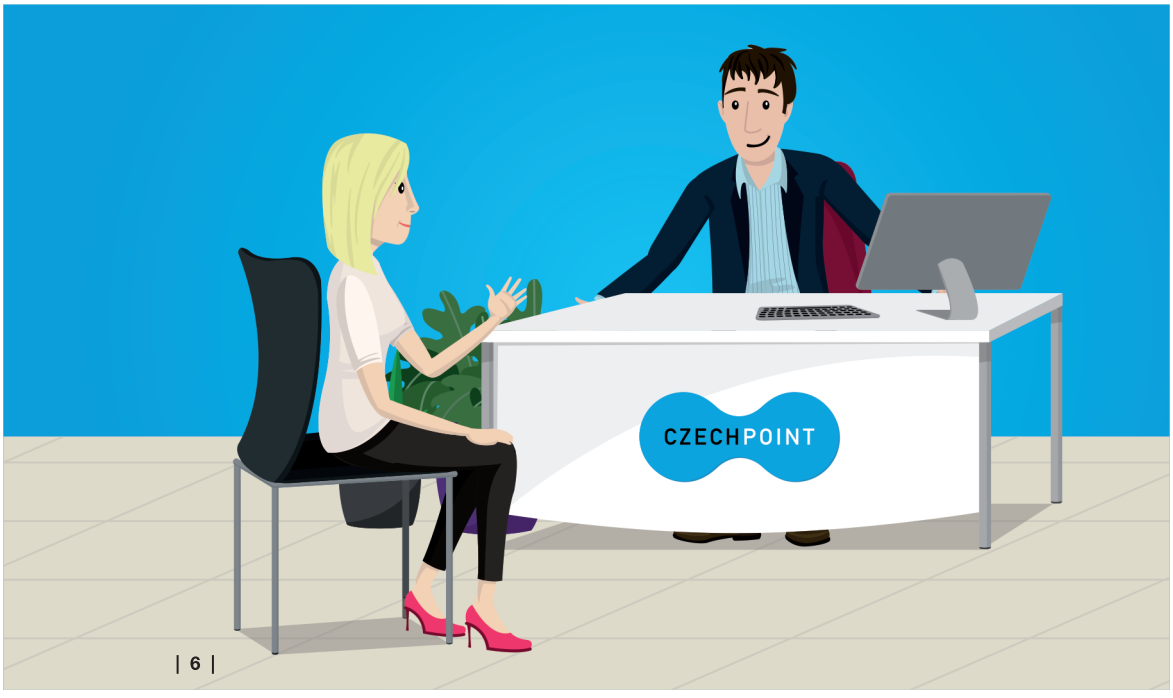
***JIP (Jednotný identitní prostor)** je zabezpečené adresářové úložiště informací o orgánech veřejné moci a fyzických osobách, které jsou příslušným OVM zmocněny k přístupu k informačním systémům státní správy. Správcem JIP je MV.

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

Osoby (mající příslušná oprávnění) jsou na Portálu CMS 2.0 vedeny při zadávání požadavků na realizaci, změnu nebo zrušení služby CMS 2.0 systémem menu, který jim dovoluje vybírat pouze z povolených seznamů hodnot (pokud je to možné), nebo která kontrolují v maximální možné míře zadávané hodnoty. Uživatel může rozpracované požadavky ukládat a později se k nim vrátit. Dále může požádat o zjištění ceny za požadavek.

Ve chvíli, kdy je žadatel s definicí požadavku hotov, požádá o jeho uložení k realizaci. CMS 2.0 v té chvíli provede všechny kontroly zadaných hodnot (některé potřebné zdroje mohly být během zadávání požadavku rezervovány pro jiný požadavek), požadované zdroje (IP adresy, výkon CPU atd.) rezervuje a uloží do fronty k realizaci. Požadavek ve frontě čeká, dokud nejsou splněny podmínky pro jeho realizaci. Typickými událostmi, na které může CMS 2.0 čekat, je potvrzení žádosti datovou schránkou nebo realizace jiného požadavku (např. čekání na vytvoření přípojky OVM k CMS 2.0).



INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

SLUŽBY CMS 2.0

Výčet služeb CMS 2.0:

- Žádost o přístup k CMS
- Publikace aplikační služby
- Přístup k aplikační službě
- Připojení OVM k CMS
- Umístění aplikace do NDC
- Služby eGSB
- Služby Certifikační autority
- Připojení OVM do Internetu
- Elektronická pošta
- Jmenné služby (DNS)
- Služby sTESTA
- Přístup k záznamům o provozu

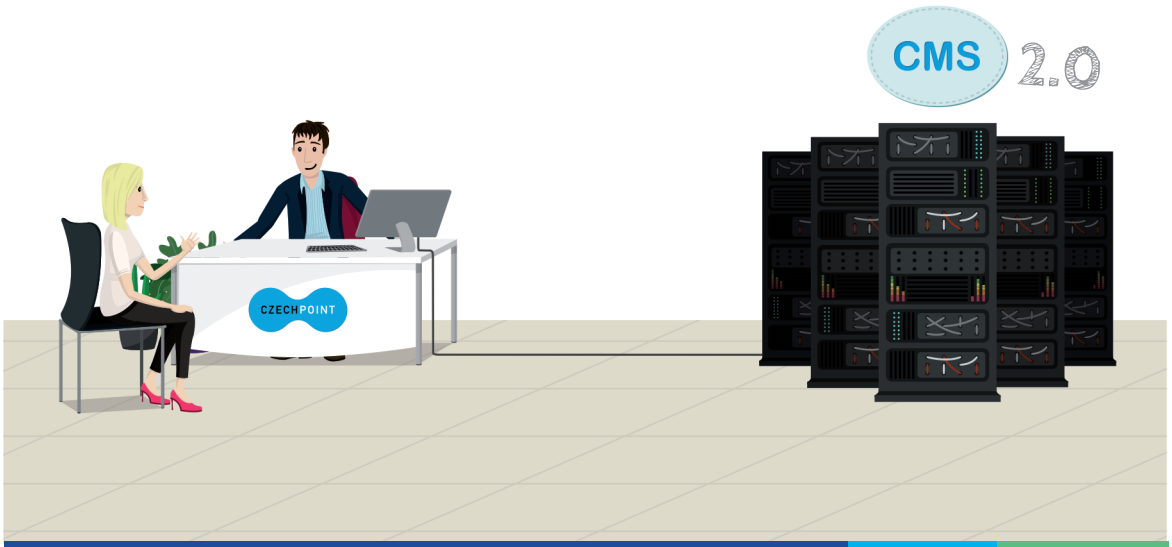
První tři služby CMS 2.0 jsme již představili. K publikaci aplikační služby dodejme, že OVM musí při požadavku na publikaci aplikační služby zadat:

- **Co se má publikovat: IP adresa a služba (TCP/UDP port).**
- **Odkud se má služba publikovat: lokalita a VPN.**
- **Prostředí, do kterého se má služba publikovat: KIVS, IPSec/SSL VPN, Internet.**
- **Pro koho se má služba publikovat: veřejná služba, pro OVM určené výčtem, pro OVM určené kategorií (např. obce s rozšířenou působností).**
- **Další nepovinné parametry: rozklad zátěže mezi lokality, ze kterých je služba poskytována, prostředky CMS 2.0, DNS záznamy pro publikovanou službu.**

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

Další služby stručně dále popisujeme v textu. Kompletní seznam služeb s popisem je uveden v Katalogu služeb CMS 2.0. Součástí popisu je mj. popis zabezpečení každé služby. Na základě toho se může každý uživatel rozhodnout, zda příslušná služba splňuje jeho bezpečnostní požadavky a tedy ji může pro své účely použít tak, jak je nebo musí implementovat dodatečná bezpečnostní opatření.



příklad: MD chce zajistit autentizovaný přístup k aplikační službě „webový přístup k CRŘ“. Příslušná služba CMS 2.0 pro publikaci aplikačních služeb nenabízí možnost autentizace uživatelů, a proto musí MD zajistit autentizaci samotnou aplikací CRŘ.
Všechny služby CMS 2.0 jsou podporovány jak na protokolu IPv4, tak na IPv6. Správce CMS 2.0 má pro potřeby adresace CMS 2.0 přiděleny veřejné IP adresy IPv4 i IPv6 a tyto adresy může poskytovat uživatelům pro zajištění služeb CMS 2.0.

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

KOMUNIKACE OVM S PROVOZOVATELEM A SPRÁVCEM CMS 2.0

Požadavky na realizaci, změny a rušení služeb CMS 2.0 zadávají osoby přes Portál CMS 2.0. Jde o osoby, kterým OVM přidělil v JIP příslušnou roli. Provozovatel CMS 2.0 požadavky realizuje a o výsledku informuje OVM změnou stavu požadavku na Portálu. V některých případech navíc informuje subjekty, kterých se požadavek týká, o realizaci požadavku datovou schránkou. Typickým příkladem je žádost OVM o povolení přístupu jiných OVM k jím publikované službě. OVM, kterým byl povolen přístup k nějaké aplikační službě na základě žádosti správce aplikační služby (a ne na základě žádosti samotného OVM), posílá provozovatel CMS 2.0 informaci do jejich datové schránky.

Service desk CMS 2.0 je dalším důležitým komunikačním kanálem pro jeho uživatele. Ten je dostupný přes Portál CMS 2.0, dále je možné se na jeho pracovníky obrátit pomocí telefonu a pomocí specializovaných aplikací (např. pro ohlašování bezpečnostních událostí).

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

PŘIPOJENÍ OVM K CMS 2.0

Pro využívání služeb CMS 2.0 je nutné LAN anebo jednotlivé počítače OVM k CMS 2.0 připojit. Znamená to, že OVM musí nějakou lokalitu se svou lokální počítačovou sítí (LAN) nebo jednotlivý počítač technicky propojit s CMS 2.0. Je několik způsobů připojení: přes operátora KIVS, přes krajskou síť a přes Internet.

Operátoři KIVS jsou komerční telekomunikační firmy, které mají smlouvu se správcem CMS 2.0. Připojení přes operátora znamená, že operátor musí zřídit fyzické propojení příslušné lokality s CMS 2.0 podle podmínek stanovených správcem CMS 2.0 a ve spolupráci s provozovatelem CMS 2.0. Toto propojení může udělat operátor buď z vlastní iniciativy nebo na žádost jednoho OVM nebo skupiny OVM, které např. sdílejí jednu lokalitu.

Pokud existuje fyzické propojení lokality přes jednoho operátora nebo více operátorů s CMS 2.0, žádají OVM využívající lokalitu o zřízení logického připojení své LAN k CMS 2.0. Toto logické připojení má podobu virtuální privátní sítě (VPN), tedy logického kanálu na fyzickém vedení. Na jednom fyzickém propojení může být zřízena a provozována řada VPN. Provoz každé VPN je oddělen od provozu jiných VPN. Součástí služby „Připojení OVM k CMS 2.0“ je možnost žádat o propojení jednotlivých VPN na síťové úrovni. Pokud každá VPN „patří“ jinému OVM, je k propojení dvou nebo více VPN požadován souhlas všech OVM.

V případě vytvoření fyzického i logického spojení uzavírají OVM s operátorem komerční smlouvy.

příklad: MD má LAN v jedné lokalitě a jeho podřízená organizace v jiné lokalitě a MD chce tyto dvě LAN propojit do jedné počítačové sítě. Obě lokality jsou fyzicky připojeny k CMS 2.0, každá přes jiného operátora. MD a podřízená organizace požádají každý zvlášť operátora o připojení své LAN k CMS 2.0 formou VPN. MD požádá provozovatele CMS 2.0 o propojení obou VPN. Provozovatel CMS 2.0 si vyžádá souhlas podřízené organizace, obě VPN připojí k CMS 2.0 a umožní mezi nimi síťový provoz bez jakéhokoli omezení.

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

V případě připojení OVM k CMS 2.0 přes **krajskou síť** si dohodne OVM připojení se správcem nebo provozovatelem příslušné krajské sítě. V takovém případě má smlouvu se správcem CMS 2.0 správce příslušné krajské sítě. A provozovatel krajské sítě zajistí fyzické i logické připojení lokalit OVM k CMS 2.0.

Pro usnadnění připojení OVM na úrovni krajů obsahuje CMS 2.0 možnost připojení přes Krajské konektory CMS 2.0.

Krajský konektor je souhrn technických síťových zařízení umístěných v každém kraji propojených s centrálními uzly CMS 2.0 komunikačními linkami CMS 2.0. Operátorům KIVS a provozovatelům krajských sítí se stačí připojit ke Krajskému konektoru CMS 2.0. Z hlediska uživatelů CMS 2.0 je připojení k centrálním uzlům CMS 2.0 a k některému z Krajských konektorů ekvivalentní.

Speciálním případem připojení skupiny serverů k CMS 2.0 je jejich umístění do Národního datového centra (NDC). **NDC** jsou DC určená pro umístění aplikací poskytujících centrální eGON služby. Správcem prostředí centrálních eGON služeb je MV, které stanovuje podmínky pro to, aby se nějaké DC mohlo stát NDC a aby nějaká aplikace mohla poskytovat centrální eGON služby.

Služba CMS 2.0 „Umístění aplikace do NDC“ pomáhá OVM zajistit podmínky pro umístění aplikace poskytující centrální eGON služby do NDC. Poskytne OVM informace nezbytné pro to, aby se aplikace stala aplikací poskytující centrální eGON služby a byla umístěna do jednoho nebo více NDC. Zprostředkuje OVM nezbytné kontakty na správce prostředí centrálních eGON služeb a na správce a provozovatele NDC. Mj. zprostředkuje pronájem konektivity (na L2 nebo L3) s definovanými technickými parametry mezi dvěma NDC. Konektivita je určena k propojení dvou instancí téže aplikace zejména pro účely klastrování a synchronizace obsahu databází a pro interní komunikaci logických částí téže aplikace umístěných v různých NDC. Součástí služby je připojení instancí aplikace k CMS 2.0 formou VPN.

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

Připojení OVM k CMS 2.0 **přes Internet** znamená připojení pomocí VPN vytvořené přes veřejný Internet. OVM má při tomto způsobu připojení do Internetu od libovolného poskytovatele připojení k Internetu. Pro připojení k CMS 2.0 potřebuje OVM technické zařízení (VPN koncentrátor) nebo software (VPN klienta), které je technicky schopné navázat spojení s VPN koncentrátorem na straně CMS 2.0. Je možné žádat o připojení celých LAN nebo o připojení jednotlivých osob.

Po vyřízení příslušné žádosti obdrží OVM od provozovatele CMS 2.0 identifikační (jméno) a autentizační (heslo anebo certifikát) údaje pro připojení svého zařízení, respektive software k VPN koncentrátoru CMS 2.0. Každá LAN i každý uživatel mají svůj individuální identifikační a autentizační údaj. Pro připojení OVM k CMS 2.0 přes Internet se používají dvě technická řešení VPN – SSL a IPSec. IPSec je určeno pro připojování jak LAN, tak jednotlivých osob. SSL je určeno pro připojování osob. IPSec a SSL VPN připojené k CMS 2.0 přes Internet jsou uvnitř CMS 2.0 reprezentovány stejným způsobem jako logická připojení OVM přes operátora KIVS, tj. formou VPN. Jde o jiný typ VPN, než je IPSec nebo SSL VPN.

příklad: MD má LAN ve dvou lokalitách a chce tyto dvě LAN propojit do jedné počítačové sítě. Jedna lokalita je fyzicky připojena k CMS 2.0 přes operátora KIVS a druhá má připojení do Internetu. MD požádá provozovatele CMS 2.0 o připojení LAN z první lokality k CMS 2.0 formou VPN, o připojení LAN z druhé lokality formou IPSec VPN a o jejich propojení. Provozovatel CMS 2.0 obě VPN připojí k CMS 2.0 a umožní mezi nimi síťový provoz bez jakéhokoli omezení.

Speciálním případem připojení k CMS 2.0 přes Internet je připojení k některému z Extranetů CMS 2.0. **Extranet** je skupina aplikačních služeb určených pro stejný okruh OVM. Složení aplikačních služeb pro jednotlivé Extranety určuje MV jakožto správce CMS 2.0. Jednotlivé OVM žádají o přístup k Extranetům při zřizování přístupu k CMS 2.0 s využitím IPSec nebo SSL VPN. Publikaci aplikačních služeb do Extranetu i jednotlivá připojení k Extranetu schvaluje správce CMS 2.0.

příklad: MV definuje ve spolupráci s dalšími orgány státní moci množinu aplikačních služeb pro podporu agend vykonávaných ORP. Provozovatel CMS 2.0 vytvoří na žádost správce CMS 2.0 Extranet s označením „Agendy ORP“. Správci jednotlivých aplikačních služeb požádají provozovatele CMS 2.0 o publikaci do Extranetu „Agendy ORP“. Jednotlivé ORP podle potřeby požádají o připojení k Extranetu.

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

SLUŽBY CERTIFIKAČNÍ AUTORITY

Certifikační autorita (CA) CMS 2.0 je neveřejná CA vydávající certifikáty pouze pro účely připojení IPSec a SSL VPN přes Internet. Uživatelé žádají o první certifikát pro určitou VPN při žádosti o připojení k CMS 2.0 přes Internet. O další certifikační služby (dočasné zablokování certifikátu, odblokování certifikátu, odvolání certifikátu) žádají službou CMS 2.0 „Služby CA".

CA CMS 2.0 poskytuje seznam odvolaných certifikátů (CRL) do prostředí Internetu i KIVS.

SLUŽBY eGSB

eGON Service Bus (eGSB) je specializovaný software určený k propojování aplikací pomocí zasílání datových zpráv. K eGSB se z jedné strany připojují aplikace, které nabízejí prostřednictvím eGSB aplikační služby a data, a z druhé strany se připojují klientské aplikace, které služby a data nabízené prostřednictvím eGSB využívají. Aplikační služby eGSB nabízené klientským aplikacím tvoří malá (v řádu jednotek) a relativně neměnná množina služeb, které jsou publikovány do prostředí KIVS, IPSec/SSL VPN (ne do Extranetů) a do Internetu. eGSB požadavky na tyto služby převede na volání aplikačních služeb, které z druhé strany eGSB nabízejí jiné aplikace.

O připojení k eGSB v roli klientských aplikací nemusejí správci aplikací žádat. K eGSB mají automaticky povolený přístup všechny IS, kterým Správa základních registrů (SZR) povolila přístup k Informačnímu systému základních registrů (ISZR). Musí tedy jít o Agendové informační systémy (AIS) splňující podmínky zákona o ZR a podmínky stanovené SZR. Pro přístup k eGSB použijí stejné certifikáty a IP adresy jako pro přístup k ISZR.

O připojení k eGSB v roli aplikací poskytujících služby prostřednictvím eGSB musí správci IS žádat standardním způsobem. Pro přístup k eGSB používají také certifikáty vydané Certifikační autoritou (CA) SZR.

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy" (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

PŘIPOJENÍ OVM DO INTERNETU

Pokud má nějaký OVM zřízenu přípojku k CMS 2.0 přes operátora KIVS, může využít služby CMS 2.0 pro připojení do Internetu. Prvním způsobem připojení je tzv. **přímé připojení do Internetu**. Při něm připojí provozovatel CMS 2.0 LAN OVM do Internetu bez jakýchkoli omezení. Tedy, provoz mezi LAN a Internetem není nijak kontrolován a filtrován.

Druhým způsobem připojení je **zabezpečené připojení do Internetu**. Při něm je obsah komunikace podroben kontrole s cílem zabránit ohrožení LAN OVM z Internetu (a naopak). Provoz mezi LAN OVM a Internetem probíhá přes proxy a firewally, je kontrolován na přítomnost škodlivého kódu a zařízení CMS 2.0 brání kybernetickým útokům včetně (D)DoS útoků z Internetu.

PŘIPOJENÍ OVM DO sTESTA

sTESTA je počítačová síť EU. Pokud má nějaký OVM zřízenu přípojku do CMS 2.0 přes operátora KIVS nebo IPSec nebo SSL VPN, může využít služby CMS 2.0 pro připojení do sTESTA. Služba umožňuje propojit OVM se sítí sTESTA. Prostupy mohou být obousměrné. Propojení se definují na úrovni IP adres a TCP/UDP portů. OVM musí akceptovat bezpečnostní pravidla sítě sTESTA.

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

ELEKTRONICKÁ POŠTA

CMS 2.0 poskytuje služby přeposílání elektronické pošty. Přeposílání znamená, že v CMS 2.0 nejsou žádné poštovní schránky. Ty musí být mimo CMS 2.0 a jejich správu a provoz zajišťují OVM. Služby elektronické pošty CMS 2.0 mají dvě varianty, které je možné používat odděleně i současně. První varianta umožňuje příjem elektronické pošty pro určené domény (např. mvcr.cz). Elektronická pošta pro domény musí být směrována na mail servery CMS 2.0. Směrování musí zajistit OVM, typicky se dělá pomocí MX záznamů v DNS. Mail servery CMS 2.0 přijímají maily pro určené domény z libovolných mail serverů (adres) z prostředí Internetu a KIVS, zkontrolují je a pošlou na mail servery OVM.

Druhá varianta umožňuje odesílání zpráv elektronické pošty. Při jejím využití musí OVM určit mail servery (pomocí IP adres) a mail domény (jména), ze kterých bude elektronická pošta odesílána. Mail servery CMS 2.0 přijímají zprávy pro odeslání pouze z určených adres a domén. Cílová adresa je libovolná a může ležet v prostředí Internetu nebo KIVS.

Hlavní přidanou hodnotou jsou v obou případech antivirová, antispamová a další bezpečnostní kontroly elektronické pošty. Další přidanou hodnotou je zvýšení dostupnosti celkového řešení elektronické pošty pro OMV. Servery CMS 2.0 ponechávají po určitou omezenou dobu zprávy ve frontách, pokud není mail server pro přeposlání dostupný, a pokoušejí se zprávu opakovaně doručit.

příklad: MD vlastní doménu mdcr.cz a má službu CMS 2.0 „Elektronická pošta“. Mezi DNS záznamy na Internetu jsou MX záznamy, které určují, že mail serverem pro doménu mdcr.cz je mdcr.gov.cz. mdcr.gov.cz je veřejná adresa mail serveru CMS 2.0 pro příjem elektronické pošty z Internetu. Na tomto mail serveru CMS 2.0 je nadefinováno, že mj. přijímá zprávy pro doménu mdcr.cz a že má zprávy pro tuto doménu poslat na adresu smtp1.mdcr.cms nebo smtp2.mdcr.cms. Mail server CMS 2.0 se pokusí veškeré zprávy pro doménu mdcr.cz doručit nejprve na první adresu a v případě její nedostupnosti na druhou adresu. Pokusy doručení opakují až do vyčerpání limitu a poté odešlou zpět odesilateli zprávu o nedoručitelnosti.

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

JMENNÉ SLUŽBY

Jmenné služby (DNS) je doplňková služba CMS 2.0. Uživatelé mají možnost žádat o přidělení DNS jmen při požadavcích na různé služby CMS 2.0 – při publikaci aplikačních služeb, příjmu elektronické pošty apod. DNS CMS 2.0 spravuje (je autoritativní) pro neveřejnou doménu „cms“ pro prostředí KIVS a pro veřejnou doménu „gov.cz“ pro prostředí Internetu. Nelze vznášet požadavky na DNS pro jakékoli jiné domény. Veškeré záznamy musí být uloženy na serverech CMS 2.0, tj. nelze delegovat správu poddomén (např. „mvcr.gov.cz“) na servery uživatelů.

Všechny spravované domény mohou být na žádost uživatele, který je „vlastníkem“ domény, zabezpečeny pomocí DNSSEC.

ZÁZNAMY O PROVOZU CMS 2.0

CMS 2.0 ukládá automaticky řadu záznamů o svém provozu. Tyto záznamy používá zejména k následujícím účelům:

- **Sledování provozu a předcházení problémovým stavům.**
- **Detekce bezpečnostních událostí.**
- **Získávání podkladu pro účtování služeb CMS 2.0 uživatelům.**
- **Poskytování údajů o provozu uživatelům CMS 2.0.**

Jednou ze služeb CMS 2.0 je poskytování údajů o provozu uživatelům CMS 2.0 jednak ve formě standardních reportů a statistik a za druhé skutečně zpřístupněním jednotlivých záznamů. Platí, že uživateli jsou zpřístupňovány pouze provozní záznamy a statistiky, které se ho týkají, tj. vznikly v souvislosti se službami CMS 2.0, které mu „patří“.

Součástí záznamů není datový obsah komunikace, ale údaje o něm. Tak např. záznamy o elektronické poště obsahují údaje o odesilateli, adresátech, času odeslání, respektive přijetí zprávy, velikosti zprávy, výsledku antispamové a antivirové kontroly a případně další podobné informace. Ne ale obsah zprávy ani jejích příloh.

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

SEZNAM ZKRATEK

CA	Certifikační autorita. Subjekt určený k vydávání certifikátů veřejných klíčů.
DC	Datové centrum.
DNS	Domain Name System. Systém překladu jmen na IP adresy a naopak.
eGON	Elektronizace veřejné správy sledující zefektivnění fungování státní správy a místní samosprávy a zjednodušení výkonu služeb veřejné správy.
eGSB	EgonServiceBus. Implementace integrační platformy pro komunikaci ISVS.
IP	Internetový protokol.
IPSec	Bezpečnostní rozšíření protokolu IP, umožňující šifrování a autentizaci každého paketu.
ISZR	Informační systém Základních registrů.
JIP	Jednotný identitiní prostor. Adresář uživatelů z veřejné správy.
KIVS	Komunikační infrastruktura Informačních systémů veřejné správy.
LAN	Local Area Network. Lokální počítačová síť.
NDC	Národní datové centrum.
OVM	Orgán veřejné moci.
SSL	Secure Socket Layer. Protokol pro zabezpečení komunikace šifrováním a digitálním podpisem.
SZR	Správa základních registrů.
TCP	Transmission Control Protocol. Protokol zajišťující přenos dat (transportní vrstva).
VPN	Virtual Private Network. Virtuální privátní síť.

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

POZNÁMKY

INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Projekt „Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy“ (CZ.1.06/1.1.00/03.05995) je spolufinancován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.

Vydalo Ministerstvo vnitra v rámci projektu Centrální místo služeb.
2015