Pravidla komunikace v systému Lékařský email

Úvod

Tento dokument specifikuje technické a procesní požadavky pro komunikaci v systému Lékařský email. Lékařský email je systém sloužící pro posílání zpráv mezi zdravotnickými zařízeními, která mají přiřazené IČP. Systém garantuje identitu odesílatele a příjemce díky certifikační politice, integritu zprávy a čitelnost zprávy pouze odesílatelem/příjemcem a nikým jiným díky standardnímu kryptografickému zabezpečení.

Vymezení pojmů

- IČP: identifikační číslo pracoviště, které přiděluje VZP zdravotnickému pracovišti a jejich seznam zveřejňuje v číselníku IČP
- eZprava: referenční implementace klientského programu splňující technické požadavky a podporující procesní požadavky definované tímto dokumentem
- Obchodní rejstřík – služba provozovaná Ministerstvem spravedlnosti na adrese https://or.justice.cz

Zúčastněné subjekty

- Registrátor a tvůrce referenční implementace – firma eZprava.net s.r.o.
- Uživatel – libovolné pracoviště zdravotnického zařízení pracoviště, které má přidělené IČP

Technické požadavky

Architektura systému je typu klient-server. Šifrování a dešifrování probíhá na straně klienta, server slouží pouze pro výměnu zašifrovaných zpráv. Systém sestává z těchto služeb:

1. Služba CA – podporuje procesy popsané v Certifikační politice
2. Adresářová služba – registrovaným uživatelům umožňuje vyhledávat v seznamu již vydaných certifikátů
3. Emailová služba – slouží k výměně emailových zpráv

Servery pro službu CA a adresářovou službu provozuje registrátor, emailové servery pak provozuje buď registrátor, uživatel, nebo libovolná třetí strana. Vzhledem k tomu, že na emailovém serveru jsou uloženy vždy jen zašifrované zprávy, tak bezpečnost těchto serverů není kriticky důležitá a v případě jejich kompromitace nedojde k ohrožení bezpečnosti dat.

Veškeré funkce na straně klienta implementuje program eZprava, uživatel ale může použít i programy třetí strany, které jsou v souladu s níže uvedenými standardy.

Použité standardy

Klientská komponenta pro využívání služeb CA musí podporovat standardy X.509, X.501, X.520, PKCS #10: Certification Request Syntax Specification, PKCS #12: Personal Information Exchange Syntax Standard. Komunikace se serverem CA probíhá dle protokolu SOAP nad protokolem HTTPS. Pro dokončení registrace musí komponenta implementovat výpočet SHA1 z *CertificationRequestInfo* obsahujícího pouze *subject* a *subjectPublicKeyInfo*, tzn. bez dalších atributů jako např. *subjectAltName*.

Klientská komponenta pro využívání adresářových služeb musí podporovat protokol HTTPS a Cryptographic Message Syntax (RFC 5652).

Emailový klient MUSÍ podporovat standard S/MIME 3.2 (RFC 5750 a RFC 5751) a všechny z toho vyplývající standardy. Dále MUSÍ podporovat RFC 2634 Enhanced Security Services for S/MIME, konkrétně „triple wrapping" a „signed receipt". Pro komunikaci s emailovým serverem je nutná podpora protokolů SMTP nad TLS a POP3 nad STARTSSL a nebo IMAP.

Emailový server MUSÍ podporovat protokol SMTP nad TLS a POP3 nad STARTSSL a nebo IMAP.

Procesní požadavky

Certifikační politika

Registrace nového uživatele

Uživatel vygeneruje pár klíčů (soukromý a veřejný) a žádost o podepsání certifikátu (CSR – certificate signing request) ve formátu dle PKCS #10. Jméno subjektu je konstruováno podle číselníku VZP:

Subject CSR	Sloupec v číselníku IČP	Příklad
CN	IČP Odbornost Osoba	56457001 128 Machek Petr
O	Název1*	Fresenius Medical Care-DS, s.r.o. [IČ 45790949]
OU	Název2	hemodialýza
L	Město; Ulice; PSČ	Louny; Rybalkova 1400; 44001
C	-	CZ
E	-	56457001.icp@lekarskyemail.cz
TelephoneNumber	-	+420 123 123 123

* k názvu je doplněno IČ zadané uživatelem

V databázi jsou evidovány tyto údaje: datum podání žádosti, IP adresa.

Registrace nového uživatele probíhá dvěma alternativními způsoby:

Pomocí poštovních služeb:

1. Uživatel zvolí IČP, IČ a vygeneruje pár klíčů a CSR podle tabulky.
2. Uživatel odešle písemnou žádost/smlouvu ve dvou vyhotoveních opatřenou razítkem a podpisem o aktivaci na adresu provozovny registrátora.
3. Uživatel odešle elektronicky CSR na server registrátora.

4. Registrátor ověří, že:
    a. CSR je zkonstruován dle tabulky a záznam v číselníku IČP má platné datum platnosti smlouvy s VZP.
    b. název1 odpovídá obchodnímu názvu vedenému v Obchodním rejstříku pro IČ
    c. smlouva je podepsána a orazítkována osobou, která má právo uzavírat smlouvy za IČ dle Obchodního rejstříku.
5. Registrátor podepíše CSR kořenovým certifikátem a v zašifrované podobě vystaví nově vzniklý certifikát uživatele na serveru, heslo pak odešle doporučeným dopisem pouze do vlastních rukou žadatele spolu s kontrasignovanou smlouvou/žádostí a to na adresu uvedenou v Obchodním rejstříku pro IČ.
6. Uživatel obdrží smlouvu a heslo, kterým dešifruje podepsaný certifikát. V tuto chvíli je uživatel viditelný pro ostatní uživatele systému a může začít přijímat a odesílat zprávy.

Elektronicky:

1. Uživatel zvolí IČP, IČ a vygeneruje pár klíčů a CSR podle tabulky.
2. Uživatel digitálně podepíše smlouvu **kvalifikovaným osobním certifikátem** a spolu s CSR ji elektronicky odešle na server registrátora.
3. Registrátor ověří, že:
    a. komponenta O (organization) v CSR je složena z názvu ekonomického subjektu a IČ. Název ekonomického subjektu odpovídá Názvu1 v platném záznamu pro IČP v číselníku IČP VZP (kde IČP je určeno z prvních osmi znaků komponenty CN) a zároveň obchodnímu názvu vedenému v Obchodním rejstříku pro IČ
    b. certifikát použitý k podpisu smlouvy je platný a byl vystaven na osobu, která má právo uzavírat smlouvy za ekonomický subjekt určený IČ. Výsledkem tohoto ověření je PDF podepsané kvalifikovaným systémovým certifikátem získané z Obchodního rejstříku.
4. V případě kladného ověření registrátor podepíše CSR kořenovým certifikátem a v nezašifrované podobě vystaví nově vzniklý certifikát uživatele na serveru. Registrátor zároveň kontrasignuje smlouvu a uloží ji na serveru a zpřístupní ji uživateli. Emailem je uživateli odeslána notifikace o úspěšné registraci. V tuto chvíli je uživatel viditelný pro ostatní uživatele systému a může začít přijímat a odesílat zprávy.

Alternativně si uživatel může nechat vystavit ekvivalentní **systémový certifikát** (kvalifikovaný, nebo komerční) od akreditované certifikační autority a registrátor zahrne tento certifikát do registru na základě smlouvy.

Prodloužení certifikátu

Platnost certifikátu je prodloužena pokud nedojde ke zrušení smlouvy mezi registrátorem a jednatelem firmy na jejíž IČP byl certifikát vystaven.

Revokace certifikátu

Certifikát je revokován zařazením do CRL (Certificate revocation list) na základě žádosti jednatele firmy na jejíž IČP byl certifikát vystaven.

Distribuce klientského programu

Referenční implementace eZprava je distribuována pomocí technologie Microsoft ClickOnce a každá verze programu je podepsána certifikátem registrátora, který byl vydán certifikační autoritou jejíž kořenový certifikát je již nainstalován v počítači klienta. Součástí instalace eZpravy je kořenový „self signed“ certifikát vydaný registrátorem a tímto certifikátem jsou podepsány certifikáty všech uživatelů eZpravy.