VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

ELEKTRONICKÁ IDENTIFIKACE A SLUŽBY VYTVÁŘEJÍCÍ DŮVĚRU PRO ELEKTRONICKÉ TRANSAKCE
ELECTRONIC IDENTIFICATION AND TRUST SERVICES IN ELECTRONIC TRANSACTIONS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Lukáš Hrbotický**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Václav Zeman, Ph.D.**
SUPERVISOR

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Informační bezpečnost**
Ústav telekomunikací

Student: Lukáš Hrbotický ***ID:*** 173657
Ročník: 3 ***Akademický rok:*** 2017/18

NÁZEV TÉMATU:

Elektronická identifikace a služby vytvářející důvěru pro elektronické transakce

POKYNY PRO VYPRACOVÁNÍ:

Uveďte definice a vysvětlení pojmů, které se využívají pro oblasti elektronické komunikace a jsou uvedeny v nařízení eIDAS (Zákon o službách vytvářejících důvěru pro elektronické transakce č. 297/2016 Sb.). Zaměřte se především na popis technických prostředků, které tyto služby zajišťují. Navrhněte a realizujte systém, který bude demonstrovat funkčnost uvedených služeb.

DOPORUČENÁ LITERATURA:

[1] DOSTÁLEK, Libor. - VOHNOUTOVÁ, Marta. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. Vyd. 2. Brno : Computer Press, 2010. 544 s. ISBN 978-80-251-2619-6.

[2] Zákon č. 297/2016 Sb. Zákonu o službách vytvářejících důvěru pro elektronické transakce. Sbírka zákonů České republiky. 2016, částka 115, s. 4466-4504. ISSN 1211-1244.

Termín zadání: 5.2.2018 ***Termín odevzdání:*** 29.5.2018

Vedoucí práce: doc. Ing. Václav Zeman, Ph.D.
Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Tato bakalářská práce se zabývá problematikou elektronické identifikace a služeb vytvářejících důvěru pro elektronické transakce. Práce popisuje a vysvětluje pojmy, které se využívají v oblasti elektronické komunikace a jsou uvedeny v nařízení eIDAS. Dále se zabývá řešeními demonstrující služby vytvářející důvěru. V praktické části je návrh laboratorní úlohy, kdy si student vyzkouší možnosti, které certifikační autorita nabízí. Cílem práce je definice a vysvětlení pojmů dle nařízení eIDAS a realizace systému, který funkčnost těchto služeb bude demonstrovat.

KLÍČOVÁ SLOVA

Elektronická transakce, elektronická identifikace, bezpečnost, eIDAS, certifikát, digitální podpis, elektronický podpis, elektronická pečeť, elektronické časové razítko, služba elektronického doporučeného doručování, autentizace internetových stránek, certifikační autorita, gnoMint, laboratorní úloha

ABSTRACT

Bachelors thesis talking about problematics of electronic identification and trust services in electronic transactions. It describes and explains concepts used in the area of electronical communication mentioned in regulation eIDAS. Solutions demonstrating trust services are part of the work. As practical part of this thesis was created laboratory exercise, in which will students try the possibilities offered by certification authority. The goal of this work is explanation and definition of concepts according to eIDAS regulations and realization of system demonstrating these services.

KEYWORDS

Electronic transactions, electronic identification, security, eIDAS, certificate, digital signature, electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services, website authentication, certification authority, gnoMint, laboratory exercise

HRBOTICKÝ, Lukáš. *Elektronická identifikace a služby vytvářející důvěru pro elektronické transakce*. Brno, 2018, 62 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: doc. Ing. Václav Zeman, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Elektronická identifikace a služby vytvářející důvěru pro elektronické transakce“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora

PODĚKOVÁNÍ

Děkuji vedoucímu práce doc. Ing. Václavu Zemanovi, Ph.D. za cenné rady, metodickou, odbornou a trpělivou pomoc při zpracování bakalářské práce.

Brno ....

podpis autora

OBSAH

SEZNAM OBRÁZKŮ

ÚVOD

Cílem této bakalářské práce je seznámení se s problematikou elektronické identifikace a služeb vytvářejících důvěru pro elektronické transakce. Dále pak realizovat systém, který bude demonstrovat funkčnost těchto služeb.

V úvodu práce je stručný rozbor nařízení eIDAS. Zmiňujeme zde důvody jeho přijetí, popisujeme jednotlivé části jeho obsahu a v přehledné tabulce uvádíme porovnání rozdílů definic pojmů dle staré a nové legislativy. Dále komentujeme technické řešení služeb vytvářejících důvěru.

Druhá kapitola se zabývá digitálním podpisem. Tento systém zde popisujeme z hlediska kryptografie a pomocí schematu vysvětlujeme mechanismus podepisování a ověřování pravosti digitálního podpisu a integrity podepsaných dat.

Třetí kapitola pojednává o výhodách využití certifikátů a distribuci veřejných klíčů s jejich využitím. Na názorných schematech popisujeme způsob, jak útočník může komunikaci kompromitovat a dále, jak probíhá ověření platnosti daného certifikátu.

Ve čtvrté kapitole popisujeme elektronický podpis jako právní pojem. Uvádíme jeho jednotlivé stupně důvěrnosti, popisujeme zde také požadavky na něj kladené a jejich možnou realizaci v technické praxi.

Pátá kapitola v krátkosti popisuje elektronickou pečeť, na kterou zde nahlížíme jen jako na právní pojem.

V šesté kapitole rozebíráme problematiku elektronických časových razítek a postup označování elektronických dokumentů tímto razítkem.

V sedmé kapitole je popsána služba elektronického doporučeného doručování.

V osmé kapitole popisujeme poslední ze služeb vytvářejících důvěru, jak nám je definuje nařízení eIDAS, a to autentizaci internetových stránek a využívání SSL/TLS protokolu.

Devátá kapitola popisuje návrh systému pro demonstraci služeb vytvářejících důvěru. Uvádíme zde přehled dostupných řešení spolu s jejich výhodami a nevýhodami.

Poslední kapitola je návrhem laboratorní úlohy, kde si klademe za cíl seznámit se s principem činnosti certifikační autority.

V závěru shrnujeme poznatky uvedené v této bakalářské práci.

1 NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) Č. 910/2014

Náplní této kapitoly je stručně si povědět základní informace o Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS). Řekneme si, proč vůbec bylo nařízení přijato a co si klade za cíl. Dále velmi zkráceně nastíníme obsah eIDAS a v závěru si na praktickém příkladu popíšeme služby vytvářející důvěru.

1.1 Důvody přijetí nařízení

Důvodem pro přijetí eIDAS a jeho hlavním cílem je snaha dotvořit jednotný digitální trh Evropské unie a zvýšit důvěryhodnost a bezpečnost poskytovaných služeb tak, aby v budoucnu bylo možné nahradit papírový svět světem digitálním.

Pro lepší pochopení si uveďme příklad. Pokud např. obchodujeme, tak víme, že na druhé straně sedí obchodník a nikoli neviditelný pes o jehož identitě nic nevíme (název neviditelný pes byl vymyšlen právě proto, že nevíme, kdo sedí na druhé straně) [3]. Naopak pokud my, jako obchodník, komunikujeme se svým zákazníkem, tak víme, že existuje, a že má nějakou fyzickou identitu.

Úmyslně jsme zvolili tento příklad, protože eIDAS není zdaleka jen pro veřejnou správu. Je to úprava důvěru vytvářejících služeb pro celou Evropskou unii na celém digitálním trhu, tj. jak komerční sféru, tak i veřejnoprávní sféru.

1.2 Forma eIDAS a jeho rozdělení

Přestože Evropská unie vydává mnoho směrnic, pro eIDAS byla zvolena forma nařízení. Nařízení je přímo aplikovatelné a má aplikační přednost před vnitrostátními právními předpisy. Pro aplikaci směrnice je nutné, aby členský stát vytvořil transpoziční zákon, který by na tuto směrnici adaptoval právní řád [8]. Tím se proces přijetí prodlužuje.

Nařízení eIDAS má tři hlavní části:

- elektronická identifikace,
- služby vytvářející důvěru a
- elektronický dokument.

Podrobnější popis jednotlivých částí si uvedeme v následujících kapitolách.

1.2.1 Elektronická identifikace

V oblasti elektronické identity si eIDAS neklade za cíl zavést harmonizaci, ale interoperabilitu [23]. Reguluje výhradně uznávání přeshraniční elektronické identity. Tedy ne to, co daná identita znamená vnitrostátně a k čemu jsou ti jednotliví uživatelé autorizováni.

Definice: EIDAS [22] definuje elektronickou identifikaci takto: elektronickou identifikací se rozumí postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo zastupující právnickou osobu.

1.2.2 Služby vytvářející důvěru

Naproti tomu v oblasti služeb vytvářejících důvěru je cílem harmonizace [23]. Reguluje jejich poskytování, aby byl napříč Evropskou unií dosažen jednotný stupeň důvěryhodnosti elektronických dokumentů, a aby byly na důvěryhodné elektronické transakce kladeny podobné nároky.

Elektronický podpis

- elektronický podpis
- zaručený elektronický podpis
- kvalifikovaný elektronický podpis

Elektronické pečetě

- elektronická pečeť
- zaručená elektronická pečeť
- kvalifikovaná elektronická pečeť

Elektronická časová razítka

- elektronické časové razítko
- kvalifikované elektronické časové razítko

Služba elektronického doporučeného doručování

- služba elektronického doporučeného doručování
- kvalifikovaná služba elektronického doporučeného doručování

Autentizace internetových stránek

U problematiky autentizace internetových stránek nalezneme pouze rozdělení podle stupně důvěryhodnosti certifikátu:

- certifikát pro autentizaci internetových stránek,
- kvalifikovaný certifikát pro autentizaci internetových stránek.

Požadavky, které musejí případné certifikáty splňovat, jsou stanoveny v příloze IV [22].

Definice: Pro jednoznačnost si uveďme přesnou definici služeb vytvářejících důvěru tak, jak nám ji stanovuje článek 3 [22]: Službou vytvářející důvěru je elektronická služba, která je zpravidla poskytována za úplatu a spočívá ve vytváření, ověřování shody a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami nebo ve vytváření, ověřování shody a ověřování platnosti certifikátů pro autentizaci internetových stránek nebo v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami.

1.2.3 Elektronické dokumenty

Poslední, spíše minoritní, část týkající se elektronických dokumentů nám ve své podstatě jen říká, že elektronickému dokumentu nesmí být upírány právní účinky jen z důvodu, že má elektronickou podobu.

Definice: EIDAS [22] definuje elektronický dokument takto: elektronickým dokumentem se rozumí jakýkoli obsah uchovaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka.

1.3 Porovnání definic pojmů

Nařízení eIDAS přináší oproti zákonu č. 227/2000 Sb. Zákon o elektronickém podpisu (zrušen k 19. 9. 2016) nové definice řady pojmů týkající se služeb vytvářejících důvěru. Některé změny jsou pouze formální, jiné však zásadní. Je proto výhodné uvést si přehled těchto pojmů (viz tab. 1.1), protože řada lidí si jisté pojmy stále ještě spojuje se starými definicemi, což často vede k mylnému výkladu problematiky.

Tab. 1.1: Porovnání definic pojmů [11]

Pojem	**Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)**	**Definice dle nařízení č. 910/2014 (eIDAS)**
Podepisující osoba	Fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby.	Fyzická osoba, která vytváří elektronický podpis.
Elektronický podpis	Údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.	Data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání.
Zaručený elektronický podpis	Elektronický podpis, který splňuje následující požadavky: 1. je jednoznačně spojen s podepisující osobou, 2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě, 3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou, 4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.	Elektronický podpis, který splňuje požadavky stanovené v článku 26: a) je jednoznačně spojen s podepisující osobou; b) umožňuje identifikaci podepisující osoby; c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou; a d) je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
Kvalifikovaný elektronický podpis	Není výslovně definován.	Zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy.
Data pro vytváření elektronických podpisů	Jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu.	Jedinečná data, která podepisující osoba používá k vytváření elektronických podpisů.
Certifikát pro elektronický podpis	Datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu.	Elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických podpisů s určitou fyzickou osobou a potvrzuje alespoň jméno nebo pseudonym této osoby.
Kvalifikovaný certifikát pro elektronický podpis	Certifikát, který má náležitosti podle § 12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb. Podle §12: 1. Kvalifikovaný certifikát musí obsahovat a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona, b) v případě právnické osoby obchodní firmu nebo název a	Certifikát pro elektronický podpis, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze I: Kvalifikované certifikáty pro elektronické podpisy obsahují: a) označení, alespoň ve formě vhodné pro automatické zpracování, že

Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
	stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen, c) jméno, popřípadě jména, a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym, d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu, e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby, f) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný certifikát vydává, g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb, h) počátek a konec platnosti kvalifikovaného certifikátu,	se certifikát vydává jako kvalifikovaný certifikát pro elektronický podpis; b) soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikované certifikáty, včetně alespoň členského státu, v němž je poskytovatel usazen, a - v případě právnické osoby: název a případné registrační číslo uvedené v úředních záznamech, - v případě fyzické osoby: jméno osoby; c) alespoň jméno podepisující osoby nebo pseudonym. Je-li použit pseudonym, musí být tato skutečnost jasně vyznačena; d) data pro ověřování platnosti elektronických podpisů, která odpovídají datům pro vytváření elektronických podpisů; e) označení začátku a konce doby platnosti certifikátu; f) identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru;

Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
	i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití, j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít. 2. Omezení pro použití kvalifikovaného certifikátu podle odstavce 1 písm. i) a j) musí být zjevná třetím stranám. 3. Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby.	g) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává; h) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g); i) údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu; j) pokud jsou data pro vytváření elektronických podpisů spojená s daty pro ověřování platnosti elektronických podpisů obsažena v kvalifikovaném prostředku pro vytváření elektronických podpisů, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.
Služba vytvářející důvěru	-	Elektronická služba, která je zpravidla poskytována za úplatu a spočívá: a) ve vytváření, ověřování shody a ověřování platnosti elektronických podpisů, elektronických pečetí nebo

Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
		elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami nebo b) ve vytváření, ověřování shody a ověřování platnosti certifikátů pro autentizaci internetových stránek nebo c) v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami.
Kvalifikovaná služba vytvářející důvěru	-	Služba vytvářející důvěru, která splňuje použitelné požadavky stanovené v tomto nařízení.
Poskytovatel služeb vytvářejících důvěru	Poskytovatelem certifikačních služeb se rozumí fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy.	Fyzická nebo právnická osoba, která poskytuje jednu či více služeb vytvářejících důvěru buď jako kvalifikovaný, nebo jako nekvalifikovaný poskytovatel služeb vytvářejících důvěru.
Kvalifikovaný poskytovatel služeb vytvářejících důvěru	Kvalifikovaným poskytovatelem certifikačních služeb se rozumí poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo	Poskytovatel služeb vytvářejících důvěru, který poskytuje jednu či více kvalifikovaných služeb vytvářejících důvěru a kterému orgán dohledu

Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
	kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů (dále jen "kvalifikované certifikační služby") a splnil ohlašovací povinnost podle § 6.	udělil status kvalifikovaného poskytovatele.
Produkt	Nástrojem elektronického podpisu se rozumí technické zařízení nebo programové vybavení, nebo jejich součásti, používané poskytovatelem certifikačních služeb pro vytváření nebo ověřování elektronických podpisů nebo pro zajištění certifikačních služeb.	Technické zařízení nebo programové vybavení či jejich příslušné součásti, které jsou určeny k používání pro poskytování služeb vytvářejících důvěru.
Prostředek pro vytváření elektronických podpisů	Technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů.	Konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických podpisů.
Kvalifikovaný prostředek pro vytváření elektronických podpisů	-	Prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v příloze II: 1. Kvalifikované prostředky pro vytváření elektronických podpisů vhodnými technickými prostředky a postupy přinejmenším zajistí, aby:

Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
		a) byla přiměřeně zajištěna důvěrnost dat pro vytváření elektronických podpisů, která byla použita při vytváření elektronického podpisu; b) data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu se mohla prakticky vyskytnout pouze jednou; c) bylo přiměřeně zajištěno, že data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu nelze odvodit a že elektronický podpis je v současnosti dostupnými technickými prostředky spolehlivě chráněn proti padělání; d) oprávněná podepisující osoba měla možnost data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu spolehlivě chránit před jejich zneužitím třetí osobou. 2. Kvalifikované prostředky pro vytváření elektronických podpisů nesmějí měnit podepisovaná data ani bránit tomu, aby byla tato data předložena podepisující

Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
		osobě před vlastním podepsáním. 3. Data pro vytváření elektronických podpisů může jménem podepisující osoby vytvářet nebo spravovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru. 4. Aniž je dotčen bod 1 písm. d), smějí kvalifikovaní poskytovatelé služeb vytvářejících důvěru, kteří spravují data pro vytváření elektronických podpisů jménem podepisující osoby, kopírovat data pro vytváření elektronických podpisů pouze pro účely zálohování a jsou-li splněny tyto požadavky: a) bezpečnost zkopírovaných souborů dat je na stejné úrovni jako u původních souborů dat; b) počet zkopírovaných souborů dat nepřesáhne minimum potřebné pro zajištění kontinuity služby.
Pečetící osoba	Označující osobou se rozumí fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a	Právnická osoba, která vytváří elektronickou pečeť.

Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
	označuje datovou zprávu elektronickou značkou.	
Elektronická pečeť	Elektronickou značkou se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky: 1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu, 2. byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou, 3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.	Data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu.
Zaručená elektronická pečeť	-	Elektronická pečeť, která splňuje požadavky stanovené v článku 36: Zaručená elektronická pečeť musí splňovat tyto požadavky: a) je jednoznačně spojena s pečetící osobou;

Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
		b) umožňuje identifikaci pečetící osoby; c) je vytvořena pomocí dat pro vytváření elektronických pečetí, která může pečetící osoba s vysokou úrovní důvěry použít k vytváření elektronické pečeti pod svou kontrolou; a d) je k datům, ke kterým se vztahuje, připojena takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.
Kvalifikovaná elektronická pečeť	-	Zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť.
Data pro vytváření elektronických pečetí	Daty pro vytváření elektronických značek se rozumí jedinečná data, která označující osoba používá k vytváření elektronických značek.	Jedinečná data, která pečetící osoba používá k vytváření elektronických pečetí.
Certifikát pro elektronickou pečeť	Datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických	Elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických pečetí s určitou právnickou osobou a potvrzuje název této osoby.

Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
	značek s označující osobou a umožňuje ověřit její identitu.	
Kvalifikovaný certifikát pro elektronickou pečeť	Certifikát, který má náležitosti podle § 12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb. Podle §12: 1. Kvalifikovaný certifikát musí obsahovat a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona, b) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen, c) jméno, popřípadě jména, a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym, d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu, e) data pro ověřování podpisu, která odpovídají datům pro vytváření	Certifikát pro elektronickou pečeť, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze III: Kvalifikované certifikáty pro elektronické pečetě obsahují: a) označení, alespoň ve formě vhodné pro automatické zpracování, že se certifikát vydává jako kvalifikovaný certifikát pro elektronickou pečeť; b) soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikované certifikáty, včetně alespoň členského státu, v němž je poskytovatel usazen, a - v případě právnické osoby: název a případné registrační číslo uvedené v úředních záznamech, - v případě fyzické osoby: jméno osoby; c) alespoň jméno pečetící osoby a případné registrační číslo uvedené v úředních záznamech;

Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
	podpisu, jež jsou pod kontrolou podepisující osoby, f) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný certifikát vydává, g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb, h) počátek a konec platnosti kvalifikovaného certifikátu, i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití, j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít. 2. Omezení pro použití kvalifikovaného certifikátu podle odstavce 1 písm. i) a j) musí být zjevná třetím stranám. 3. Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby.	d) data pro ověřování platnosti elektronických pečetí, která odpovídají datům pro vytváření elektronických pečetí; e) označení začátku a konce doby platnosti certifikátu; f) identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru; g) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává; h) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g); i) údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu; j) pokud jsou data pro vytváření elektronických pečetí spojená s daty pro ověřování platnosti elektronických pečetí

Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
		obsažena v kvalifikovaném prostředku pro vytváření elektronických pečetí, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.
Prostředek pro vytváření elektronických pečetí	Prostředkem pro vytváření elektronických značek se rozumí zařízení, které používá označující osoba pro vytváření elektronických značek a které splňuje další náležitosti stanovené tímto zákonem.	Konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických pečetí.
Kvalifikovaný prostředek pro vytváření elektronických pečetí	-	Prostředek pro vytváření elektronických pečetí, který přiměřeně splňuje požadavky stanovené v příloze II.
Elektronické časové razítko	-	Data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku.
Kvalifikované elektronické časové razítko	Kvalifikovaným časovým razítkem se rozumí datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické	Elektronické časové razítko, které splňuje požadavky stanovené v článku 42: 1. Kvalifikované elektronické časové razítko musí splňovat tyto požadavky: a) spojuje datum a čas s daty takovým způsobem, aby byla přiměřeně

Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
	podobě existovala před daným časovým okamžikem.	zamezena možnost nezjistitelné změny dat; b) je založeno na zdroji přesného času, který je spojen s koordinovaným světovým časem; a c) je podepsáno s použitím zaručeného elektronického podpisu, opatřeno zaručenou elektronickou pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru nebo označeno jinou rovnocennou metodou.
Elektronický dokument	Datovou zprávou se rozumí elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na technických nosičích dat, používaných při zpracování a přenosu dat elektronickou formou, jakož i data uložená na technických nosičích ve formě datového souboru.	Jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka.
Služba elektronického doporučeného doručování	Upraveno zákonem č. 300/2008 Sb. (Zákon o elektronických úkonech a autorizované konverzi dokumentů)	Služba, která umožňuje přenášet data mezi třetími osobami elektronickými prostředky a poskytuje důkazy týkající se nakládání s přenášenými daty, včetně dokladu o odeslání a přijetí dat, a která chrání přenášená data před rizikem

Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
		ztráty, odcizení, poškození nebo neoprávněných změn.
Kvalifikovaná služba elektronického doporučeného doručování	Upraveno zákonem č. 300/2008 Sb. (Zákon o elektronických úkonech a autorizované konverzi dokumentů)	Služba elektronického doporučeného doručování, která splňuje požadavky stanovené v článku 44: 1. Kvalifikované služby elektronického doporučeného doručování musí splňovat tyto požadavky: a) jsou poskytovány jedním či více kvalifikovanými poskytovateli služeb vytvářejících důvěru; b) s vysokou úrovní spolehlivosti zajišťují identifikaci odesílatele; c) zajišťují identifikaci příjemce před doručením dat; d) odesílání a přijímání dat je zabezpečeno prostřednictvím zaručeného elektronického podpisu nebo zaručené elektronické pečeti kvalifikovaného poskytovatele služeb vytvářejících důvěru tak, aby byla vyloučena možnost nezjistitelné změny dat; e) odesílatel a příjemce dat jsou jednoznačně vyrozuměni o případných změnách dat potřebných za účelem odeslání nebo přijetí dat;

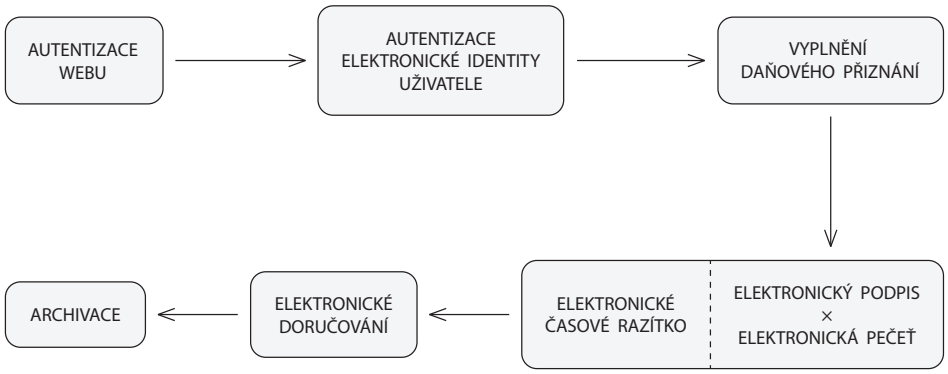
Pojem	Definice dle zákona č. 227/2000 Sb. (Zákon o elektronickém podpisu)	Definice dle nařízení č. 910/2014 (eIDAS)
		f) datum a čas odeslání, přijetí a případná změna dat jsou označeny prostřednictvím kvalifikovaného elektronického časového razítka.
Data pro ověřování platnosti	Daty pro ověřování elektronických podpisů se rozumí jedinečná data, která se používají pro ověření elektronického podpisu.	Data, která se používají k ověření platnosti elektronického podpisu nebo elektronické pečeti.
Ověřování platnosti	-	Postup ověřující shodu a potvrzující platnost elektronického podpisu nebo elektronické pečeti.

1.4 Možnost praktického využití služeb vytvářejících důvěru na příkladu

Pro lepší pochopení využití služeb vytvářejících důvěru v praxi si uveďme jednoduchý příklad podávání daňového přiznání online [23]. Schema postupu je znázorněno na obr. 1.1 a je to jeden z možných postupů, nikoli povinný, jak nahlížet na elektronickou transakci. Nyní si toto schema popíšeme.

1. První služba, kterou začínáme, je autentizace webu. Musíme mít jistotu, že komunikujeme se serverem daňové správy.
2. V další kroku se musíme identifikovat (a následně autentizovat, aby naše identifikace byla důvěryhodná) my, jako daňoví poplatníci, a že daňové přiznání podáváme jménem někoho konkrétního (ať už za sebe nebo za osobu, která nás k tomuto úkonu zmocnila).
3. Vyplněné daňové přiznání předáme do portálu veřejné správy a ten nám jeho přijetí potvrdí. V obou fázích lze využít různé prostředky k tomu, abychom daňové přiznání uzamkli a učinili ho neměnným. Následně dostaneme potvrzení, že bylo v uzamčené podobě přijato a nikdo nám ho nezmodifikoval. K tomuto účelu slouží různá kombinace prostředků:
   - *elektronický podpis* jako prostředek vyjadřující vůli fyzické osoby,
   - *elektronická pečeť* jako prostředek vyjadřující vůli právnické osoby,
   - případně v kombinaci s *elektronickým časovým razítkem*, které je legálním doložením času, kdy jsme tento úkon učinili a kdy jsme přes doručovací kanál přijali potvrzení.
4. Potvrzení o přijetí daňového přiznání nám daňová správa může poslat např. systémem doporučeného elektronického doručování (v kontextu České republiky se jedná o datovou schránku).
5. Na závěr musí existovat metody, jak daňové přiznání uložit a archivovat pro případ auditu třetí stranou nebo pro případ daňové kontroly.

Závěrem toho příkladu chceme upozornit na rozdíl významu slov *může* a *musí*. V různých fázích elektronické transakce se vybírají různé prostředky na to, co považujeme za důvěryhodné, a kromě zákonného rámce daného eIDASem, případně národní legislativou, je zbytek na komunikujících stranách. Nikde není stanoven přesný postup a pořadí použití jednotlivých služeb. To záleží na principech a provozních pravidlech té konkrétní poskytující služby [23].



Obr. 1.1: Využití služeb vytvářejících důvěru

1.5 Technické řešení na základě legislativy

Použití hardwarových tokenů anebo softwarovou implementaci eIDAS ani jeho prováděcí vyhlášky neřeší [27]. Podle vyjádření vedoucího oddělení vývoje České pošty, s.p., která je mj. provozovatelem certifikační autority PostSignum, jsme zjistili, jak se k této záležitosti staví právě certifikační autorita PostSignum.

Využívají výhradně kryptografický algoritmus založený na RSA s podpisovým algoritmem SHA256. Podporují velikost klíčů 2048 a 4096 bitů, přičemž 4096 bitů je v současnosti výjimkou. Hardwarové úložiště klíčů (token, čipové karty) podporují velikost klíčů pouze 2048 bitů. Výše uvedené algoritmy se využívají při podepisování všech typů vydávaných certifikátů pro koncové uživatele i pro certifikáty infrastrukturní, tedy i certifikáty pro podpis časových razítek. Pokud jde o normy technické a právní, tak certifikáty vydávají v souladu s nařízením EU 910/2014 – tzv. eIDAS a navazujícím zákonem 297/2016 Sb. o službách vytvářejících důvěru pro el. transakce. Certifikační autorita má status kvalifikovaného poskytovatele služeb vytvářející důvěru, takže můžou vydávat kvalifikované certifikáty dle eIDAS. [12]

Pokud jde o technické normy, tak jsme získali informaci, že se řídí dle:

- *ETSI EN 319 401* – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers,
- *ETSI EN 319 411* – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1 – 3,
- *ETSI EN 319 412* – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 – 5,
- *ETSI EN 119 312* – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites,

- *RFC 6960* – Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP,
- *RFC 5280* – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,
- *RFC 3647* – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

Jelikož technické normy nejsou závazné [18] [30], jedná se pouze o doporučení, kterými je, z důvodu zajištění dostatečné bezpečnosti, vhodné se řídit.

2 DIGITÁLNÍ PODPIS

V této kapitole si řekneme o digitálním podpisu jako o kryptografickém systému. Dále si vysvětlíme proces podepisování dat a následné ověření tohoto podpisu.

Je to kryptografický systém na bázi asymetrické kryptografie, kterým zajistíme, že pokud data útočník zmodifikuje, tak příjemce tuto skutečnost rozpozná. Digitální podpis nám také umožňuje v anonymním světě Internetu jednoznačně identifikovat totožnost podepisující entity. Digitální podpis přináší tyto výhody:

- integrita – příjemce má jistotu, že data nebyla od podpisu změněna,
- nepopiratelnost – odesílatel nemůže popřít, že daná data podepsal,
- **identita podepisujícího** – lze jednoznačně ověřit podepisující entitu.

Využití si digitální podpis našel mimo jiné i v oblasti veřejné správy, kde je snaha omezit papírové písemnosti. Aby měly státní orgány jistotu, že odeslaná data jsme skutečně vyplnili my, využijeme k tomu právě digitální podpis. Tím si také příjemce ověří, zda data přijal nezměněná a ve stejné podobě, v jaké jsme je odeslali.

Stejně tak v opačném případě, když dostaneme potvrzení o přijetí, vyrozumění, vyjádření . . . , které je digitálně podepsané, tak si můžeme ověřit jak totožnost podepisující entity, tak i jeho integritu.

Nyní si na příkladu elektronických dat popíšeme celý mechanismus podepisování a následné ověření digitálního podpisu a integrity doručených dat, jak je schematicky znázorněno na obr. 2.1.

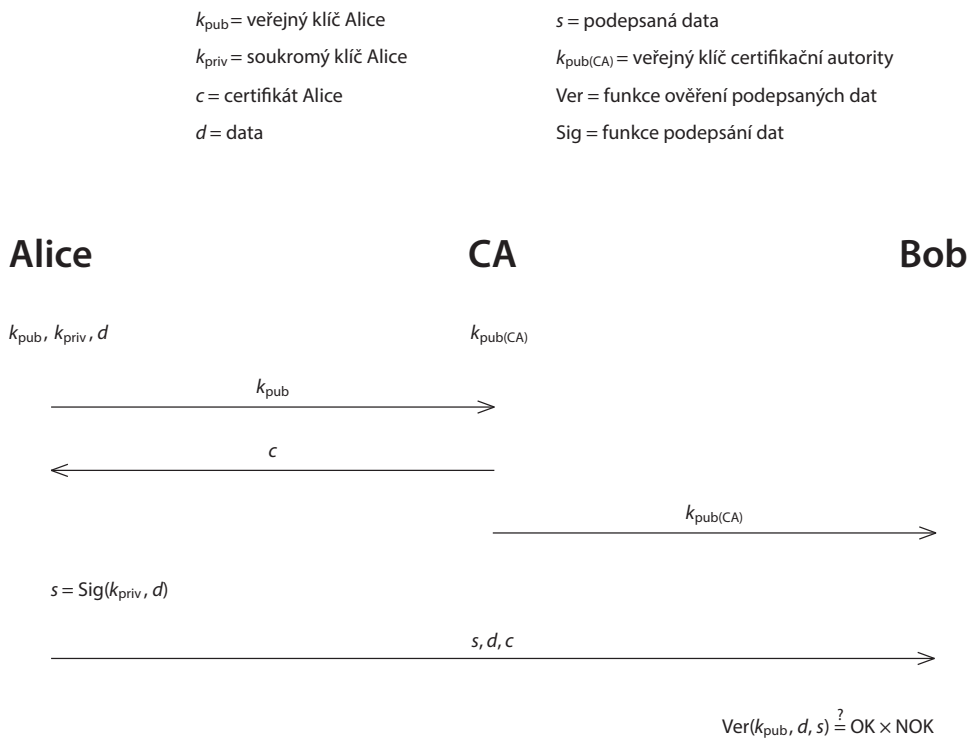
Podepisování: Z našich dat se pomocí hashovací funkce vytvoří *hash* (někdy mylně označován jako kontrolní součet [2]). Jako hashovací funkci použijeme některou z rodiny SHA-2 [13]. Tento se následně s využitím soukromého klíče odesílatele podepíše pomocí asymetrického kryptografického algoritmu. Využijeme některého z bezpečných algoritmů, třeba dle standardu ETSI TS 119312 jsou to např. RSA (s minimální délkou klíče 1 900 b.) nebo DSA (s délkou klíče minimálně 2 048 b.). Podle tohoto standardu se řídí i české certifikační autority; První certifikační autorita, a.s. a PostSignum (viz výše).

Přenos dat: Původní data, podepsaný hash a veřejný klíč odesílatele následně předáme příjemci. Pro doručení dat můžeme využít např. Internet, vnitřní podnikovou síť anebo některé z paměťových zařízení. Veřejný klíč se předává jako součást *certifikátu*, který obsahuje také informace o podepisující osobě a informace o certifikační autoritě, jenž tento certifikát vydala. Zjednodušeně můžeme certifikát chápat, jako veřejný klíč odesílatele podepsaný soukromým klíčem certifikační autority [4].

Pro zvýšení důvěryhodnosti přenosového kanálu, v případě využití veřejné sítě Internet, můžeme použít např. Virtual Private Network (VPN). Tento prostředek

vytvoří jakýsi šifrovaný „tunel“ mezi komunikujícími stranami, který zabrání případné nežádoucí činnosti útočníka.

Ověření podpisu: Poslední fází je ověření pravosti digitálního podpisu a integrity dat na straně příjemce. Příjemce dat, s využitím veřejného klíče odesílatele, ověří přijatý hash. Důvěryhodnost veřejného klíče si ověří na serveru vydávající certifikační autority. Stejnou hashovací funkcí, jako činil odesílatel, provede výpočet hashe z přijatých dat a tento porovná s ověřeným hashem. Pokud jsou porovnávané hashe shodné, můžeme prohlásit, že data byla doručena bez zásahu útočníka. Naopak, pokud jsou hashe rozdílné, můžeme mít podezření na modifikaci dat útočníkem nebo na chybu během přenosu.



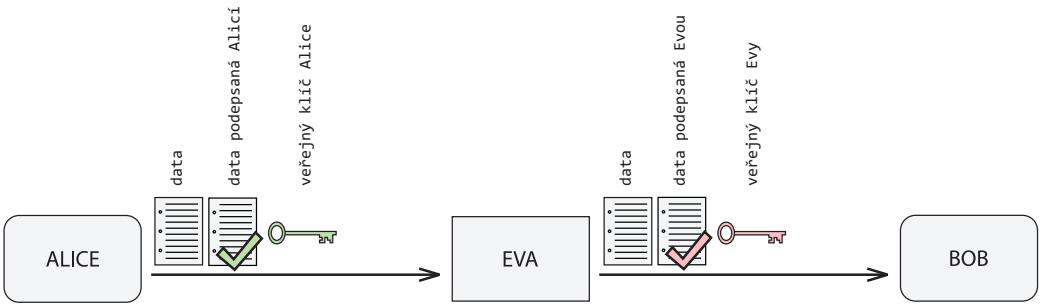
Obr. 2.1: Podepisování elektronických dat

Definice: Je to asymetrický kryptografický systém, který nám umožní zjistit, že pokud data útočník zmodifikuje, tak příjemce tuto skutečnost rozpozná. Obecně se pod pojmem digitální podpis chápe podpis vytvořený kryptografickými prostředky. [7]

3 CERTIFIKÁT

Zde si objasníme problematiku digitálních certifikátů, jejich význam, klasifikaci dle nařízení eIDAS a ukážeme si strukturu konkrétního certifikátu.

Digitální podpis využívá výhod asymetrické kryptografie, proto současně s podepsanými daty odesíláme příjemci (*Bob*) i veřejný klíč odesílatele (*Alice*), abychom byli schopni podpis ověřit. Je zde však riziko, že se do komunikace vloží třetí nežádoucí strana, útočník (*Eva*). Ten odchytne data odeslaná *Alicí*, znovu je podepíše, avšak za využití svého soukromého klíče, a takto nově podepsaná data spolu se svým veřejným klíčem odešle *Bobovi*. Tato situace je znázorněna na obr. 3.1.



Obr. 3.1: Útočník kompromitující komunikaci

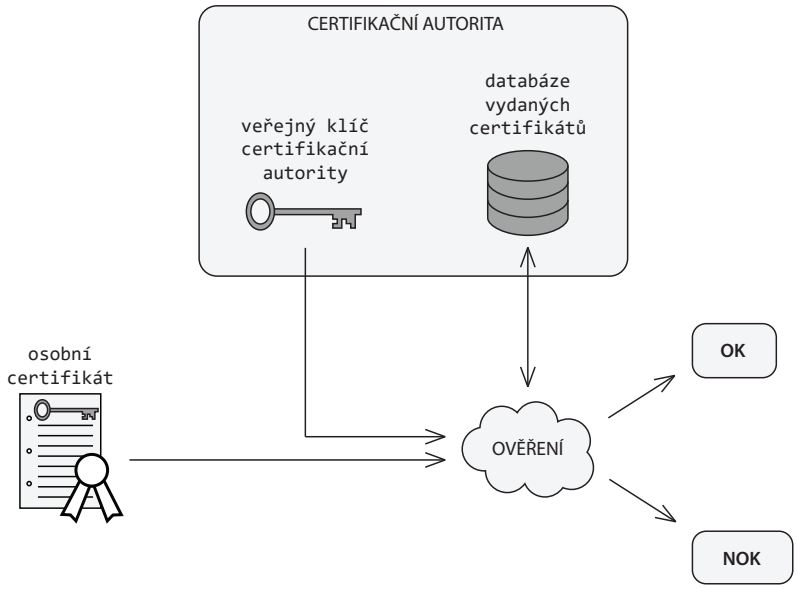
Pokud bychom nevyužívali výhod certifikátů, tak se *Bob* nedozví, že došlo k podepsání dat nežádoucí osobou. Jak jsme již zmínili, digitální podpis využívá výhod asymetrické kryptografie. Je tedy potřeba distribuce veřejného klíče mezi komunikujícími stranami, a to bezpečně! Za bezpečnou distribuci veřejného klíče můžeme považovat distribuci pomocí *certifikátu*.

Certifikát je soubor, který obsahuje mimo veřejný klíč vlastníka certifikátu i další informace jako např. informace o vlastníkovi a vydavateli certifikátu, době platnosti atd. Požadavky na údaje, které musejí být v certifikátu zahrnuty jsou uvedeny v přílohách nařízení eIDAS. Musíme zmínit, že eIDAS rozlišuje více druhů certifikátů a to podle účelu jejich použití:

- kvalifikované certifikáty pro elektronické podpisy,
- kvalifikované certifikáty pro elektronické pečetě,
- kvalifikované certifikáty pro autentizaci internetových stránek.

V *Příloze I*, *III* a *IV* nařízení eIDAS jsou uvedeny všechny údaje, které ten daný druh certifikátu musí obsahovat. Tento soubor, se všemi potřebnými obsaženými údaji, je podepsán soukromým klíčem certifikační autority, abychom zabránili jeho nežádoucí modifikaci.

Příjemce podepsaných dat a veřejného klíče podepisující osoby si pomocí volně dostupného veřejného klíče certifikační autority a databáze vydaných certifikátů ověří, zda není přijatý veřejný klíč podvržený útočníkem. Mechanismus ověření veřejného klíče u certifikační autority je znázorněn na obr. 3.2.



Obr. 3.2: Ověření pravosti certifikátu

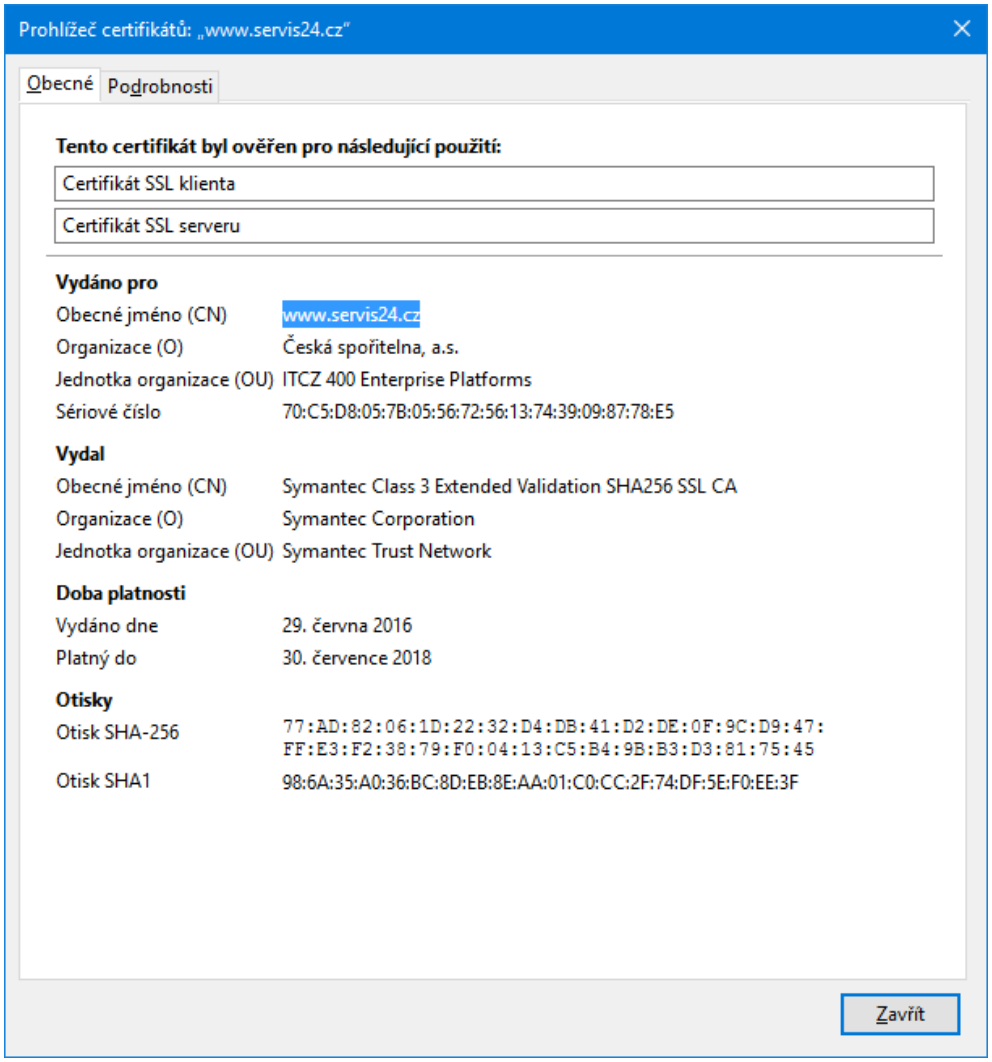
3.1 Ukázka certifikátu

Koncový uživatel si může certifikát zobrazit a ověřit vydávající certifikační autoritu anebo dobu platnosti. Pro ukázku si zvolíme certifikát České spořitelny. Na obr. 3.3 vidíme obecné informace o certifikátu zobrazené ve webovém prohlížeči Mozilla Firefox. Pokud se přepneme na kartu *Podrobnosti*, uvidíme všechny údaje certifikátu. Pro získání základního přehledu si uveďme:

- verze certifikátu,
- sériové číslo,
- algoritmus podpisu certifikátu,
- vydavatel,
- platnost od,
- platnost do,
- subjekt,
- algoritmus veřejného klíče subjektu,
- **veřejný klíč subjektu**,
- použití klíče certifikátu (k jakým službám můžeme daný certifikát využít),

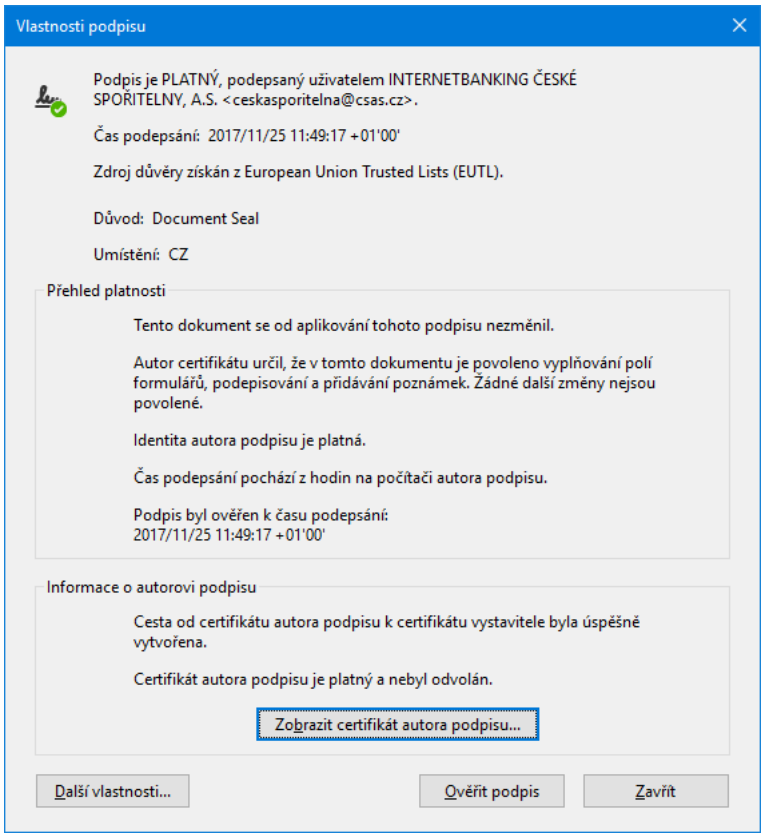
- distribuční body CRL atd.

Pokud porovnáme údaje z certifikátu s údaji uvedenými v *Příloze IV* nařízení eIDAS, zjistíme, že certifikát splňuje požadavky kladené nařízením eIDAS.

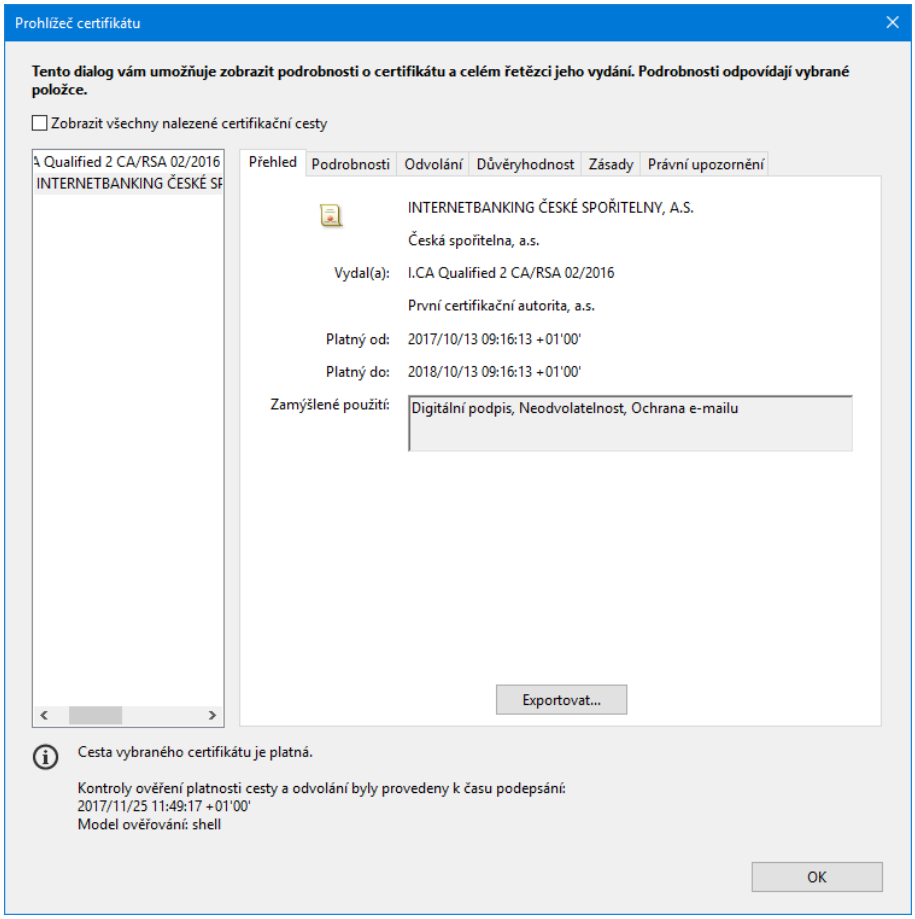


Obr. 3.3: Certifikát internetového bankovnictví České spořitelny

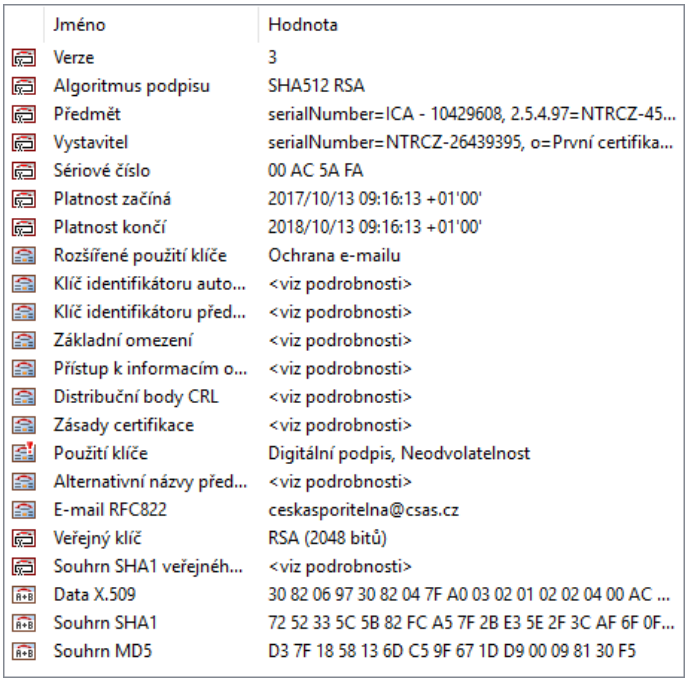
Na obr. 3.3 jsme viděli certifikát pro autentizaci internetových stránek tak, jak nám jej zobrazil webový prohlížeč. Nyní si opět na příkladu téže bankovní instituce ukážeme certifikát elektronického podpisu. Z internetového bankovnictví jsme si stáhli elektronický výpis z účtu a prohlížeč Adobe Acrobat Reader DC nám potvrdil (obr. 3.4) integritu dokumentu ověřenou elektronickým podpisem. Na obr. 3.5 vidíme přehled certifikátu. Máme možnost si všimnout, že Česká spořitelna vlastní minimálně dva certifikáty, první pro autentizaci internetových stránek a druhý pro elektronické podpisy. V podrobnostech certifikátu (obr. 3.6) můžeme vidět seznam položek, které certifikát obsazuje.



Obr. 3.4: Integrita dokumentu ověřená elektronickým podpisem



Obr. 3.5: Přehled certifikátu České spořitelny



Obr. 3.6: Podrobnosti certifikátu

Definice: Digitální certifikát je datová struktura obsahující především veřejný klíč vlastníka certifikátu (dále obsahuje např. informace o vlastníkovi a vlastnosti související s certifikátem). Nejdůležitějším úkolem certifikátu je ověření identity vlastníka veřejného klíče. Tímto zabraňujeme podvržení veřejného klíče. [16]

4 ELEKTRONICKÝ PODPIS

Právní řád nezná pojem digitální podpis, ale pouze elektronický podpis. Je to svým způsobem rezerva, kterou si zde právní řád nechává, pokud by se objevila nová forma elektronického podpisu, tak aby nebylo třeba provádět novelizaci všech dotčených právních předpisů.

Nařízení eIDAS rozlišuje tři typy elektronických podpisů podle stupně jejich důvěryhodnosti:

- elektronický podpis,
- zaručený elektronický podpis a
- kvalifikovaný elektronický podpis.

Tyto jednotlivé typy elektronického podpisu se od sebe odlišují především rozdílnými požadavky na jejich vytvoření a také jejich právní sílou.

4.1 Elektronický podpis

Jako *elektronický podpis* (bez jakéhokoli přívlastku) můžeme označit cokoliv, co je použito jako podpis dané osoby a co má elektronickou podobu. Z technického hlediska se tak může jednat např. o pouhé napsání našeho jména na konec emailové zprávy. Je tady zřejmé, že není zaručeno jednoznačné spojení s podepisující osobou.

4.2 Zaručený elektronický podpis

Zaručený elektronický podpis musí být jednoznačně spojen s podepisující osobou a musí umožňovat její identifikaci. Musí být také vytvořen pomocí dat pro vytváření elektronických podpisů. Z toho nám plyne, že zaručený elektronický podpis musí být vytvořen pomocí certifikátu, avšak na tento certifikát nejsou kladeny žádné požadavky. Nemusí se jednat o certifikát vydaný kvalifikovaným poskytovatelem. Může se tak jednat o jakýkoliv certifikát, který si můžeme vystavit i svépomocí.

4.3 Kvalifikovaný elektronický podpis

Posledním typem je *kvalifikovaný elektronický podpis*. Jedná se ve své podstatě o zaručený elektronický podpis, pouze vytvořený kvalifikovaným prostředkem pro vytváření elektronických podpisů a je založen na kvalifikovaném certifikátu pro elektronické podpisy. Kvalifikovaným certifikátem se rozumí certifikát, který byl vydán

kvalifikovaným poskytovatelem služeb vytvářejících důvěru. To je takový poskytovatel, kterému orgán dohledu udělil status kvalifikovaného poskytovatele. Takové kvalifikované poskytovatele máme v současné době v České republice tři:

- První certifikační autorita, a. s.,
- APCS eIdentity a. s. a
- certifikační autorita PostSignum provozovaná státním podnikem Česká pošta.

Z technického hlediska není mezi zaručeným a kvalifikovaným elektronickým podpisem žádný rozdíl. Mechanismus podepisování probíhá vždy totožně a to tak, jak popisujeme v kapitole 2.

4.4 Uznávaný elektronický podpis

Označení *uznávaný elektronický podpis* je spíše národní specialita České republiky, kterou unijní legislativa nezná (proto také není uveden v nařízení eIDAS). Dříve byl uznávaný elektronický podpis takový podpis, který nevyžadoval bezpečný prostředek (a byl založen na kvalifikovaném certifikátu). Dnes je tento pojem „legislativní zkratka“ pro dva různé druhy elektronických podpisů:

- pro kvalifikovaný podpis – takový, co vyžaduje kvalifikovaný prostředek,
- pro prosazenou výjimku – elektronický podpis, který nevyžaduje kvalifikovaný prostředek, ale jen kvalifikovaný certifikát.

Důvodem pro zavedení této legislativní zkratky je zřejmě to, aby se nemusely novelizovat úplně všechny dosavadní zákony, které původní termín *uznávaný elektronický podpis* používají. [26]

Definice: Elektronickým podpisem se rozumí data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání. [22]

5 ELEKTRONICKÁ PEČEŤ

Nařízení eIDAS nám přináší poměrně významnou změnu a tou je nahrazení stávajících elektronických značek elektronickými pečetěmi. Elektronické značky byly zavedeny jako elektronický podpis generovaný automatem (strojem) bez právní presumpce seznámení se s obsahem [26]. Příkladem takového použití může být generování výpisů z elektronických rejstříků, což se děje bez účasti člověka.

Nyní eIDAS již neřeší skutečnost, zda se podepisuje strojově nebo podepisuje člověk. Stejně jako se u elektronických pečetí i u elektronických podpisů nově nepracuje s presumpcí seznámení se s obsahem. Elektronická pečeť se vydává jen právnickým osobám avšak s důležitou skutečností a to, že právnická osoba nemůže svou elektronickou pečetí opatřit cokoliv, ale jen to, co pochází od ní (čeho je původcem) [26].

Z hlediska technické proveditelnosti je proces pečetění elektronickou pečetí totožný s podepisováním elektronickým podpisem. Děje se tak stejným mechanismem, jako popisujeme v kapitole 2.

Definice: Elektronickou pečetí se rozumí data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu. [22]

6 ELEKTRONICKÉ ČASOVÉ RAZÍTKO

Jak je již z názvu zřejmé, elektronické časové razítko slouží k označování elektronických dat a dokazuje nám, kdy data existovala a v jakém tvaru. Souvisí totiž velmi úzce s elektronickým podpisem a to tak, že nám udává zaručený čas, kdy byla daná elektronická data podepsaná.

Pokud data elektronicky podepisujeme, jako čas podpisu se použije systémový čas počítače. Na ten se nedá příliš spoléhat, protože si jej může uživatel dle vlastní vůle změnit jak do minulosti, tak i do budoucnosti. Samozřejmě tak nemusí činit, ale nemáme žádnou jistotu. Jistotu správného času a datumu nám poskytne třetí, nezávislá, strana, která bude mít správně seřízený datum a čas a nebude moci s nimi svévolně manipulovat. Maximální záruku korektního času nám poskytnou až *kvalifikovaná* elektronická časová razítka. Tedy taková, která nám vydala *kvalifikovaná*, státem uznávaná, třetí strana.

Tento důvěryhodný údaj se k datům připojí ve formě elektronického časového razítka. Může existovat jako zcela samostatný objekt, ale častěji se s ním setkáme v podobě tzv. *podpisového časového razítka* [5]. Tedy jako něčeho, co je vloženo přímo do zaručeného či uznávaného elektronického podpisu na elektronických datech či zprávě [5]. Je důležité si vyjasnit, že elektronické časové razítko nám neříká, kdy byla data opatřená elektronickým podpisem, ale pouze k jakému okamžiku daná data již existovala (tedy data již opatřená elektronickým podpisem).

Postup opatřování elektronických dat elektronickým časovým razítkem je z technického pohledu následující; z požadovaných dat vytvoříme pomocí hashovací funkce hash a ten pošleme certifikační autoritě s žádostí o elektronické časové razítko. Ta na konec hashe přidá svůj (důvěryhodný) údaj o datu a času. Takto „obohacený“ hash podepíše svým soukromým klíčem a pošle nám jej nazpět.

Definice: Elektronickým časovým razítkem se rozumí data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku. [22]

7 SLUŽBA ELEKTRONICKÉHO DOPORUČENÉHO DORUČOVÁNÍ

V oblasti služeb elektronického doporučeného doručování je eIDAS velmi stručný. Řeší především právní účinky této služby. Z technického hlediska nás zajímají uvedené požadavky kladené na *kvalifikované* služby elektronického doporučeného doručování. Z nich, jako nejdůležitější, uveďme, že odesílání a přijímání dat je zabezpečeno prostřednictvím zaručeného elektronického podpisu nebo zaručené elektronické pečeti kvalifikovaného poskytovatele tak, aby byla vyloučena možnost nezjistitelné změny dat. Datum a čas odeslání, přijetí a případná změna dat jsou označeny prostřednictvím kvalifikovaného elektronického časového razítka. [22]

Definice: Službou elektronického doporučeného doručování se dle nařízení eIDAS rozumí: služba, která umožňuje přenášet data mezi třetími osobami elektronickými prostředky a poskytuje důkazy týkající se nakládání s přenášenými daty, včetně dokladu o odeslání a přijetí dat, a která chrání přenášená data před rizikem ztráty, odcizení, poškození nebo neoprávněných změn.

8 AUTENTIZACE INTERNETOVÝCH STRÁNEK

Nařízení eIDAS míří i na SSL/TLS certifikáty pro autentizaci webových stránek, která představuje jednu ze služeb vytvářejících důvěru. Nařízení je v tomto ohledu značně strohé a autentizaci internetových stránek upravuje pouze ve dvou odstavcích. Ani tuzemská úprava v zákonu [33] není zrovna rozsáhlá. Odvolává se však na *Přílohu IV* nařízení eIDAS, kde jsou uvedeny všechny položky, které musí kvalifikované certifikáty pro autentizaci internetových stránek obsahovat.

Docela zásadní zádrhel však nastává v povinnosti používání SSL/TLS certifikátů veřejnou správou. Zatímco v případě elektronických podpisů eIDAS stanovuje povinnost využívat tuto službu ke komunikaci s veřejnou správou [9], u serverových certifikátů tomu tak není. Ostatně nám tuto skutečnost potvrzuje i důvodová zpráva: *Poskytování a využívání služeb autentizace internetových stránek je zcela dobrovolné* [22].

Další zbrzděním v masivním nasazením kvalifikovaných certifikátů pro autentizaci internetových stránek vydávaných kvalifikovaným poskytovatelem je fakt, že většina serverů využívá certifikáty vydávané americkými společnostmi jako je např. GeoTrust, Thawte či Symantec. Děje se tak především z důvodu, že hlavní vývojáři internetových prohlížečů se neřídí statusem kvalifikovaného poskytovatele dle evropských pravidel, ale využívají vlastní seznamy důvěryhodných certifikátů. Důkazem je asi dva roky starý případ výměny serverových certifikátů daňového portálu [34].

8.1 SSL/TLS protokol

První podpory se Secure Sockets Layer (SSL) protokol dočkal v roce 1994 díky webovému prohlížeči Mosaic. Svého následovníka v podobě Transport Layer Security (TLS) protokolu se dočkal v roce 1996. V síťovém modelu TCP/IP pracuje tento bezpečnostní protokol mezi *aplikační* a *transportní* vrstvou.

Při přístupu uživatele na webovou stránku, pošle koncová stanice na server požadavek na zabezpečené připojení. Ten, pokud umožňuje zabezpečenou komunikaci, odešle koncové stanici svůj SSL certifikát a ta může navázat zabezpečenou komunikaci mezi klientem a webovou stránkou.

Definice: Nařízení eIDAS nám autentizaci internetových stránek přímo nespecifikuje, nalezneme však definici certifikátu pro autentizaci internetových stránek: potvrzení, které umožňuje autentizovat internetové stránky a spojuje je s fyzickou nebo právnickou osobou, jíž je certifikát vydán.

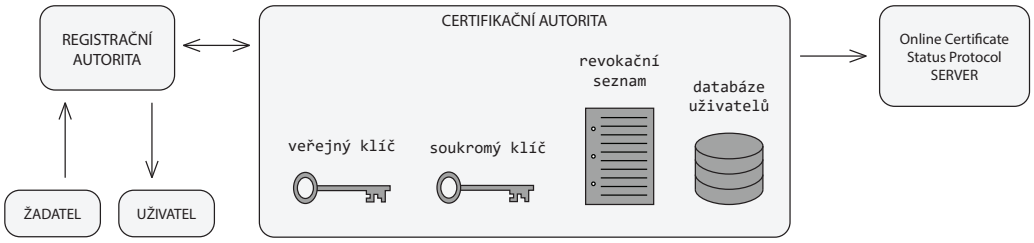
9 NÁVRH ŘEŠENÍ PRO DEMONSTRACI SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Pro demonstraci funkčnosti služeb vytvářejících důvěru využijeme některého z volně dostupného open-source řešení certifikační autority. Takových řešení se na Internetu nachází hned několik. My si některé z nich vybereme, popíšeme si je, včetně jejich výhod a nevýhod, a na základě tohoto přehledu vybereme to nejvhodnější pro naše potřeby.

9.1 Certifikační autorita

Je to třetí strana, která se neúčastní elektronické transakce mezi dvěma stranami. Certifikační autorita vydává certifikáty koncovým entitám, při elektronické transakci ověřuje platnost těchto certifikátu a v případě potřeby daný certifikát zneplatní. Certifikační autorita může být pouhá aplikace (jako v našem případě) nebo i velká společnost čítající desítky zaměstnanců. Je do maximální možné míry nezávislá a nekompromitovatelná [6].

Certifikační autorita se může jevit, jako *nějaký* velký systém, který funguje. Ve skutečnosti se však certifikační autorita skládá z několika vzájemně vhodně propojených komponent [32]. Obr. 9.1 znázorňuje, z kterých částí se certifikační autorita skládá a jak tyto části mezi sebou komunikují. Velmi také záleží, jaké služby daná certifikační autorita poskytuje, od této skutečnosti se odvíjí i její reální struktura.



Obr. 9.1: Základní struktura certifikační autority

9.2 Let's Encrypt

Jde o certifikační autoritu, která byla spuštěna 12. dubna 2016 [20]. Bezplatně poskytuje certifikáty X.509 pro šifrovaný TLS přenos prostřednictvím automatizovaného procesu, jehož cílem je eliminovat dříve složitý proces manuálního vytvoření, validace, podepsání, instalace a obnovení certifikátů pro zabezpečené webové stránky.

Let's Encrypt však nabízí pouze certifikáty pro autentizaci webových stránek. Je to sice jedna ze služeb vytvářejících důvěru, ale také jediná se kterou je tato certifikační autorita schopná pracovat. Z tohoto hlediska je pro nás tento systém nevyhovující.

9.3 EJBCA

EJBCA (Enterprise Java Beans Certificate Authority) je volně šiřitelná certifikační autorita pro infrastrukturu veřejných klíčů. Má více než 16letou historii (první vydání 5. prosince 2001) a je stále aktuální (poslední stabilní verze je z 8. listopadu 2017). Tento systém je vyvíjen v Javě EE a je navržen tak, aby byl nezávislý na platformě. Podporuje také použití Hardware Security Module (HSM), který poskytuje další zabezpečení. EJBCA se vyznačuje několika výhodami [15]. Na ukázku si uveďme:

- paralelní běh několika certifikačních autorit v rámci jedné instalace,
- využití Certificate Revocation List (CRL) nebo protokolu Online Certificate Status Protocol (OCSP) pro online zjištění stavu certifikátu,
- s ohledem na integraci podporuje většinu standardních protokolů (např. Certificate Management Protocol (CMP), Simple Certificate Enrollment Protocol (SCEP)) a
- vysoký výkon.

9.4 OpenXPKI

Projekt začal v roce 2005 a je stále aktuální [25]. Je udržován aktualizačními balíčky, které jsou vydávány několikrát ročně. Projekt OpenXPKI je zaměřen na vývoj open-source software Public Key Infrastructure (PKI) pro podnikové účely. Je vyvíjen v programovacím jazyce Perl a je možné jej implementovat na UNIX operační systémy. OpenXKPI se vyznačuje několika výhodami [19]. Uveďme třeba:

- paralelní běh několika certifikačních autorit v rámci jedné instalace,
- webové uživatelské rozhraní a
- podpora HSM pro kryptografické operace.

9.5 OpenCA Research Labs

Snahou tohoto projektu pravděpodobně bylo vyvinout robustní a plnohodnotnou open-source certifikační autoritu, která je založena na open-source projektech; OpenLDAP, OpenSSL a Apache. Poslední stabilní verze byla však vydána 10. května 2014

a na serveru GitHub mají soubory staré několik let, tudíž se pravděpodobně již nejedná o aktuální a stále podporovaný systém.

9.6 GnoMint

Je to bezplatný nástroj na správu certifikačních autorit. Jeho hlavním cílem je snadná a přehledná ovladatelnost. Díky jeho jednoduchému grafickému rozhraní tomu tak opravdu je. V případě potřeby zpracování většího množství požadavků je možné použít dávkové příkazy skrze příkazový řádek. Umožňuje vytváření certifikačních autorit, vydávání X.509 digitálních certifikátů včetně seznamu zneplatněných certifikátů CRL. Při svém vzniku (asi před 11lety) tento projekt reagoval na díru na trhu, kdy chyběl nástroj na rychlé a účinné vydávání certifikátů včetně příslušných služeb, což svou jednoduchostí splňoval. Projekt můžeme stále považovat za aktivní, poslední verze byla vydána v březnu 2016.

10 NÁVRH LABORATORNÍ ÚLOHY

10.1 Cíl úlohy

Seznámit se s principem činnosti certifikační autority. Pochopit princip vydávání a zneplatňování certifikátů.

10.2 Úkoly

1. Provést instalaci operačního systému Linux ve virtualizačním nástroji.
2. Nainstalovat program gnoMint.
3. Vytvořit self-signed certifikační autoritu.
4. Podat více než jednu žádost o vydání certifikátu.
5. Zneplatnit vydaný certifikát.
6. Porovnat rozdíly mezi certifikáty.

10.3 Teoretický úvod

10.3.1 Certifikační autorita

GnoMint je free software nástroj pro správu certifikačních autorit využívajících certifikáty X.509. Jeho cílem je nabídnout uživateli přehledné a snadno použitelné rozhraní pro vytváření certifikačních autorit a souvisejících prvků, včetně digitálních certifikátů X.509, žádostí o podepsání certifikátů (CRS) a seznamu zneplatněných certifikátů (CRL). Více se o tomto projektu, včetně kompletní dokumentace, dozvíme na: `http://gnomint.sourceforge.net/`.

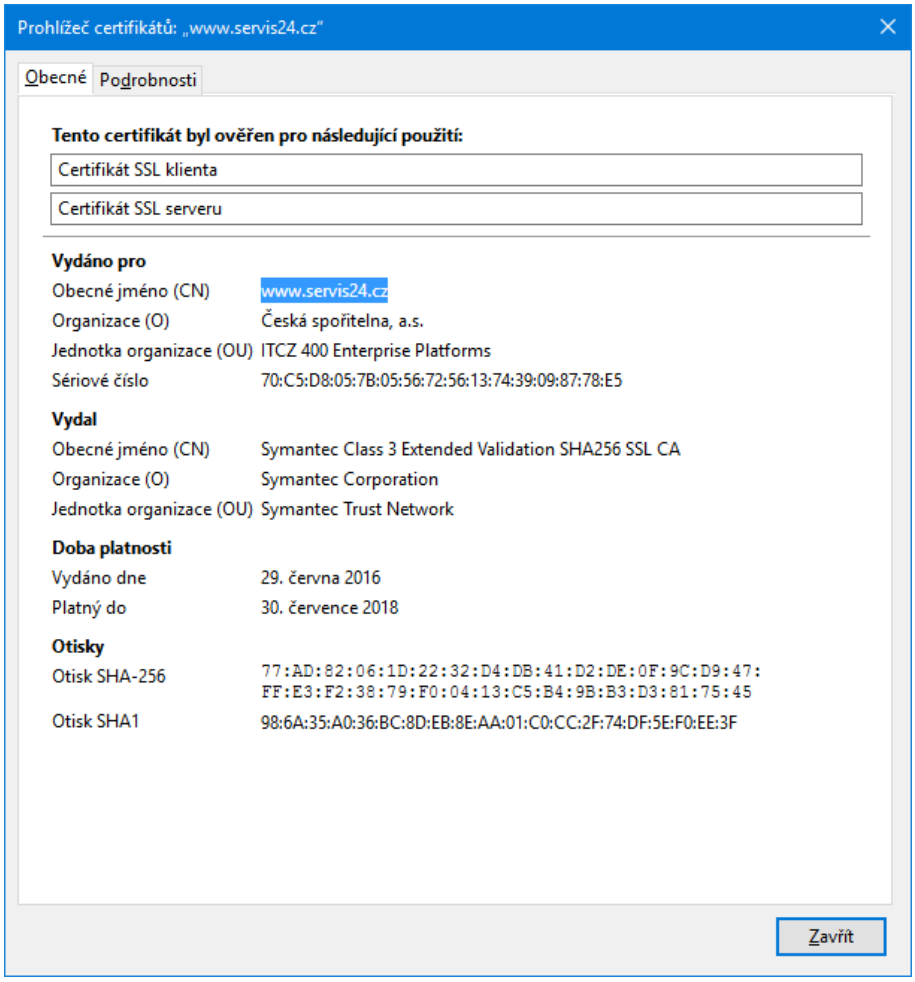
10.3.2 Certifikát

Digitální certifikát je datová struktura obsahující především veřejný klíč vlastníka certifikátu (dále obsahuje např. informace o vlastníkovi a vlastnosti související s certifikátem). Nejdůležitějším úkolem certifikátu je ověření identity vlastníka veřejného klíče. Tímto zabraňujeme podvržení veřejného klíče. [16]

Koncový uživatel si může certifikát zobrazit a ověřit vydávající certifikační autoritu anebo dobu platnosti. Pro ukázku si zvolíme certifikát České spořitelny. Na obr. 10.1 vidíme obecné informace o certifikátu zobrazené ve webovém prohlížeči Mozilla Firefox. Pokud se přepneme na kartu *Podrobnosti*, uvidíme všechny údaje certifikátu. Pro získání základního přehledu si uveďme:

- verze certifikátu,

- sériové číslo,
- algoritmus podpisu certifikátu,
- vydavatel,
- platnost od,
- platnost do,
- **subjekt**,
- algoritmus veřejného klíče subjektu,
- **veřejný klíč subjektu**,
- **použití klíče certifikátu** (k jakým úkonům můžeme daný certifikát využít),
- distribuční body CRL atd.

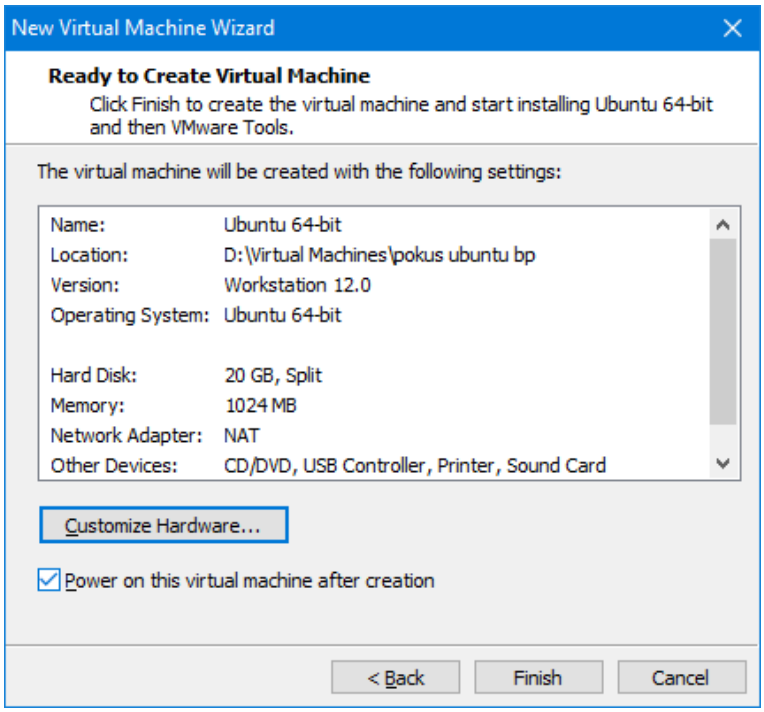


Obr. 10.1: Certifikát internetového bankovnictví České spořitelny

10.4 Pracovní postup

1. Provést instalaci operačního systému Linux ve virtualizačním nástroji: Začneme instalací některé z Linuxových distribucí v libovolném virtualizačním nástroji. Pro názornou demonstraci jsme zvolili distribuci Ubuntu a program VMware. Z adresy: `https://www.ubuntu.cz/` si stáhneme obraz instalačního disku 64bit verze Ubuntu.

Spustíme si VMware a vytvoříme si nový virtuální stroj. Zvolíme: *Player* → *File* → *New Virtual Machine...* nebo použijeme klávesovou zkratku Ctrl+N. V dialogovém okně *New Virtual Machine Wizard* zvolíme druhou možnost *Installer disc image file (iso)* a kliknutím na tlačítko *Browse...* vybereme stažený obraz instalačního disku. Uživatelské jméno a heslo volíme rozumně a snadno zapamatovatelné, nejlépe *User name:* `student` a *Password:* `student`. V reálném nasazení volíme samozřejmě hesla silnější a bezpečnější. V dialogovém okně (obr. 10.2) dokončíme nastavení virtuálního stroje.



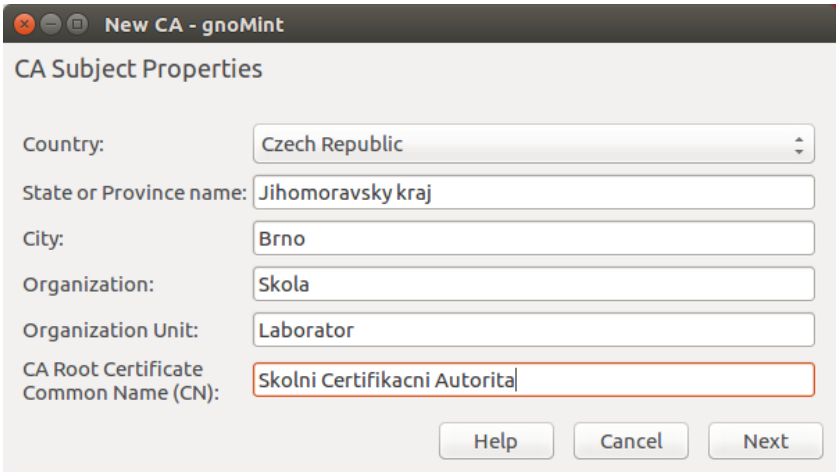
Obr. 10.2: New Virtual Machine Wizard

Vybereme právě vytvořený virtuální stroj a stiskem *Play virtual machine* jej spustíme. Počkáme na dokončení instalace operačního systému a přihlásíme se námi zadanými přihlašovacími údaji.

2. Nainstalovat program gnoMint: V prostředí Ubuntu si spustíme terminál (můžeme použít klávesovou zkratku Ctrl+Alt+T), příkazem: `sudo apt-get update`

aktualizujeme seznamy balíčků a příkazem: `sudo apt-get install gnomint` provedeme instalaci programu gnoMint.

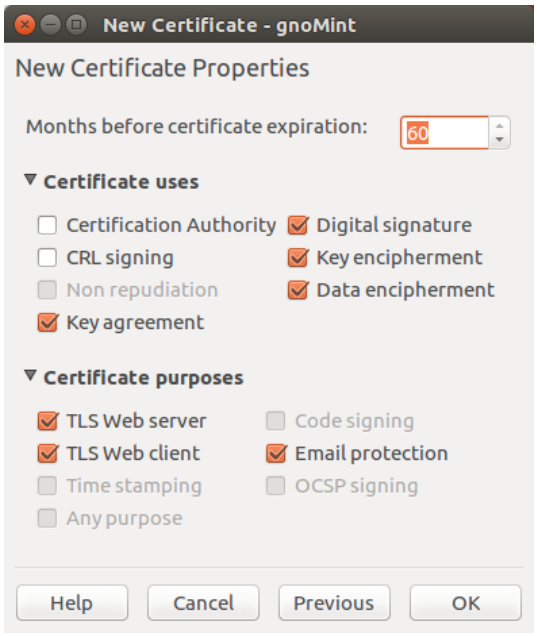
3. Vytvořit self-signed certifikační autoritu: Seznámíme se s uživatelským prostředím a nejprve si vytvoříme databázi, ve které budou uloženy certifikační autority a samotné certifikáty, kliknutím na *Certificates* → *New certificate database* a následně i self-signed certifikační autoritu. Zvolíme: *Certificates* → *Add* → *Add self-signed CA* a zobrazí se nám dialogové okno (obr. 10.3), které vyplníme vlastními údaji. Po kliknutí na *Next* zvolíme především typ soukromého klíče a jeho (dostatečně bezpečnou) délku.



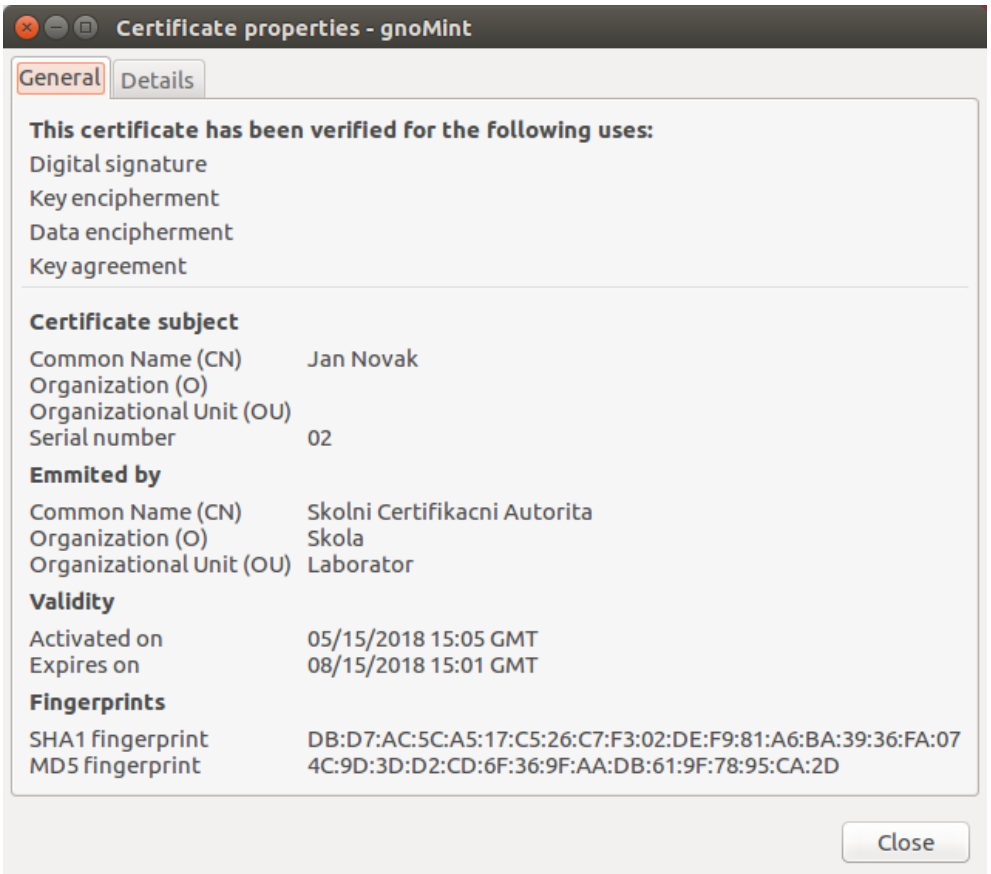
Obr. 10.3: CA Subject Properties

4. Podat více než jednu žádost o vydání certifikátu: Nyní si podáme žádost o vydání certifikátu. Klikneme na: *Certificates* → *Add* → *Add Certificate Request* a dialogové okno vyplníme údaji žadatele o certifikát. Volbou: *Certificates* → *Sign* získáme možnost podepsat tento certifikát certifikační autoritou. V případě, že program bude spravovat více certifikačních autorit máme pochopitelně na výběr, která certifikát podepíše. Dále (obr. 10.4) máme možnost určit, k jakému použití a k jakým účelům certifikát vydáváme. Kliknutím pravým tlačítkem myši a volbou *Properties* si zobrazíme souhrnné (obr. 10.5) i detailní vlastnosti certifikátu.

Stejným způsobem podáme několik dalších žádostí o certifikát a následně je podepíšeme. Při podávání žádostí volme různý typ soukromého klíče i jeho délku. Můžeme si vytvořit i druhou certifikační autoritu a pro podpis žádostí využívat nahodile obou certifikačních autorit. Uvidíme, jak program graficky rozlišuje ten který certifikát byl danou certifikační autoritou podepsaný. Při schvalování jednotlivých žádostí o certifikát využívejme možnosti volby jeho účelu a použití.



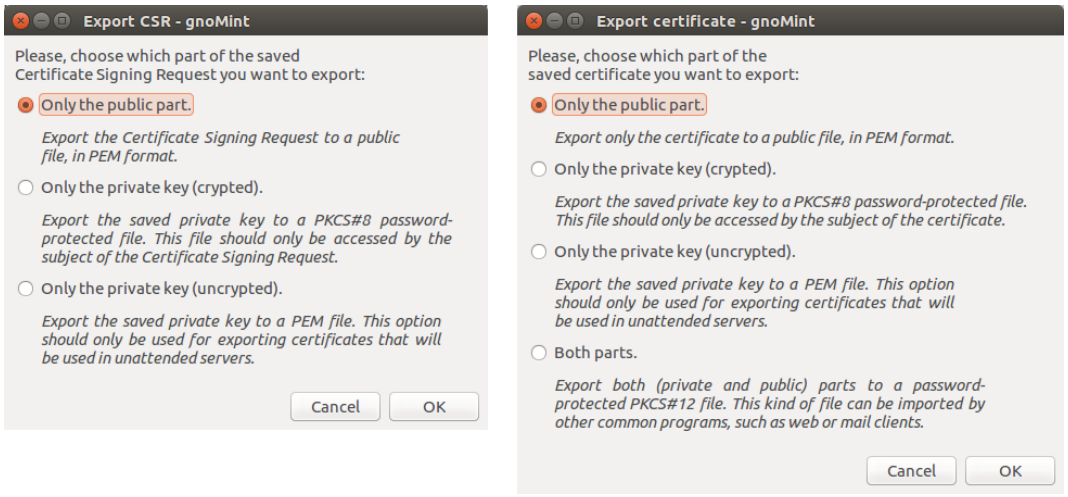
Obr. 10.4: New Certificate Properties



Obr. 10.5: Certificate properties

Kliknutím pravým tlačítkem myši na certifikát a volbou *Export* si můžeme soukromou anebo veřejnou část exportovat.

Pokud možnost *Export* zvolíme ještě před podepsáním žádosti o certifikát, všimněme si, že můžeme exportovat pouze soukromý klíč. Z toho je zřejmé, že soukromý klíč žadatele se generuje při podávání jeho žádosti. Naopak dialogové okno *Export* již podepsaného certifikátu nám nabídne export i veřejné části certifikátu (viz obr. 10.6).



Obr. 10.6: Export

5. Zneplatnit vydaný certifikát: Volbou *Revoke* a potvrzením *Yes* s okamžitou platností zneplatníme certifikát. Pokud certifikát již nevidíme v seznamu certifikátů, zaškrtneme možnost *View* → *Revoked Certificates* a revokované certifikáty se zobrazí přeškrtnuté.

Možností *Certificates* → *Generate CRL* si můžeme vygenerovat seznam zneplatněných certifikátů. Pokud máme problém s jeho otevřením v systému Linux, přeneseme si jej do prostředí Windows a soubor s příponou `*.crl` otevřeme.

Pokud seznam zneplatněných certifikátů dostaneme a chceme jej implementovat do naší certifikační autority, využijeme k tomu možnost *Certificates* → *Import*.

6. Porovnat rozdíly mezi certifikáty: Nyní si podrobně pročtěme detaily jednotlivých certifikátů a porovnejme v kterých údajích se liší. Všimněme si především typu a délky soukromého klíče a jeho použití.

10.5 Závěr

- Jaké jsou nedůležitější položky certifikátu?
- Jak můžeme certifikát zneplatnit?

- Jaké možnosti může certifikační autorita volit při podepisování certifikátu?

11 ZÁVĚR

Cíle bakalářské práce uvedení definice a vysvětlení pojmů jsme dosáhli v první a pak ve čtvrté až osmé kapitole. Cíle realizace systému, který bude demonstrovat funkčnost služeb vytvářejících důvěru jsme dosáhli v poslední, tj. desáté, kapitole.

V úvodní kapitole bakalářské práce jsme si stručně rozebrali nařízení eIDAS a uvedli jsme důvody jeho přijetí. V přehledné tabulce jsme pro názornost porovnali definice jednotlivých pojmů, související se službami vytvářející důvěru, dle nové i staré legislativy. Co se týče technického řešení služeb vytvářejících důvěru zjistili jsme, že v tomto ohledu je nařízení eIDAS nekonkrétní, a tak se můžeme řídit technickými normami, které však nejsou závazné.

Ve druhé kapitole jsme si popsali digitální podpis jako kryptografický systém, uvedli jsme výhody, které nám přináší a s pomocí názorného schematu jsme si popsali mechanismus podepisování a následného ověření digitálního podpisu a integrity doručených dat.

Ve třetí kapitole jsme si objasnili problematiku digitálních certifikátů a jejich význam. Uvedli jsme si také, jaké druhy certifikátů rozlišuje eIDAS včetně odkazů, kde nalezneme, jaké údaje musí ten který certifikát obsahovat.

V následujících pěti kapitolách jsme postupně rozebrali jednotlivé služby vytvářející důvěru, jak je definuje nařízení eIDAS. U každé služby je její přesná definice dle tohoto nařízení a případný popis funkčnosti.

Devátá kapitola pojednává o možných řešeních demonstrující funkčnost služeb vytvářejících důvěru. Uvedli jsme zde přehled open-source řešení certifikačních autorit. Na Internetu se nachází mnoho takových řešení, avšak některá jsou neaktuální, zastaralá a jejich vývoj byl ukončen. Nás zajímají pouze ta aktuální a snadno implementovatelná. Dle našeho přehledu a zjištěných informací se jako nejvhodnější řešení nabízí gnoMint. Řešení gnoMint je program s přehledným uživatelským rozhraním, který současně nabízí i možnost využití příkazového řádku pro dávkové příkazy.

Poslední kapitola je návrhem laboratorní úlohy. Kladli jsme důraz na srozumitelnost postupu a na důkladné seznámení se s principem činnosti certifikační autority.

LITERATURA

[1] *About Let's Encrypt* [online]. [cit. 1. 12. 2017]. Dostupné z URL: <https://letsencrypt.org/about/>

[2] KROPÁČOVÁ, A.: *Bezpečnost elektronických dat a elektronické komunikace* [online]. 2011, poslední aktualizace 14. 11. 2011 [cit. 17. 11. 2017]. Dostupné z URL: <http://webserver.ics.muni.cz/bulletin/articles/522.html>

[3] FELIX, O.: *Cíle a oblasti regulace eIDAS* [online]. 2016, poslední aktualizace 16. 6. 2016 [cit. 18. 10. 2017]. Dostupné z URL: <https://www.youtube.com/watch?v=loLkgFpzVUk&t=4m9s>

[4] *Co je Digitální certifikát* [online]. [cit. 5. 11. 2017]. Dostupné z URL: <https://www.ssls.cz/slovnik/digitalni-certifikat.html>

[5] PETERKA, J.: *Časové razítko, aneb: kdy vznikl elektronický podpis?* [online]. [cit. 29. 9. 2017]. Dostupné z URL: <http://www.earchiv.cz/b12/b0323001.php3>

[6] LEPA, O.: *Digitální certifikáty a certifikační autority* [online]. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2014. 91 s. Vedoucí diplomové práce Ing. Vlastimil Člupek [cit. 5. 11. 2017]. Dostupné z URL: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=84546>

[7] ZEMAN, V.: *Digitální podpis, Public Key Infrastructure* [přednáška]. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Aplikovaná kryptografie. [cit. 20. 2. 2018].

[8] BÍLEK, F.: *Důvěra napříč Evropou, nařízení eIDAS* [online]. 2016, poslední aktualizace 31. 5. 2016 [cit. 1. 10. 2017]. Dostupné z URL: <https://www.youtube.com/watch?v=kreoIj4Kf4k&t=2m26s>

[9] PRŮŠA, J.: *eIDAS: Jak evropské nařízení (ne)ovlivní webové certifikáty?* [online]. [cit. 7. 11. 2017]. Dostupné z URL: <https://www.lupa.cz/clanky/eidas-jak-evropske-narizeni-ne-ovlivni-webove-certifikaty/>

[10] *Elektronický podpis a jeho využití* [online]. [cit. 8. 3. 2018]. Dostupné z URL: <http://www.businessinfo.cz/cs/clanky/elektronicky-podpis-a-jeho-vyuziti-7476.html>

[11] SMEJKAL, V.; KODL, J.; UŘIČAŘ, M.: *Elektronický podpis podle nařízení eIDAS.* Revue pro právo a technologie. [online]. 2015, č. 11, s. 189. [cit.

27. 3. 2018]. Dostupné z URL: <https://journals.muni.cz/revue/article/view/3586>

[12] *E-mailová komunikace s Miroslavem Trávníčkem.* 18. 12. 2017.

[13] *ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites* [online]. Valbonne: European Telecommunications Standards Institute, 2014. 37 s. [cit. 29. 9. 2017]. Dostupné z URL: <http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf>

[14] MARÍN, D.: *Features* [online]. [cit. 30. 11. 2017]. Dostupné z URL: <http://gnomint.sourceforge.net/?q=node/3>

[15] *Features* [online]. [cit. 30. 11. 2017]. Dostupné z URL: <https://www.ejbca.org/features.html>

[16] LOUTOCKÝ, T.: *Hardwarové kryptografické moduly pro zabezpečení LAN* [online]. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2008. 88 s. Vedoucí diplomové práce doc. Ing. Václav Zeman, Ph.D. [cit. 14. 3. 2018]. Dostupné z URL: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=5859>

[17] *How It Works* [online]. [cit. 30. 11. 2017]. Dostupné z URL: <https://letsencrypt.org/how-it-works/>

[18] *Jsou české technické normy v ČR závazné? A jak je tomu ve světě?* [online]. [cit. 13. 5. 2018]. Dostupné z URL: <http://www.unmz.cz/urad/prehlrub.asp?cd=53&typ=c>

[19] *Key features* [online]. [cit. 30. 11. 2017]. Dostupné z URL: <http://openxpki.readthedocs.io/en/latest/introduction.html#key-features>

[20] CIMPANU, C.: *Let's Encrypt Launched Today, Currently Protects 3.8 Million Domains* [online]. [cit. 30. 11. 2017]. Dostupné z URL: <http://news.softpedia.com/news/let-s-encrypt-launched-today-currently-protects-3-8-million-domains-502857.shtml>

[21] *Nařízení, směrnice a další právní akty* [online]. [cit. 13. 12. 2017]. Dostupné z URL: <https://europa.eu/european-union/eu-law/legal-acts_cs>

[22] *Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES* [online]. Brusel: Úřední věstník Evropské unie, 2014. [cit. 30. 9. 2017]. Dostupné z URL: <http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014R0910&qid=1513069506914&from=CS>

[23] PIFFL, R.; FELIX, O.: *Nařízení eIDAS – Cíle, nástroje, důsledky* [online]. [Praha]: Ministerstvo vnitra České republiky; 2016, poslední aktualizace 15. 6. 2016 [cit. 2. 10. 2017]. Dostupné z URL: <http://www.mvcr.cz/soubor/1-eidas-narizeni-eidas-cile-nastroje-dusledky.aspx>

[24] *PKI Architectures* [online]. [cit. 30. 11. 2017]. Dostupné z URL: <https://www.ejbca.org/docs/architecture.html>

[25] *Project History* [online]. [cit. 30. 11. 2017]. Dostupné z URL: <http://www.openxpki.org/about.html>

[26] PETERKA, J.: *První půlrok s nařízením eIDAS: přichází elektronické pečeti* [online]. [cit. 5. 10. 2017]. Dostupné z URL: <https://www.lupa.cz/clanky/prvni-pulrok-s-narizenim-eidas-prichazi-elektronicke-peceti/>

[27] STUPKA, V. *Rozhovor s přednášejícím kyberkriminality.* Brno 15. 3. 2018.

[28] HREBENAR, J.: *SSL a TLS: Úvod do SSL a TLS* [online]. [cit. 18. 10. 2017]. Dostupné z URL: <http://programovani.blog.zive.cz/2010/11/ssl-a-tls-uvod-do-ssl-a-tls/>

[29] OLENSKI, J.: *SSL vs. TLS - What's the Difference?* [online]. [cit. 18. 10. 2017]. Dostupné z URL: <https://www.globalsign.com/en/blog/ssl-vs-tls-difference/>

[30] TŮMA, J.: *Standardy bezpečnosti IT* [online]. [cit. 13. 5. 2018]. Dostupné z URL: <http://www.karlin.mff.cuni.cz/~tuma/ciphers/1_Uvod.pdf>

[31] SVOBODA, P.: *Úvod do evropského práva.* 4. vydání. Praha: C.H. Beck, 2011. ISBN 978-807-4003-349.

[32] DOSTÁLEK, L.: *Velký průvodce protokoly TCP/IP: bezpečnost* [online]. [cit. 13. 12. 2017]. Dostupné z URL: <http://download.matus.in/it/VelkypruvodceprotokolyTCP-IP-bezpecnost/>

[33] *Zákon č. 297/2016 Sb. Zákon o službách vytvářejících důvěru pro elektronické transakce.* s. 4466–4504. Sbírka zákonů České republiky, 2016. ISSN 1211-1244.

[34] *Změna vydavatele komerčních serverových certifikátů (SSL certifikátů) aplikací Daňového portálu* [online]. [cit. 6. 12. 2017]. Dostupné z URL: <http://www.financnisprava.cz/cs/dane-elektronicky/novinky/2015/zmena-vydavatele-certifikatu-ssl-aplikaci-danoveho-portalu-6165>

SEZNAM SYMBOLŮ, ZKRATEK A POJMŮ

CA	Certifikační autorita
CMP	Certificate Management Protocol
CRL	Certificate Revocation List
DSA	Digital Signature Algorithm
eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
EU	Evropská unie
HSM	Hardware Security Module
Nařízení	Nařízení EU je právním aktem Evropské unie, který platí v celém svém rozsahu v celé EU [21].
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, Adleman
SCEP	Simple Certificate Enrollment Protocol
Směrnice	Směrnice EU je normativním právním aktem Evropské unie. Směrnice je specifický nástroj harmonizace předpisů členských států, především v oblasti, kde má EU jen nevýlučné pravomoci [31].
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
VPN	Virtual Private Network

A OBSAH PŘILOŽENÉHO CD

/ ..... kořenový adresář přiloženého CD
- `eIDAS.pdf` ..... Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
- `xhrbot00_BP.pdf` ..... bakalářská práce