ZNALECKÝ POSUDEK

Znalecký posudek č. 164-18/2017

Posouzení naplnění požadavků Nařízení EU 679/2016 o GDPR komunikačním systémem eZpráva

Účel posudku	Podklad pro Zadavatele
Posudek k datu	20. října 2017
Objednatel znaleckého posudku	MUDr. Petr Machek Zabušany 120 417 71 Zabrušany
Zhotovitel znaleckého posudku	Vít Lidinský, znalec Jeseniova 500/8 130 00 Praha 3, Žižkov IČ: 71443029
Číslo výtisku/počet výtisků	posudek je vyhotoven ve dvou výtiscích č. 1 – č. 2, z toho oba výtisky jsou určeny pro objednatele.
Posudek obsahuje celkem	12 stran textu včetně titulní strany ve formě A4, přílohy na CD
Datum a místo zpracování:	20. října 2017, Praha
Výtisk číslo:	2
Zpracoval	Vít Lidinský

Obsah:

Seznam použitých zkratek a pojmů:

- PKI – Public Key infrastructure;
- eZpráva – eZprava.net s.r.o.;
- GDPR – General Data Protection Regulation;
- ISDS – Informační systém datových schránek;
- IČO – Identifikační číslo;
- IČP – Identifikační číslo provozovny;
- NIS – Nemocniční informační systém;
- OS – Operační systém;
- CA – Certifikační autorita;
- VZP – Všeobecná zdravotní pojišťovna;
- SW – Software;
- EU – Evropská unie;

1. Nález

1.1. Účel zpracování posudku

Účelem zpracování posudku je vytvořit podklad pro Objednatele.

1.2. Předmět posudku

Předmětem posudku je Odpovědět na následující otázku Objednatele:

Posuďte, zda komunikační systém eZpráva může být využit v souladu s požadavky Nařízení EU 679/2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (General Data Protection Regulation).

Tabulka č. 1: Základní identifikace Objednatele

Název	MUDr. Petr Machek
Sídlo	Zabrušany 120, 417 71 Zabrušany
Identifikační číslo	
Kontaktní osoba objednatele	Petr Machek, Petr.Machek@fmc-ag.com

2. Výchozí podklady

Poklady využité při zpracování znaleckého posudku obsahuje Tabulka č. 2

Tabulka č. 2: Podklady pro posouzení

1.	Schůzka s p. Petrem Machkem ze dne 9.10.2017
2.	Prezentace o projektu eZpráva (10 slidů)
3.	Pravidla komunikace v systému Lékařský email (4 strany)
4.	Lékařský email - elektronická výměna dat ve zdravotnictví pomocí S/MIME (5 stran)
5.	

Uvedené podklady pro posouzení poskytl objednatel nebo byly pořízeny zpracovatelem posudku z veřejně dostupných zdrojů.

3. Posudek

3.1. Popis vzniklé situace

Společnost eZprava.net s.r.o. vyvinula komunikační systém eZpráva. Jedná se o komunikační systém založený na emailových zprávách šifrovaných za pomoci asymetrické kryptografie. eZpráva je primárně zaměřena na komunikaci mezi zdravotnickými zařízeními, jednotlivými lékaři a laboratořemi.

V souvislosti s Nařízením EU 679/2016 GDPR (dále jen „nařízení“) je Znalec žádán o prověření, zda komunikační systém eZpráva vyhovuje požadavkům uvedeného nařízení na ochranu osobních údajů a ochranu zvláštních kategorií osobních údajů.

3.2. Požadavek GDPR

Vzhledem k povaze komunikačního systému eZpráva Znalec akcentuje požadavek nařízení uvedený v článku 32, který se věnuje zabezpečení zpracování osobních údajů.

Podle článku 32, odst. 2 se při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Podle článku 32, odst. 1 s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku.

Na základě zkušeností Znalce s implementací požadavků GDPR ve zdravotnictví vyvstává problém s předáváním zvláštních kategorií osobních údajů (zdravotnické záznamy) mezi jednotlivými zdravotnickými pracovišti nebo laboratořemi. V současné době se tak běžně děje emailovou komunikací, která je z pohledu požadavku GDPR zcela nevyhovující, jelikož nedochází k žádné ochraně osobních údajů.

3.3. eZpráva

Komunikační systém eZpráva se zaměřuje výhradně na ochranu komunikace mezi zdravotníky, zdravotnickými zařízeními nebo laboratořemi. Z hlediska GDPR je možno systém eZpráva porovnat s ISDS, který rovněž zajišťuje komunikaci informací různých typů údajů zabezpečeným způsobem. V rámci ISDS je ovšem nevyhovující vazby jedné schránky na jednu

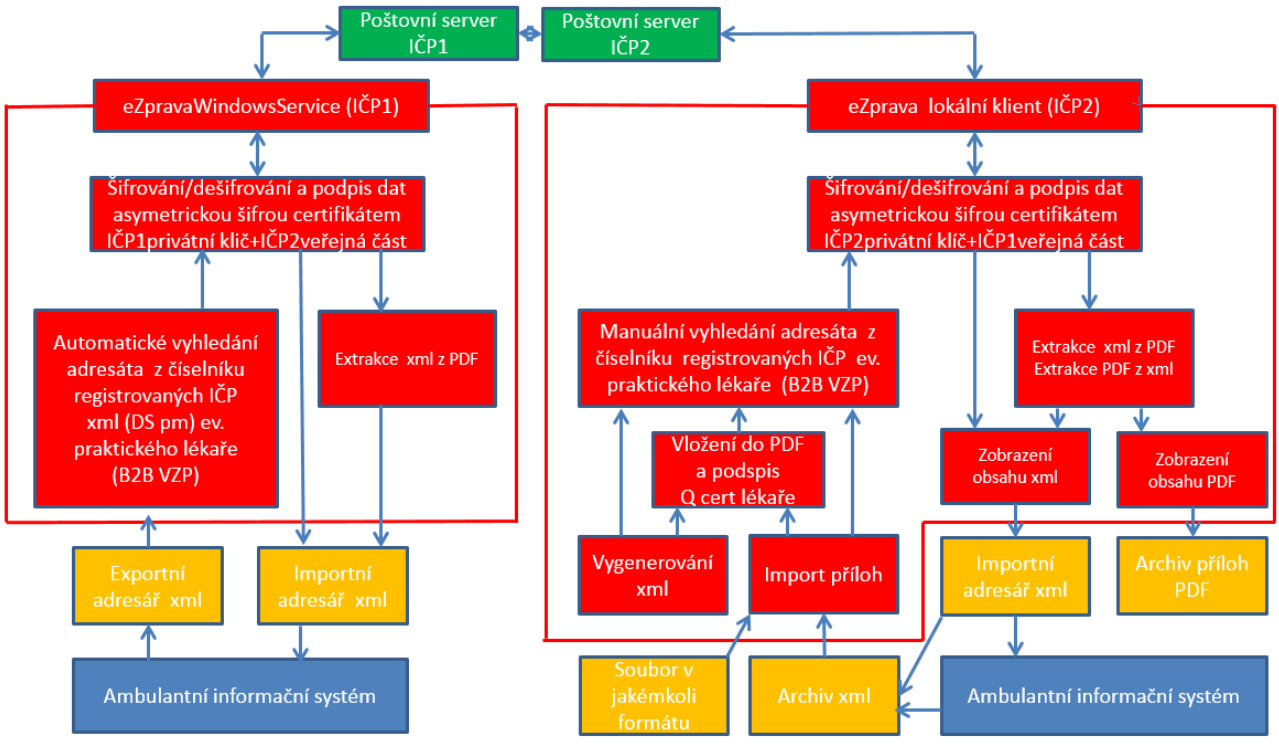
organizaci (IČO), přičemž uvnitř organizace je nezbytné zajistit distribuci a přidělování zpráv jiným způsobem. Navíc v případě, kdy zdravotník není orgánem veřejné moci, musí za každou zprávu hradit poplatek 18,-Kč.

eZpráva má systém adresátů navázán na IČP. IČP je v tomto případě identifikační číslo pracoviště v rámci jednoho zdravotnického zařízení (IČO), případně se jedná o jednoho konkrétního samostatného lékaře. IČP přiděluje VZP a aktuální seznam přidělených IČP zveřejňuje. IČP je vázáno na konkrétní pracoviště a je spjaté s vedoucím atestovaným lékařem. eZpráva tedy umožňuje prostřednictvím IČP adresovat samostatné lékaře, případně vedoucí lékaře jednotlivých oddělení.

3.4. Architektura eZpráva

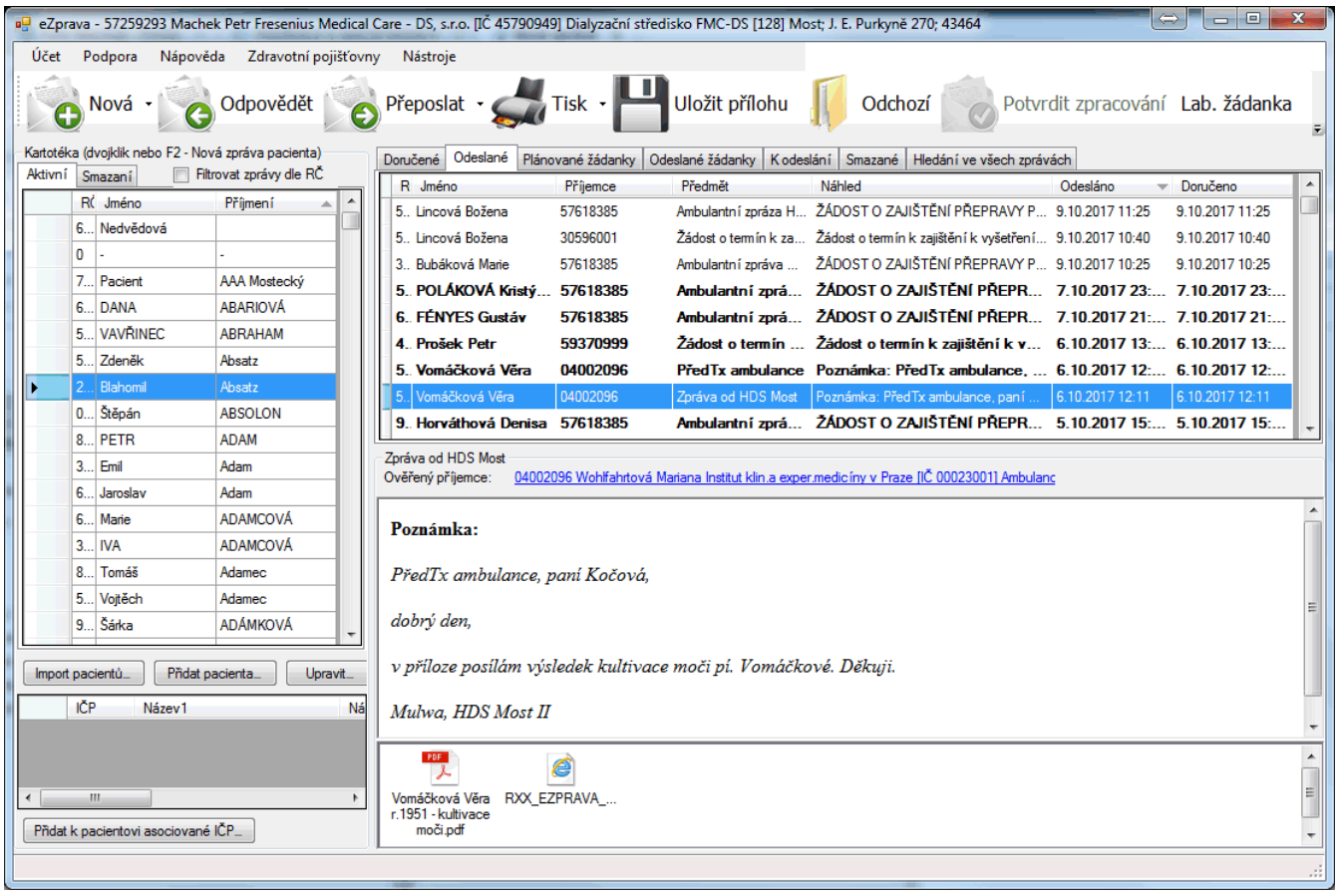
eZpráva je komunikačním systémem, který je založen na PKI. K tomuto účelu využívá vlastní CA. Důvodem využití vlastní CA je množství informací, které jsou vedeny v certifikátu (kormě jména a příjmení držitele také IČO organizace a IČP).

eZpráva dále disponuje dvěma variantními aplikacemi, jejichž schémata jsou uvedena na následujícím obrázku.



eZpráva může být nasazena ve formě serverové aplikace, která načítá a exportuje zprávy do NIS. Takto aplikace funguje v případech, kdy jsou jednotlivé zprávy uživateli prezentovány za pomoci NIS.

eZpráva může být dále nasazena jako samostatná lokální aplikace, která zajišťuje přenos zpráv a současně disponuje prezentační vrstvou pro uživatele, v rámci které zajišťuje čtení a odesílání datových zpráv. Prostředí lokální aplikace eZpráva je zobrazeno na následujícím obrázku.



Samotné šifrování zprávy v rámci eZpráva je realizováno za pomoci veřejného klíče IČP (fyzické osoby), které je zpráva doručována. Doručenou zprávu tak nemůže dešifrovat jiná osoba, než vlastník soukromého klíče. Tento způsob šifrování poskytuje významně vyšší úroveň bezpečnosti než již zmíněný ISDS nebo jiný prostředek na bázi symetrického šifrování, kdy klíčový materiál je k dispozici na více místech, čímž je násobně náchylnější k provedení jeho kompromitaci.

3.5. Získání certifikátu

Pro získání certifikátu CA eZpráva (možnost používání aplikace) je nezbytné provést stažení aplikace eZpráva. Samotný instalační soubor aplikace sZpráva je podepsán nezávislým poskytovatelem certifikačních služeb společností Comodo pro zajištění důvěrnosti instalačního balíčku aplikace.

Po provedení stažení je realizováno generování žádosti o vystavení certifikátu. Generování žádosti probíhá v rámci aplikace eZpráva na lokálním počítači uživatele. V aplikaci je rovněž uchován privátní klíč uživatele shodně jako následně vydaný certifikát. eZpráva nevyužívá standardních prostředků úložiště certifikátů OS Windows. Do certifikátu je uvedeno jméno žadatele, email, IČP a IČO.

Žádost o vystavení certifikátu je odeslána společnosti eZprava.net s.r.o., která reaguje zasláním smlouvy. V rámci smluvního ujednání je provedeno nezbytné ověření toho, že dané IČP patří ke konkrétní organizaci (IČO). Smlouva o vystavení certifikátu fyzické osobě reprezentující IČP je tak potvrzena jednatelem konkrétní zdravotnické organizace. Tímto způsobem je ze strany eZprávy též zajištěn seznam ČP v rámci jednotlivých zdravotnických zařízení, kterým je možno provést doručení eZprávy.

Po provedení ověření vazby IČO a IČZ a současně provedení kontroly na aktivní certifikáty daného IČP je certifikát vydán. Postupy pro vydávání a odvolání certifikátu jsou uvedeny na webových stránkách www.lekarskyemail.cz.

3.6. Bezpečnostní rizika eZprávy

V rámci hodnocení rizik aplikace eZpráva je možné vyloučit možnost dešifrování zpráv na úrovni jednotlivých pracovníků společnosti eZprava.net s.r.o., jelikož tito pracovníci nedisponují privátním klíčem jednotlivých IČP a tedy je technicky vyloučena možnost zásahu, čtení nebo editování jednotlivých zpráv.

Ze strany administrátorů tedy nehrozí zásadní rizika, maximálně možnost zřízení IČP, které dosud není obsazeno, přičemž na toto IČP by následně mohly být doručeny osobní údaje. Takový postup je ovšem značně komplikovaný a odhalitelný nastavenými procesy ve společnosti.

Jako středně významné je z hlediska Znalce hodnoceno riziko uchování zdravotnických záznamů po provedení jejich dešifrování v otevřené podobě na lokálním počítači uživatele. Toto riziko je ovšem platné pouze do verze 3.0.0.0. aplikace eZpráva, od které jsou data na lokálním disku zašifrována. Jejich bezpečnost je tak od verze 3.0.0.0. možno hodnotit jako nesrovnatelně vyšší než ostatní zdravotnické aplikace (kartotéka pacientů, evidenční lékařský či jiný SW).

4. Výrok

Na základě všech skutečností zjištěných tímto znaleckým posudkem konstatuji, že:

Komunikační systém eZpráva může být využit v souladu s požadavky Nařízení EU 679/2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (General Data Protection Regulation). Komunikační systém eZpráva splňuje požadavky článku 32 GDPR na zajištění bezpečnosti dat a to na technicky velmi vysoké úrovni asymetrické kryptografie. Za pomoci systému eZpráva lze jistě zasílat též zvláštní kategorie osobních údajů.

V Praze dne 20. října 2017

Vít Lidinský

znalec

5. Znalecká doložka

Znalecký posudek jsem podal jako znalec jmenovaný rozhodnutím Městského soudu v Praze ze dne 8.9.2011 č.j. 1820/2011 pro základní obor ekonomika, pro odvětví ceny a odhady se specializací informační systémy, dále pro obor kybernetika, odvětví výpočetní systémy se specializací informační systémy.

Znalecký úkon je zapsán pod pořadovým číslem 164-18/2017 do znaleckého deníku.

Znalečné a náhradu nákladů /náhradu mzdy/ účtuji podle připojené likvidace na základě dokladu č. 2017024.

V Praze dne 20. října 2017

Vít Lidinský

znalec

6. Přílohy

- Podkladové materiály objednatele

Všechny přílohy jsou pro zajištění autenticity elektronicky podepsány Znalcem.