Lékařský email — elektronická výměna dat ve zdravotnictví pomocí S/MIME

eZprava.net s.r.o.

21. ledna 2015

Abstrakt

Tento dokument popisuje technické požadavky nutné pro zabezpečenou výměnu dat ve zdravotnictví kompatibilní s referenční implementací „eZpráva“ [eZprava].

1 Úvod

Elektronická komunikace ve zdravotnictví vyžaduje vysokou míru zabezpečení. Odesílatel i příjemce musí být jednoznačně identifikovatelní, zpráva musí být čitelná pouze pro odesílatele a příjemce nesmí být schopen přeposlat zprávu třetí osobě jménem odesílatele. Odesílatel musí být informován o doručení zprávy do informačního systému příjemce.

2 Technická specifikace

Celé řešení vychází z existujících standardů tak aby bylo možné v co největší míře využít existující emailovou infrastrukturu a snížit tak náklady na implementaci a přitom zaručit vysokou škálovatelnost a dostupnost.

2.1 Obsah zprávy

Tato specifikace nijak neomezuje obsah zprávy. Stejně jako u emailu je tělo zprávy buď text a nebo HTML, v příloze lze pak zaslat libovolný formát dat. Následující odstavce jsou pouze doporučení vhodná pro použití ve zdravotnictví.

Zpráva by měla být strojově zpracovatelná a zároveň by měla splňovat požadavky pro vedení zdravotní dokumentace v čistě elektronické podobě. Tyto požadavky splňuje příloha ve formátu PDF 1.3 a vyšší nebo PDF/A podepsaná kvalifikovaným certifikátem obsahující v příloze soubor ve formátu DASTA 3. Důvody jsou popsány dále.

Je vhodné, aby zpráva byla strojově zpracovatelná. Jako doporučený formát strukturovaných dat se v současnosti jeví DASTA 3 [DASTA3]. Tento formát vzniklý pod záštitou Ministerstva zdravotnictví

je podporován mnoha informačními systémy používanými ve zdravotnictví.

Pro vedení zdravotní dokumentace v čistě elektronické podobě je nutné splnit podmínky dané legislativou, konkrétně Předpis č. 372/2011 Sb. Zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách). Podle § 55 a bodu h) musí být výstupy ze zdravotnické dokumentace převeditelné do listinné podoby autorizovanou konverzí dokumentu. Autorizovanou konverzi do listinné podoby lze provést podle Předpisu č. 300/2008 Sb. Zákon o elektronických úkonech a autorizované konverzi dokumentu pouze pokud je dokument opatřen podpisem kvalifikovaným certifikátem a prováděcí vyhláška pak určuje, že dokument musí být ve formátu PDF 1.3 a vyšším nebo v PDF/A. Digitální podpis pak může být součástí PDF, nebo externí. Zatímco certifikát sloužící k podpisu a šifrování zprávy může být sdílen mezi pracovníky daného pracoviště, tak kvalifikovaný certifikát sloužící k podpisu PDF musí být vázán pouze na konkrétního pracovníka, který PDF vytvořil a je za jeho obsah odpovědný.

Z důvodu dlouhodobé archivace je pak vhodné aby podpis splňoval požadavky na Advanced Electronic Signature dle [RFC5126], tzn. minimálně musí být přítomen podepsaný atribut `signing-certificate-v2` dle [RFC5035].

Podepsané soubory by měly být co nejdříve opatřeny kvalifikovaným časovým razítkem z důvodu nepopiratelnosti a poté vždy když končí platnost certifikátu časového razítka a nebo použité kryptografické přestanou být považovány za bezpečné. Řešení popsané v [RFC4998] poskytuje návod na implementaci pomocí Merkleova stromu.

2.2 Formát zprávy

Zpráva před zašifrováním musí být ve formátu Internet Message Format podle [RFC5322]. Hlavičky zprávy nesmí obsahovat citlivá data (např. v předmětu nesmí být uvedeno RČ). Tělo zprávy musí být ve formátu MIME [RFC2045]. Pokud zpráva obsahuje v příloze strukturovaná data, pak by tato data měla být reprezentována i v čitelné podobě (kvůli uživatelům, jejichž informační systém, mají-li nějaký, neumí zpracovávat strukturovaná data).

Vzhledem k tomu, že předmět v hlavičce emailu nesmí obsahovat citlivá data, certifikát příjemce i odesílatele může být vztažen k více pracovištím a zpráva se může týkat konkrétního pacienta, pak je vhodné aby v takových případech zpráva obsahovala přílohu s metadaty ve formátu DASTA 3:

- Předmět
- IČP[1] odesílatele
- IČP příjemce
- RČ, jméno a příjmení pacienta

2.3 Zabezpečení zprávy

Tělo zprávy musí být podepsáno, poté zašifrováno a poté může být znova podepsáno kvůli zabránění podloudnému přeposílaní. Způsob šifrování i podpisu je definován v [RFC5751], Triple wrapping

[1] identifikační číslo pracoviště

(podepsání vnější obálky) je definováno v [RFC2634]. Zprávy, které nemají vnější podpis mohou být zobrazeny uživateli s upozorněním, že odesílatele zprávy nelze prokazatelně určit. Pokud však zpráva obsahuje informaci o příjemci (např. ve formátu DASTA 3), pak vnější podopis není nutný. Zcela nepodepsané zprávy by měly být ignorovány protože se může jednat o spam.

2.4 Transport zprávy

Zprávy musí být odesílány pomocí SMTP [RFC5321] na emailovou adresu příjemce uvedenou v certifikátu, který byl použit k zašifrování zprávy.

2.5 Zpracování doručené zprávy

Informační systém příjemce musí vždy potvrdit úspěšné přijetí zprávy odesláním Message Disposition Notification [RFC3798], `disposition-type` musí mít hodnotu `processed`. Toto potvrzení potvrzuje pouze přijetí zprávy informačním systémem příjemce, ne že uživatel zprávu četl nebo ji porozuměl.

Bezpečnější alternativou k MDN je Signed receipt definovaný v [RFC2634]. Zda je jeho použití nezbytné je věcí další diskuze.

2.6 Adresář uživatelů

Globální adresář uživatelů je tvořen množinou certifikátů, kde každý certifikát identifikuje zdravotnické pracoviště. Údaje o pracovišti zrcadlící číselník IČP VZP jsou součástí certifikátu podepsaného eZprava CA nebo akreditovanou certifikační autoritou.

Certifikáty jsou dostupné prostřednictvím protokolu HTTP. Získání certifikátu příjemce probíhá ve dvou krocích - stažení seznamu certifikátů a stažení jednotlivých certifikátů. Seznam certifikátů je textový soubor kde je na každé řádce SHA1 otisk certifikátu. Klient tento soubor získá na dohodnuté adrese, přičemž nutnost stažení souboru nejprve zkontroluje pomocí hlavičky `Last-Modified`. Podle otisku lze pomocí HTTP GET získat konkrétní certifikát. Při prvním spuštění stáhne klient všechny certifikáty uvedené v seznamu, při dalším spuštění pak stahuje jen nové certifikáty.

Kromě globálního adresáře může informační systém uživateli umožnit správu lokálního adresáře certifikátů, v němž nejsou certifikáty vázané na IČP. To umožní komunikaci uživatele např. s jednotlivými lékaři, pacienty či firmami.

2.6.1 Dynamické získání certifikátu

S ohledem na budoucí rozvoj je vhodné aby bylo možné získat certifikát příjemce standardizovaným způsobem pokud odesílatel zná emailovou adresu příjemce. Toho lze dosáhnout uložením certifikátu do DNS záznamu typu `CERT` dle [RFC4398]. Toto řešení je škálovatelné, protože cachování certifikátu zajišťuje infrastruktura DNS. Dotazy na certifikát tak nemusí obsluhovat server příjemce, ale např. DNS server poskytovatele internetového připojení odesílatele.

2.7 Požadavky na kryptografické funkce

V souladu s doporučením [NIST] musí být používány RSA klíče o velikosti alespoň 2048 bitů a hashovací funkce silnější než SHA1, např. SHA-224. Pro šifrování musí být použito Three-key Triple DES nebo AES-128 a silnější.

3 Závěr

Dokument popisuje doporučený obsah, formát, zabezpečení, transport a zpracování zpráv. Nespecifikuje formát přenášených dat ani jejich zpracování z hlediska zdravotnického informačního systému uživatele.

Reference

[RFC5322] Resnick, P. *Internet Message Format* [online]. Dostupný z WWW: <http://tools.ietf.org/html/rfc5322>.

[RFC2045] Freed, N., Borenstein, N. *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies* [online]. Dostupný z WWW: <http://tools.ietf.org/html/rfc2045>.

[RFC5751] Ramsdell, B., Turner, S. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification* [online]. Dostupný z WWW: <http://tools.ietf.org/html/rfc5751>.

[RFC5321] Klensin, J. *Simple Mail Transfer Protocol* [online]. Dostupný z WWW: <http://tools.ietf.org/html/rfc5321>.

[RFC3798] Hansen, T., Vaudreuil, G. *Message Disposition Notification* [online]. Dostupný z WWW: <http://tools.ietf.org/html/rfc3798>.

[RFC5126] Pinkas, D., Pope, N., Ross, J. *CMS Advanced Electronic Signatures (CAdES)* [online]. Dostupný z WWW: <http://tools.ietf.org/html/rfc5126>.

[RFC5035] Schaad, J. *Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility* [online]. Dostupný z WWW: <http://tools.ietf.org/html/rfc5035>.

[RFC2634] Hoffman, P. *Enhanced Security Services for S/MIME* [online]. Dostupný z WWW: <http://tools.ietf.org/html/rfc2634>.

[RFC4398] Josefsson, S. *Storing Certificates in the Domain Name System (DNS)* [online]. Dostupný z WWW: <http://tools.ietf.org/html/rfc4398>.

[RFC4998] Gondrom, T., Brandner, R., Pordesch, U. *Evidence Record Syntax (ERS)* [online]. Dostupný z WWW: <http://tools.ietf.org/html/rfc4998>.

[DASTA3] MZ ČR *Datový standard MZ ČR* [online]. Dostupný z WWW: <http://ciselniky.dasta.mzcr.cz>.

[eZprava] eZprava.net s.r.o. *eZpráva* [počítačový program]. Dostupný z WWW: <https://www.lekarskyemail.cz>.

[NIST] Barker, E., Roginsky, A. *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.* Dostupný z WWW: <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>.