Katedra informatiky
Přírodovědecká fakulta
Univerzita Palackého v Olomouci

# DIPLOMOVÁ PRÁCE

Úložiště důvěryhodných dokumentů založené na normách ETSI – standard AdES

2017

Bc. Petr Freiberg

Vedoucí práce: RNDr. Jan Konečný, Ph.D.

Studijní obor: Informatika, prezenční forma

**Bibliografické údaje**

| | |
|---|---|
| Autor: | Bc. Petr Freiberg |
| Název práce: | Úložiště důvěryhodných dokumentů založené na normách ETSI – standard AdES |
| Typ práce: | diplomová práce |
| Pracoviště: | Katedra informatiky, Přírodovědecká fakulta, Univerzita Palackého v Olomouci |
| Rok obhajoby: | 2017 |
| Studijní obor: | Informatika, prezenční forma |
| Vedoucí práce: | RNDr. Jan Konečný, Ph.D. |
| Počet stran: | 93 |
| Přílohy: | 1 CD |
| Jazyk práce: | český |

**Bibliograhic info**

| | |
|---|---|
| Author: | Bc. Petr Freiberg |
| Title: | Storage of trusted documents based on ETSI standards – AdES standard |
| Thesis type: | master thesis |
| Department: | Department of Computer Science, Faculty of Science, Palacký University Olomouc |
| Year of defense: | 2017 |
| Study field: | Computer Science, full-time form |
| Supervisor: | RNDr. Jan Konečný, Ph.D. |
| Page count: | 93 |
| Supplements: | 1 CD |
| Thesis language: | Czech |

## Anotace

*Standardizace formátů pro bezpečnostní prvky digitálních dat je v posledních letech velmi diskutovaným tématem. Evropský institut pro telekomunikační standardy (ETSI) za tímto účelem vydává specifikace a definice způsobů použití standardu AdES (Advanced Electronic Signature). V diplomové práci popisuji všechny tři referenční formáty elektronického podpisu, které do tohoto standardu patří: XAdES, CAdES a PAdES. Čtenáře postupně seznamuji s důvody, které vedou státy EU k jejich zavádění do praxe. Jednou z hlavních výhod je možnost dlouhodobého ověření platnosti podpisu. Praktické využití představuji na úložišti pro správu důvěryhodných dokumentů, které podporuje všechny tři výše uvedené formáty.*

## Synopsis

*In recent years, the standardization of formats for digital data security has been a highly debated topic. European Telecommunications Standards Institute (ETSI) has issuing specifications and definitions pertaining to the use of Advanced Electronic Signature (AdES). In the thesis, I have described all three reference formats of electronic signature that belong to this standard: XAdES, CAdES and PAdES. My intention is to gradually familiarize readers with the reasons behind the move by EU countries for putting them into practice. One of the key main benefits is the ability of long term validation (LTV) of signatures. Practical use is introduced on a trusted documents management repository, which supports all three above mentioned formats.*

**Klíčová slova:** AdES; XAdES; CAdES; PAdES; důvěryhodný dokument; úložiště důvěryhodných dokumentů; eIDAS; elektronický podpis

**Keywords:** AdES; XAdES; CAdES; PAdES; trusted document; trusted documents repository; eIDAS; electronic signature

Děkuji RNDr. Janu Konečnému, Ph.D. za rady a ochotu při vedení diplomové práce. Svému otci pak za trefné připomínky k jazykové podobě práce, díky kterým se doufám čte stejně dobře jako jím vytvářené titulky k filmům.

*Místopřísežně prohlašuji, že jsem celou práci včetně příloh vypracoval/a samostatně a za použití pouze zdrojů citovaných v textu práce a uvedených v seznamu literatury.*

datum odevzdání práce podpis autora

# Obsah


**1 Úvod** **9**

**2 Struktura práce** **11**

**3 Dokument** **12**
3.1 Definice dokumentu . . . 12
3.2 Listinný a elektronický dokument . . . 12
3.3 Důvěryhodný dokument . . . 13
3.4 Podpis . . . 14
3.4.1 Podpis listinného dokumentu . . . 14
3.4.2 Podpis elektronického dokumentu . . . 14
3.4.3 Ověření vlastnoručního a elektronického podpisu . . . 15
3.5 Ztráta důvěryhodnosti . . . 16
3.6 Výhody a nevýhody listinných a elektronických dokumentů . . . 16

**4 Bezpečnostní prvky digitálních dat** **18**
4.1 Asymetrická kryptografie . . . 18
4.2 Elektronický podpis . . . 18
4.2.1 Záruky elektronického podpisu . . . 19
4.2.2 Tvorba elektronického podpisu . . . 20
4.2.2.1 Hašování . . . 20
4.2.2.2 Kryptografické hašovací funkce . . . 21
4.2.2.3 Kolizní dokumenty . . . 22
4.2.2.4 Zjednodušené schéma . . . 23
4.2.3 Elektronická pečeť . . . 24
4.2.4 Digitální certifikát . . . 24
4.2.5 Certifikační autorita . . . 25
4.2.6 Kvalifikovaný poskytovatel služeb vytvářejících důvěru . . . 26
4.2.7 Trusted Services List (TSL) . . . 26
4.2.8 Kořenové a podřízené certifikační autority . . . 27
4.2.9 Infrastruktura veřejného klíče (PKI) . . . 27
4.2.9.1 Strom důvěry . . . 28
4.2.9.2 Vyjádření důvěry certifikátu . . . 29
4.2.9.3 Certifikační cesta . . . 30
4.2.9.4 Zjednodušené schéma s certifikátem . . . 30
4.2.9.5 Revokace certifikátů . . . 31
4.2.10 Kvalifikované a komerční certifikáty . . . 33
4.3 Časové razítko . . . 34
4.3.1 Tvorba časového razítka . . . 34
4.3.2 Zjednodušené schéma s časovým razítkem . . . 35
4.4 Zastarávání elektronických podpisů . . . 37
4.5 Ověřování elektronických podpisů . . . 38

4.5.1 Kontrola integrity . . . 39
4.5.2 Kontrola platnosti certifikátu . . . 39
4.6 Dlouhodobě ověřitelný elektronický podpis . . . 40
4.7 XML Advanced Electronic Signatures (XAdES) . . . 44
4.7.1 XML Digital Signature (XML-DSig) . . . 44
4.7.1.1 Struktura podpisu . . . 44
4.7.1.2 Formy podpisu . . . 46
4.7.1.3 Tvorba podpisu . . . 46
4.7.1.4 Ověření podpisu . . . 47
4.7.2 Výhody XAdES oproti XML-DSig . . . 48
4.7.3 Kvalifikované vlastnosti a struktura . . . 49
4.7.3.1 Podepsané vlastnosti podpisu . . . 50
4.7.3.2 Podepsané vlastnosti dat . . . 51
4.7.3.3 Nepodepsané vlastnosti podpisu . . . 51
4.7.4 XAdES Baseline Profile . . . 53
4.8 CMS Advanced Electronic Signatures (CAdES) . . . 55
4.8.1 Cryptographic Message Syntax (CMS) . . . 55
4.8.1.1 Struktura podpisu . . . 55
4.8.1.2 Formy podpisu . . . 58
4.8.1.3 Atributy podpisu . . . 58
4.8.1.4 Tvorba podpisu . . . 59
4.8.1.5 Ověření podpisu . . . 59
4.8.2 Výhody CAdES oproti CMS . . . 60
4.8.3 Atributy a struktura . . . 60
4.8.4 CAdES Baseline Profile . . . 61
4.8.5 Srovnání XAdES a CAdES formátu . . . 61
4.9 PDF Advanced Electronic Signatures (PAdES) . . . 63
4.9.1 Portable Document Format (PDF) . . . 63
4.9.1.1 Struktura PDF dokumentu . . . 64
4.9.1.2 Přírůstkové aktualizace . . . 67
4.9.1.3 Struktura podpisu . . . 67
4.9.1.4 Tvorba a ověření podpisu . . . 71
4.9.2 Výhody PAdES oproti podpisům dle ISO 32000-1 . . . 71
4.9.3 Struktura . . . 72
4.9.3.1 Validační data a atributy pro archivní validační data . . . 72
4.9.4 PAdES Baseline Profile . . . 73
4.9.5 XAdES zanořený v PAdES . . . 73
4.10 Ověřování elektronických podpisů standardu AdES . . . 74

**5 Legislativa v ČR a EU** **75**
5.1 Předchozí právní úprava v ČR . . . 75
5.2 Nová právní úprava v ČR (eIDAS) . . . 76
5.3 Přechodové období . . . 76

5.4 Novinky v elektronických podpisech . . . . . 76
5.5 Princip nediskriminace . . . . . 77

**6 Úložiště důvěryhodných dokumentů** **79**
6.1 Proč používat úložiště? . . . . . 79
6.2 Základní vlastnosti úložiště . . . . . 80
6.3 Na jakém formátu úložiště vybudovat? . . . . . 81
6.4 Příjem, čtení a důkazní materiály . . . . . 82
6.5 Smazání dokumentu . . . . . 83
6.6 Pravidelná kontrola . . . . . 84
6.7 Komerční řešení . . . . . 84
6.8 Navazující diplomová práce . . . . . 85

**Závěr** **86**

**Conclusions** **87**

**A Obsah přiloženého CD** **88**

**Seznam použitých zkratek** **89**

**Literatura** **91**

# Seznam obrázků


1 Vlastnoruční podpis John von Neumanna . . . . . 14
2 Podrobné informace o elektronickém podpisu . . . . . 15
3 Zjednodušené schéma tvorby elektronického podpisu . . . . . 23
4 Zjednodušené schéma ověření elektronického podpisu . . . . . 24
5 Znázornění jednoho stromu důvěry . . . . . 28
6 Zjednodušené schéma tvorby elektronického podpisu s certifikátem 31
7 Zjednodušené schéma tvorby elektronického podpisu s časovým razítkem . . . . . 36
8 Základní struktura PDF dokumentu . . . . . 64
9 Přírůstková aktualizace . . . . . 68
10 Bajtový rozsah, ze kterého se počítá haš . . . . . 70
11 Schéma TDPS [23] . . . . . 84

# 1 Úvod

V posledních dvou dekádách dochází v soukromé i státní sféře k masivnímu přesunu na internet a s tím spjaté rozsáhlé digitalizaci. Desítky miliónů obyvatel Evropské unie (EU) i zbytku světa se každý den dostávají do styku s e-komerce, prostřednictvím internetu komunikují s úřady a využívají jej při každodenní práci. Současný trend digitalizace je srovnatelný s průmyslovou revolucí na přelomu 18. a 19. století či automatizací a rozmachem informačních technologií v polovině století dvacátého, protože stejně tak zasahuje do všech oblastí lidské činnosti. Hovoří se proto často o čtvrté průmyslové revoluci.

Ač digitalizace prostupuje celou společností, nemá na všechny její části stejný dopad. Některá odvětví mění rychleji, jiná naopak pomaleji. Velký vliv na to má nejen technologická, ale taktéž legislativní připravenost. V České republice můžeme v posledních letech pozorovat snahu o dohnání poměrně zanedbané situace na poli digitální ekonomiky. Ať už to byla první významnější strategie *Státní politika v elektronických komunikacích – Digitální Česko* z roku 2011 či projekt s názvem *Digitální Česko* z roku 2015. Problémem však zůstává naplňování těchto strategií a vizí, které často zůstávají daleko za původním očekáváním.

Největší vliv na náš současný legislativní stav v této oblasti má tak paradoxně Evropská unie. Nejvýznamnějším počinem posledních let je nařízení Evropského parlamentu a Rady (EU) č. 910/2014 *o elektronické identifikaci a službách vytvářejících důvěru na vnitřním trhu*[1], neboli eIDAS[2]. Publikováno bylo 28. srpna 2014 na Úředním věstníku Evropské unie a v České republice vstoupilo v platnost 1. července 2016. Jeho cílem je sjednotit legislativu napříč státy EU a maximalizovat použitelnost a přenositelnost elektronické identifikace (elektronické prokazování totožnosti) a služeb vytvářejících důvěru pro elektronické transakce na vnitřním trhu EU. To vše s úmyslem, aby elektronická transakce měla stejné právní postavení a byla stejně přenositelná jako transakce prováděná na papíře.

My se budeme zabývat druhou půlkou tohoto nařízení a to *službami vytvářejícími důvěru*. Do poněkud krkolomně pojmenované skupiny *služeb vytvářejících důvěru*[3] spadají mimo jiné služby pro vytváření, ověřování a uchovávání bezpečnostních prvků digitálních dat. Mezi tyto prvky řadíme elektronické podpisy a pečeti, časová razítka a digitální certifikáty.

O důvěryhodnost, autenticitu a přenositelnost jde v eIDAS především. Předchozí unijní směrnice 1999/93/ES *o zásadách Společenství pro elektronické podpisy*, kterou eIDAS nahrazuje, sice upravovala bezpečnostní prvky digitálních dat a s nimi související legislativu, ale neposkytovala ucelený přeshraniční rámec. To z důvodu, že šlo o směrnici a nikoli o nařízení. Což zapříčinilo stav, ve kterém měl

[1] Plným názvem *o elektronické identifikaci a službách vytvářejících důvěru na vnitřním trhu a o zrušení směrnice 1999/93/ES*.

[2] Zkratka vychází ze slov electronic IDentification, Authentication and trust Services.

[3] Jako *službu vytvářející důvěru* pojmenovává eIDAS „něco“, z čeho je důvěra odvozována nebo na čem je naše důvěra zakládána. Příkladem mohou být elektronické podpisy, ze kterých odvozujeme, kým byl elektronický dokument podepsán a na této informaci pak stavíme důvěru v samotný dokument a jeho obsah.

každý stát EU svůj vlastní pohled na tuto oblast a vytvářel vlastní omezení a výjimky. eIDAS, protože jde o nařízení, žádné zásadní modifikace neumožňuje a všechny členské státy díky tomu legislativně sjednocuje. Vzniká tak prostředí, ve kterém může jakýkoliv subjekt z jakéhokoliv členského státu standardizovaným způsobem komunikovat v rámci celé EU.

Důvěryhodnost, autenticita a přenositelnost je velmi důležitá i u právně nezpochybnitelného elektronického dokumentu. Díky stále se zrychlující digitalizaci a přesunu od papírových k elektronickým dokumentům má právě důvěryhodný elektronický dokument stále významnější postavení jak ve státní správě, tak v soukromé sféře. Míra využívání elektronických dokumentů se jednoznačně odvíjí od jasných pravidel, jak s takovými dokumenty zacházet, aby jejich důvěryhodnost zůstala zachována. K tomu, aby byly elektronické dokumenty akceptovány napříč společností, je nutné pravidla dodržovat ve státní správě i soukromé sféře. Dle nařízení eIDAS musí důvěryhodnost elektronického dokumentu primárně vycházet z dokumentu samotného a z jeho atributů. Proto zavádí povinnost používat formát elektronického podpisu v souladu se standardem AdES. Jako referenční formáty určuje XAdES, CAdES a PAdES.

Cílem práce je popsat technologickou a legislativní stránku, na které může být vystavěno úložiště pro dlouhodobou správu důvěryhodných elektronických dokumentů, které využívá výše zmíněné referenční formáty. Dokument, který bude uložen v takovém úložišti, bude pokládán ve všech státech EU za důvěryhodný po neomezeně dlouhou dobu.

# 2 Struktura práce

Kapitola 3 čtenáře seznámí se základními pojmy z domény, kterou se práce zabývá. Mezi ně patří například dokument, podpis, důvěryhodnost a rozdíl mezi dokumentem v listinné a elektronické podobě.

Kapitola 4 čtenáře postupně seznamuje s bezpečnostními prvky digitálních dat a je podstatou diplomové práce. Začíná od základních pojmů jako je asymetrická kryptografie, hašování, elektronický podpis, digitální certifikát a postupně popisuje složitější konstrukce jako je zastarávání elektronických podpisů, dlouhodobé ověřování či formáty XAdES, CAdES a PAdES.

Prvním cílem bylo kapitolu strukturovat způsobem, aby byl čtenář s novými pojmy seznámen postupně a ve chvíli, kdy je bude potřebovat znát. Ne stylem odkazování na budoucí sekce, kde bude pojem vysvětlen, nebo hůře, že není vysvětlen vůbec a očekává se, že si jej čtenář dohledá jiným způsobem. To se bohužel týká mnohé literatury, která se tímto tématem zabývá. Problém je dle mého názoru způsoben faktem, že se jedná o velmi rozsáhlou a komplikovanou problematiku, kdy detailnějšího vysvětlení jednoho pojmu způsobí rozvětvení na mnohé další pojmy, které je zapotřebí vysvětlit taktéž.

Druhým cílem tedy bylo zvolit takovou úroveň detailu, aby vše důležité bylo řečeno, čtenář se v textu „neztrácel“, a v případě zájmu o prohloubení znalostí k daném tématu byl odkázán na relevantní informace. Zároveň si práce musela udržela přiměřený počet stran.

Třetím a posledním cílem bylo provázat pojmy probírané v rámci kapitoly do jednoho celku a z něj vyvodit závěry, které nejsou na první pohled zřejmé. Ideálně by čtenář na konci kapitoly měl chápat důvody, které vedly Evropskou unii a organizaci ETSI k vyvinutí a zavedení standardizovaných formátů elektronického podpisu a jak jej nyní může široká veřejnost zužitkovat.

Kapitola 5 seznamuje čtenáře se základy legislativy, která se týká bezpečnostních prvků digitálních dat. Především pak s nařízením eIDAS, které má v současné době v rámci EU na proces digitalizace velký vliv. Pokud se kapitola 4 dívá na problematiku očima IT, pak kapitola 5 se o to snaží z pohledu práva.

Kapitola 6 přibližuje technické řešení úložiště důvěryhodných dokumentů, které je v souladu s předchozími kapitolami.

V rámci všech kapitol je snaha o co nejobecnější popis řešené domény, aby mohl čtenář poznatky této práce využít při řešení své vlastní problematiky.

# 3 Dokument

Cílem kapitoly je čtenáře seznámit se základními pojmy z domény, kterou se práce zabývá. Zavést pojem dokument, popsat rozdíl mezi listinnou a elektronickou podobou či objasnit, co znamená, když o dokumentů tvrdíme, že je důvěryhodný.

## 3.1 Definice dokumentu

Pojem dokument je jasně definován v českém právním řádu zákonem o archivnictví a spisové službě:

*Dle § 2 písm. e) zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, je dokument každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové, či digitální, která byla vytvořena původcem nebo byla původci doručena.*

Dokument nemusí být jen písemnosti, ale také různé fotografické, filmové či zvukové záznamy. Jak můžeme vidět, zákon pracuje s mírně odlišnou terminologií. Místo o *listinném dokumentu hovoří* o *analogovém dokumentu* a o *elektronickém dokumentu* hovoří jako o *digitálním dokumentu*. Tento problém vyvstává z důvodu, že neexistuje ustálená terminologie a různá ministerstva vydávají zákony, které tyto pojmy různě kombinují či se jim zcela vyhýbají a vytváří si své vlastní[4]. V rámci této práce bude použita terminologie *listinného* a *elektronického* dokumentu, která je použita i v nařízení eIDAS.

## 3.2 Listinný a elektronický dokument

Vznikem písma před přibližně 5 000 lety [1] byly vytvořeny nezbytné základy pro uchovávání, zpracovávání a zpřístupňování informací. Pro zápis sloužily nejprve kameny, hliněné destičky, papyry či hedvábí. Postupem času dospěla civilizace k papíru, který se ukázal jako efektivní nosič informací, přičemž jeho efektivnost ještě navýšil vynález knihtisku.

S rychlým vývojem nových prostředků pro komunikaci na počátku 20. století postupně ztrácel i papír své výlučné postavení. Kromě písemností lidé začali zaznamenávat obraz, pohyb a zvuk. Papír přestal být jediným nosičem, na kterém by bylo možno uchovávat všechny informace. Filmové technologie poskytly metody mikrofilmování a mikrofišování dokumentů, které byly původně zaznamenány na papíře, a tím umožnily novým způsobem uchovávat dokumenty.

Doposud poslední významný milník přišel na přelomu 20. a 21. století v podobě digitálních médií a internetu. Tyto technologie konkurují listinným dokumentům ještě zřetelněji, a to ve smyslu co nejvíc upozadit papír ve prospěch digitální komunikace a uchování dokumentů v elektronické podobě.

[4] Místo o elektronickém dokumentu hovoří například o *dokumentech obsažených v datové zprávě*.

Elektronické dokumenty vyžadují počítač nebo jiné elektronické zařízení, aby mohly být zobrazovány, interpretovány a zpracovávány. Jsou generovány softwarem a ukládány na HDD/SSD disky, CD/DVD a další zařízení sloužící k uchovávání digitálních dat. Na rozdíl od listinných dokumentů mohou obsahovat taktéž nelineární informace jako jsou hypertextové odkazy. Elektronické dokumenty nejsou novým typem dokumentu, ale moderní formou nosiče a způsobu zaznamenávání informací.

## 3.3 Důvěryhodný dokument

České právo nezná definici *důvěryhodného dokumentu*. Avšak existují vlastnosti, které od takového dokumentu očekáváme. Patří mezi ně:

1. Pravost, která není rozporována.
2. Spolehlivost obsahu dokumentu.
3. Vypovídací hodnota, která nebude soudem zpochybňována.

Abychom mohli dokument považovat za pravý a spolehlivý (bod 1. a 2.), tak musí být:

- originální nebo odvozený z originálního dokumentu (u kopie, repliky nebo konverze lze doložit shodu s originálem),
- nepadělaný,
- obsahově nezměněný a neupravovaný.

A dále:

- lze prokázat jeho existenci k určitému datu,
- lze identifikovat původce,
- musí odrážet skutečnou vůli stran,
- musí být čitelný.

Bod 3., zda soud bude nebo nebude zpochybňovat vypovídací hodnotu dokumentu jakožto důkazního prostředku v soudním řízení, je vždy na rozhodnutí konkrétního soudu.

Významnou roli pro splnění výše uvedených vlastností má podpis, který je důležitým bezpečnostním prvkem každého důvěryhodného dokumentu.

## 3.4 Podpis

Podpis se v právu považuje za nezpochybnitelný doklad souhlasu osoby s takto písemně projevenou vůlí. Podpisy mají tři funkce:

1. Označovací: identifikace toho, kdo učinil právní úkon.
2. Deklarační: potvrzení projevu vůle.
3. Důkazní: ověření totožnosti jednajícího.

Dokumenty mohu být kupříkladu opatřeny podpisem autora, jednatele firmy, či osoby odpovídající za správnost.

Podepsaný dokument lze považovat za důvěryhodný pouze tehdy, pokud je zřejmé, za jakým účelem byl dokument podepsán. Účel může plynout z typu podepsaného dokumentu (například smlouvy podepisujeme za účelem vyjádření vůle podepisujících stran splnit povinnosti stanovené ve smlouvě) nebo z explicitního prohlášení účelu podpisu, které je například součástí připojené doložky.

O spolupodpisu mluvíme tehdy, pokud je k platnosti nějakého aktu potřeba více podpisů.

### 3.4.1 Podpis listinného dokumentu

Jedná se většinou o podpisy vlastnoruční. Podpisy listinných dokumentů jsou nejčastěji psány písmem, které se běžně používá ve státě, kde je text podepsán. V České republice je to latinka. Pokud má písmo tiskací i psací variantu, je preferovaná psací podoba. Ve středověku byly používány i podpisy symbolické, například kryptogramy jmen. Velký význam a rozlišovací hodnotu má vlastnoruční podpis především pro svou mimořádně obtížnou padělatelnost.

Obrázek 1: Vlastnoruční podpis John von Neumanna

Pro některé dokumenty je zapotřebí *úředně ověřený podpis*, což je podpis, který byl ověřen notářsky, soudně či úředně.

### 3.4.2 Podpis elektronického dokumentu

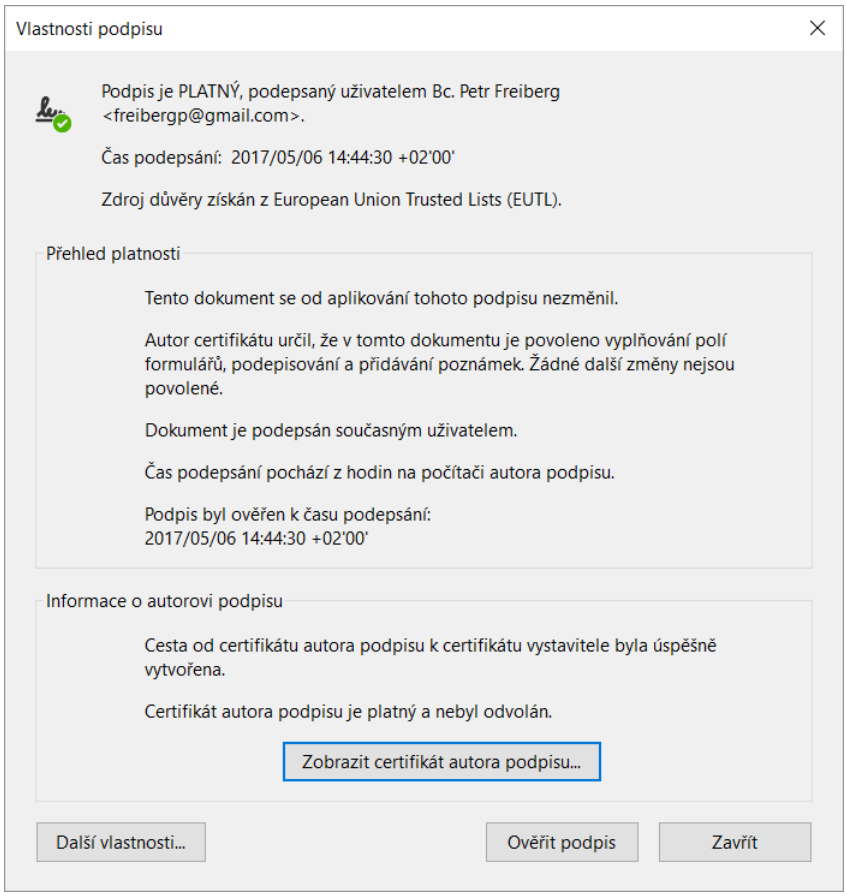
Podepsání u elektronických dokumentů zajišťují elektronické podpisy nebo elektronické pečeti/značky[5]. Jedná se o specifická data, která nahrazují klasický

[5]V rámci sjednocení české legislativy s nařízením eIDAS budou po dvou letech od přijetí tohoto nařízení, které proběhlo 1. 7. 2016, elektronické značky zrušeny. Zůstanou pouze elektronické pečeti.

vlastnoruční podpis a jsou součástí samotného dokumentu nebo jsou s ním logicky spojeny. Dnes jsou nejčastěji založeny na asymetrické kryptografii. Pokud budeme hovořit o *elektronickém podpisu* a nebude uvedeno jinak, tak máme na mysli právě tento druh elektronického podpisu.

Elektronický podpis není ve své podstatě ničím jiným než číslem. Jelikož se jedná o velmi dlouhé číslo, nepracuje se s ním v binární podobě, ale je kódován. V praxi uživatel s elektronickým podpisem v číselné podobě nepracuje. Pracují s ním programy, které elektronický podpis vytváří a ověřují. Výsledek ověření pak prezentují v uživatelsky přívětivé podobě (viz obrázek 2).

Podrobně se budeme elektronickým podpisům, pečetím a dalším bezpečnostním prvkům elektronických dokumentů věnovat v kapitole 4.




Obrázek 2: Podrobné informace o elektronickém podpisu

### 3.4.3 Ověření vlastnoručního a elektronického podpisu

Vlastnoruční podpisy zkoumá písmoznalec, který zkoumá a porovnává podpisy za účelem potvrzení nebo vyvrácení identity pisatele. Zkoumá výšku, šířku a sklony jednotlivých znaků či rozložení tlaku a plynulost psaní jednotlivých psacích tahů.

U elektronického podpisu samozřejmě nic takového nemá smysl zkoumat. Místo toho se porovnává hodnota elektronického podpisu a validita jeho atributů. Mezi to například patří ověření, zda nebyl revokován certifikát, na kterém je podpis založen. Podrobně se tímto zabývá kapitola 4.5.

## 3.5 Ztráta důvěryhodnosti

Listinný i elektronický dokument ztrácí svou důvěryhodnost, pokud:

- je nečitelný,
- byl obsahově změněn.

Elektronický dokument navíc ztrácí důvěryhodnost, jestliže nelze jednoznačně prokázat platnost bezpečnostních prvků, kterými je dokument ošetřen právě pro potřeby zaručení důvěryhodnosti. Na ztrátu důvěryhodnosti u elektronického dokumentu nejčastěji přijdeme ve chvíli, kdy ověřujeme platnost bezpečnostních prvků.

## 3.6 Výhody a nevýhody listinných a elektronických dokumentů

Používání listinného a elektronického dokumentu sebou nese jisté výhody a nevýhody:

### Dostupnost

Elektronický dokument je většinou doručen adresátovi téměř okamžitě, v řádu sekund. Oproti tomu u listinného dokumentu se doba doručení pohybuje od několika minut po dny v závislosti na vzdálenosti a použitém přepravním prostředku. To samé platí pro dobu obdržení potvrzení o doručení dokumentu.

### Operace nad dokumentem

Vyhledávání a analýza jsou u elektronických dokumentů nesrovnatelně rychlejší a efektivnější, protože jsou téměř vždy prováděny strojově.

### Přehlednost procesů

Elektronické dokumenty umožňují snadnější kontrolu stavu zpracování (nový, přiděleno zpracovateli, zpracováno, ...). Samozřejmě, že je to možné zvládnout i klasickými prostředky, ale je to značně náročné ve chvíli, kdy například chceme zajistit přesně definovaný oběh dokumentu mezi více lidmi.

### Archivace

Největší problém u elektronických dokumentů způsobuje zajištění dlouhodobé validity. Zatímco u listinných dokumentů víme, jak je udržovat i po dlouhou dobu (jsme schopni bez sebemenších problémů přečíst listinné dokumenty staré stovky

let), u elektronických dokumentů je to stále řešenou otázkou. Například účetní doklady nemáme jen pro aktuální období, ale musíme je uchovávat i mnoho let po jejich vystavení a být je po celou dobu schopni přečíst. To, že je v současnosti elektronický dokument považován za čitelný, neznamená, že tomu tak bude i za 10 nebo 100 let. Za relativně krátkou historii elektronických dokumentů jsme se setkali s několika případy zastarání velmi rozšířených technologií (např. diskety). Velmi složitou problematikou je taktéž udržení důvěryhodnosti a možnost i po dlouhé době s určitostí ověřit, že měl elektronický dokument k určitému časovému okamžiku platné všechny bezpečností prvky (tímto se budeme podrobně zabývat v kapitole 4.2). U listinných dokumentů je tento problém opět už dávno vyřešený.

### Ochrana dokumentu

U elektronického dokumentu jsou nutná hardwarová a softwarová opatření pro zálohování a ochranu. U listinných dokumentů pak ochrana souvisí například se správnou vlhkostí vzduchu v místnosti, kde jsou dokumenty skladovány. Ochrana dokumentů v elektronické podobě je levnější v nákladech na manipulaci s dokumenty, ušetří se na tisku, papírech a prostorech potřebných pro uskladnění. Platit se naopak musí za hardware a software. Náklady mohou být různé, ale dá se říci, že čím více dokumentů uchováváme, tím je ochrana elektronických dokumentů levnější a listinných dražší.

### Zabezpečení dokumentu

Elektronický dokument lze s použitím elektronického podpisu snadno ochránit před možností nezpozorovaného pozměnění obsahu. Listinný dokument se před pozměněním obsahu může chránit několika vyhotoveními (nejčastěji dvěma), kdy každá protistrana dostane jedno vyhotovení. Pokud však existuje jen jedno vyhotovení, může být zjištění změny mnohem složitější (a v některých případech až nemožné). Ověření, zda nedošlo k pozměnění dokumentu, je opět u elektronické podoby záležitostí sekund. U listinné podoby například záleží na počtu stran a zkušenosti toho, kdo kontrolu provádí.

S pomocí šifrování pak lze elektronický dokument lehce chránit proti odpozorování. Šifrování se u listinných dokumentů dá provést taktéž, ale proces šifrování a dešifrování je mnohem pomalejší. Alternativou je listinný dokument umístit na chráněné místo jako je bankovní schránka.

# 4 Bezpečnostní prvky digitálních dat

Zabezpečení digitálních dat, do čehož řadíme například elektronického podpisy, digitální certifikáty či možnost dlouhodobého ověření, je velice rozsáhlá problematika, která by vydala na mnoho knih. Cílem kapitoly proto není podrobný popis, ale ucelený pohled na její důležité aspekty. Po přečtení kapitoly by měl čtenář mít povědomí o problematice, znát její významné nástrahy a rozumět potřebě zavedení standardizovaných formátů elektronického podpisu.

## 4.1 Asymetrická kryptografie

Asymetrická kryptografie (kryptografie s veřejným klíčem) je skupina kryptografických metod, ve kterých se pro šifrování a dešifrování používají odlišné klíče:

1. soukromým klíčem šifrujeme,
2. veřejný klíčem dešifrujeme.

Asymetrická kryptografie eliminuje sdílené tajemství. Ten, kdo šifruje, nemusí s příjemcem, který dešifruje, sdílet klíč, což se dá považovat za zásadní výhodu oproti symetrické kryptografii, kde se stejným klíčem šifruje i dešifruje. Nevýhodou je, že v závislosti na implementaci může být asymetrická kryptografie při šifrování i dešifrování zásadně pomalejší než kryptografie symetrická.

Soukromý a veřejný klíč jsou spolu matematicky svázány a nezbytnou podmínkou je, aby ze znalosti veřejného klíče nešlo odvodit klíč soukromý. K tomu se využívají tzv. *jednocestné funkce*, což jsou operace, které lze snadno provádět pouze v jednom směru. Snadno ze vstupu spočítáme výstup, ale jen velmi obtížně z výstupu spočítáme vstup. Příkladem může být kupříkladu násobení, kdy velmi snadno vynásobíme dvě velká čísla, ale jen obtížně získáme rozklad součinu na činitele. Na tomto matematickém problému je postaven asymetrický šifrovací algoritmus RSA.

Je zapotřebí mít na paměti, že při použití teoretického nekonečného výpočetního výkonu není žádná metoda asymetrické kryptografie bezpečná. Důkazy o bezpečnosti jsou založeny na omezeném výpočetním výkonu, kterého lze v praxi dosáhnout. Právě díky omezenému výpočetnímu výkonu mohou důkazy těchto metod například tvrdit, že je metoda rozluštitelná s využitím současné výpočetní techniky nejdříve za milión let. S rostoucím výpočetním výkonem se ovšem zároveň zkracuje i potřebná doba.

Elektronické podpisy jsou jednou z oblastí, kde se asymetrické kryptografie využívá.

## 4.2 Elektronický podpis

Práce s elektronickými podpisy se liší od práce s podpisy vlastnoručními a opírá se o zcela odlišné principy. S využitím veřejně dostupných nástrojů může být

srovnatelně jednoduchá, a pokud je správně aplikována, může přinášet mnohonásobně vyšší míru spolehlivosti. Elektronické podpisy, o kterých budeme mluvit, jsou založeny na asymetrické kryptografii:

1. Soukromý klíč: používá se při podepisování a musíme ho mít ve svém výhradním vlastnictví. Pokud by byl klíč kompromitován, mohl by sloužit k vytváření falešných podpisů.

2. Veřejný klíč: používá se k ověření podpisu vytvořeného pomocí soukromého klíče. Veřejný klíč musíme zveřejnit, aby ho ostatní mohli použít k ověření platnosti našeho podpisu.

Za elektronický podpis (s přízviskem *prostý*) lze považovat například i textový podpis v patičce e-mailu či scan vlastnoručního podpisu. Takové elektronické podpisy však nemají v podstatě žádnou přidanou hodnotu, a proto je nebudeme dále uvažovat. Elektronické podpisy, které jsou založeny na asymetrické kryptografii, jsou legislativně označovány jako *zaručené elektronické podpisy*. Pokud je v práci použit pojem *elektronický podpis*, tak je tím myšlen elektronický podpis využívající asymetrickou kryptografii, legislativně nazývaný jako *zaručený elektronický podpis*.

### 4.2.1 Záruky elektronického podpisu

Elektronický podpis nám poskytuje jisté záruky, řadí se mezi ně:

1. Integrita (neporušenost či neměnnost): základní záruka elektronického podpisu. Nedokáže sice předejít tomu, že podepsaný elektronický dokument nebude moci být pozměněn, ale dává nám jistotu, že pokud k tomu dojde, spolehlivě to poznáme. Nedozvíme se ovšem, jak moc a kde byl pozměněn. Jestli byl pozměněn v pár bitech, nebo byl dokonce změněn celý. Narušení integrity odhalíme ve chvíli, kdy budeme vyhodnocovat platnost podpisu. Máme záruku, že pokud je podpis po vyhodnocení označen za platný, tak se od podepsání nezměnil.

   Ke změně může dojít záměrně, když někdo dopíše do smlouvy něco, s čím bychom nesouhlasili a smlouvu kvůli tomu nepodepsali. Stejně tak ke změně může dojít selháním techniky, například během přenosu po síti. O dokumentu, jehož integrita je neporušená, se říká, že je pravý (autentický).

2. Nepopiratelnost: osoba, která elektronický podpis vytvořila, nemůže popřít jeho vytvoření ani důsledky, kterou sebou elektronický podpis přináší. Důvodem je fakt, že pro vytvoření elektronického podpisu je zapotřebí vlastnit soukromý klíč, který je svázán s veřejným klíčem a tento soukromý klíč musí být ve výhradním vlastnictví autora podpisu. S pomocí soukromého klíče se elektronický podpis vytváří a s využitím veřejného klíče ověřuje.

3. Autentizace: umožňuje zjistit identitu toho, komu elektronický podpis patří, tzv. *podepisující osobu* či *původce*. Autenticita je realizována pomocí *přenosu důvěry*.

### 4.2.2 Tvorba elektronického podpisu

Pro tvorbu elektronického podpisu potřebujeme:

1. Nástroj pro vytváření elektronických podpisů. Tím může být například program Adobe Acrobat Reader DC (dále Adobe Reader).

2. Individuální data pro vytváření elektronických podpisů, tedy soukromý klíč.

3. Dokument, který chceme elektronickým podpisem opatřit.

Vybraný nástroj načte soukromý klíč, dokument, který chceme podepsat, a pomocí zvoleného asymetrického algoritmu (například RSA) vytvoří elektronický podpis.

Aby byla tvorba elektronických podpisů dostatečně rychlá, je zapotřebí, aby data, která tvoří dokument a podepisujeme je, byla relativně malá. Navíc je zapotřebí pracovat s bloky dat o pevné velikosti z toho důvodu, že metody a algoritmy, které se k podepisování používají, toto vyžadují. Pokud při tvorbě elektronického podpisu použijeme asymetrický šifrovací algoritmus RSA se soukromým klíčem o velikosti 2048 bitů, můžeme podepsat data o maximální velikosti 1712 bitů. Velmi často potřebujeme podepsat data větší, než je zde uvedená velikost. Data by samozřejmě šlo rozdělit na menší části a podepsat každou část samostatně, nicméně by to enormně zvyšovalo složitost a náklady bez jakékoliv přidané hodnoty. Pro vyřešení tohoto problému se využívají hašovací funkce. Vstupem do hašovací funkce jsou data libovolné velikosti, výstupem jsou data o pevné velikosti, tzv. *haš*. Takto můžeme podepsat jakkoliv velká data, nebudeme totiž podepisovat samotná data, ale vždy jejich haš.

#### 4.2.2.1 Hašování

Formálně jde o matematickou funkci $h$, která převádí vstupní posloupnost bitů na posloupnost pevné délky $n$ bitů. Výstupu hašovací funkce říkáme haš či otisk. Hašovací funkce mají vícero použití, využívají se například pro:

- Hašovací tabulky: datová struktura, která slouží k ukládání dvojic klíč-hodnota a umožňuje rychlé vyhledávání položek, který jsou v ní uloženy. Hodnota klíče je spočítána ze vstupní hodnoty pomocí hašovací funkce.

- Kontrolního otisku digitálních dat: slouží jako metoda pro detekci náhodných a neúmyslných chyb při přenosu dat nebo jejich ukládání.

- Elektronické podpisy.

Požadavky na ně se dle použití liší. Mezi základní vlastnosti obecně patří:

1. Pro stejná vstupní data bude vždy vrácen stejný haš.

2. Haše by měly být co nejrovnoměrněji distribuovány v oboru hodnot, do kterého jsou mapovány.

3. Jakkoliv velká vstupní data budou mít haš pevné velikosti.

4. I malá změna ve vstupních datech velmi ovlivní výslednou podobu haše.

Třetí bod řeší problém algoritmů používaných při tvorbě elektronických podpisů, které umí pracovat jen s bloky dat o pevné velikosti. Čtvrtý bod zajišťuje integritu, základní záruku elektronického podpisu.

Při tvorbě elektronických podpisů se využívá speciální třída hašovacích funkcí, tzv. *kryptografické hašovací funkce*.

#### 4.2.2.2 Kryptografické hašovací funkce

Kryptografické hašovací funkce jsou speciální třídou hašovacích funkcí, které mají specifické vlastnosti vhodné pro použití v kryptografii. Základní vlastnosti, které jsme si uvedli výše, rozšiřují o tyto silné požadavky:

1. Odolnost vůči získání předlohy: jedinou cestou, jak získat vstupní data z výstupního haše kryptografické hašovací funkce, je pouze útok hrubou silou, tedy systematické otestování všech možných kombinací.

2. Odolnost vůči nalezení kolize: nalézt dva vstupy, které budou mít na výstupu stejný haš, je opět možné pouze útokem hrubou silou.

Jak za chvíli zjistíme, druhý bod, tedy *odolnost vůči nalezení kolize*, je u elektronických podpisů **klíčový požadavek**. Mezi další požadavky na kryptografické hašovacích funkcí často patří:

1. Neexistující korelace mezi vstupními daty a výstupním hašem pro ztížení kryptoanalýzy[6].

2. Obtížné nalezení dvou vstupů, u kterých se haš liší jen v malém počtu bitů.

3. Obtížné nalezení jen části vstupu z výsledného haše.

*Odolnost* a *obtížnost* vychází z výpočetní složitosti, která musí být u používaných kryptografických hašovacích funkcí natolik vysoká, aby byla mimo možnosti současné výpočetní techniky. Mezi dnes nejpoužívanější kryptografické hašovací funkce patří rodina funkcí SHA-2 (SHA-256, SHA-512, ...).

Předchůdcem byla SHA-1, u které byl však v roce 2005 nalezen algoritmus, který umožňoval zásadně snížit výpočetní složitost pro nalezení kolize. Metoda nalezení kolize hrubou silou byla však stále nad možnosti tehdejší techniky. V únoru roku 2017 pak firma Google demonstrovala kolizní funkci, která umožňuje v relativně krátkém čase vytvořit dva kolizní dokumenty ve formátu PDF.

[6] Obor zabývající se metodami získávání obsahu šifrovaných informací.

Tedy možnost vytvořit dva různé dokumenty, které mají při použití hašovací algoritmu SHA-1 stejný haš.

Existenci kolizních dokumentů nelze zabránit, protože ta vyplývá ze samotné podstaty hašování. Neexistuje totiž prosté zobrazení z větší do menší množiny. A je to právě odolnost vůči nalezení kolize a hrozba kolizních dokumentů, co vyžaduje velkou pozornost.

#### 4.2.2.3 Kolizní dokumenty

Použití hašovacích funkcí řeší problém s podepisováním libovolně velkých elektronických dokumentů, ale přináší sebou nepříjemný problém v podobě kolizí. Budou totiž vždy existovat takové dokumenty, které sice jsou vzájemně odlišné, ale jejich haše se rovnají. Podpisem stejných hašů vznikne identický elektronický podpis. Máme-li dva různé dokumenty, jeden podpis a nejsme schopni rozlišit, kterému dokumentu podpis patří, tak můžeme říci, že došlo ke kolizi. Existují dva typy kolizí:

1. Kolize prvního řádu: vytvoření dvou jakýchkoliv dokumentů, které mají stejný haš.

2. Kolize druhého řádu: máme dokument a jsme k němu schopni vytvořit odlišný dokument se stejným hašem.

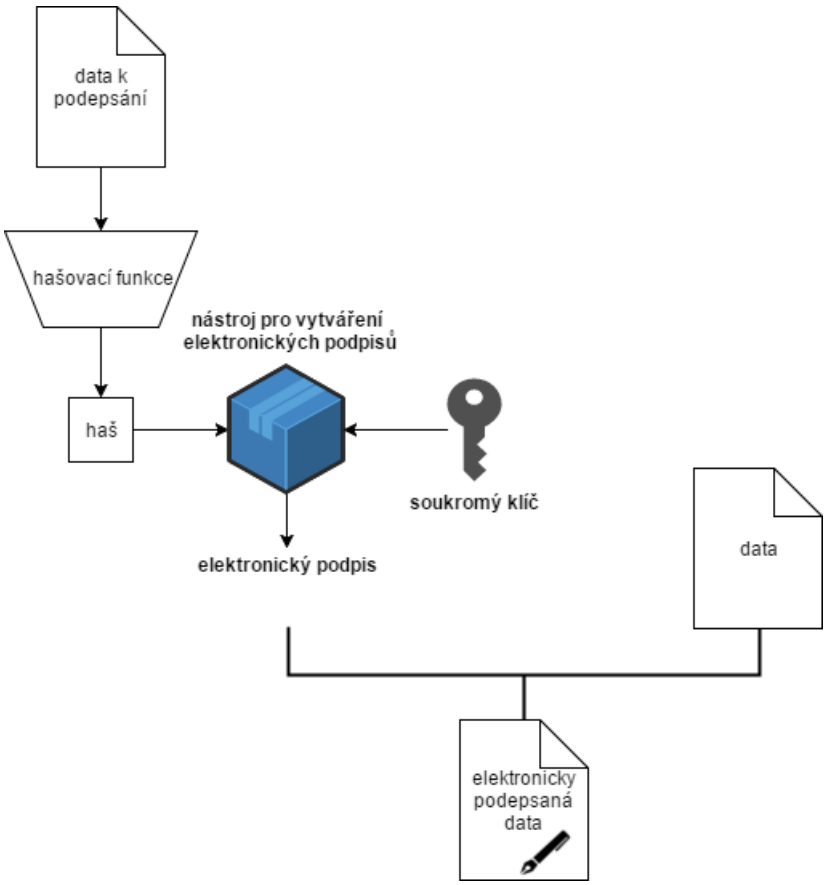
Kolize druhého řádu je složitější, ale o to nebezpečnější. Například můžeme elektronicky podepsat dokument, který následně někdo pozmění a bude s ním operovat vůči třetí straně. Haše obou dvou elektronických dokumentů (originálu a falzifikátu) se budou stále shodovat a nebude tak porušena integrita elektronického podpisu. Třetí strana nebude mít možnost poznat, že byl od našeho podpisu dokument změněn.

Jak uvidíme později, elektronický podpis je s dokumentem vždy propojen na základě nějaké struktury. V té je místo pro dokument a pro podpis. Samotná výměna originálního dokumentu za falzifikát by pak proběhla na úrovni této struktury.

Je tedy nezbytné, aby nikdo nebyl schopen v rozumném čase (tisíce či milióny let) nalézt jakýkoliv kolizní dokument, který by umožnil zneužití. To zajišťuje správně navržená kryptografické hašovací funkce. Jedná se však o nikdy nekončící boj, kdy na jedné straně máme stále silnější a propracovanější hašovací funkce, s větším počtem bitů, na druhé straně však máme stále vyšší výpočetní sílu počítačů. Ty sice v dané chvíli nedokáží nalézt v rozumném čase kolizní dokument, ale při dnešním rapidním vývoji technologií stejný výpočet provedou za určitou dobu v podstatně kratším čase (několik let, či jen měsíce nebo dny). Průběžné posilování ochrany proti kolizním dokumentům je zapotřebí provádět s dostatečným předstihem. Pokud by totiž už existovaly, nemáme možnost od sebe odlišit podepsané originální a falzifikované elektronické dokumenty. K průběžnému posílení došlo například v roce 2010, kdy byla hašovací funkce SHA-1 nahrazena rodinou hašovacích funkcí SHA-2.

#### 4.2.2.4 Zjednodušené schéma

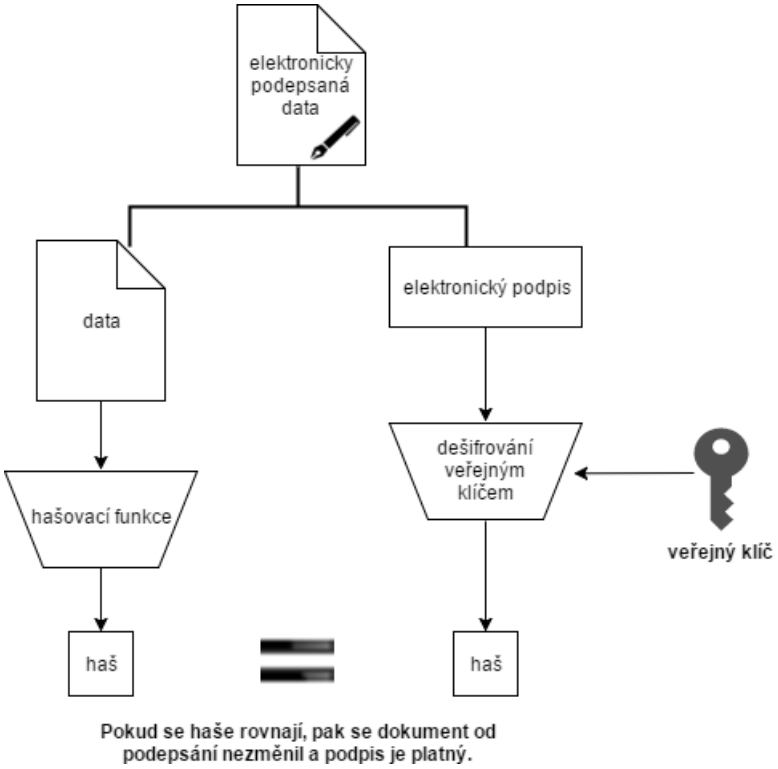
Na zjednodušeném schématu, které demonstruje tvorbu elektronického podpisu, můžeme vidět, že na data dokumentu, který chceme podepsat, je aplikována hašovací funkce. Na haš a soukromý klíč potom nástroj pro vytváření elektronických podpisů aplikuje zvolený algoritmus (například RSA). Výstupem je elektronický podpis, což je binární číslo, které je následně kódováno a umístěno do struktury, která jej logicky spojuje s dokumentem.




Obrázek 3: Zjednodušené schéma tvorby elektronického podpisu

Druhé zjednodušené schéma demonstruje ověření elektronického podpisu. Na příjmu jsou elektronicky podepsaná data rozdělena na samotná data a elektronický podpis. Na data je aplikován hašovací algoritmus a výsledný haš je porovnán s dešifrovaným elektronickým podpisem. Pokud se haše rovnají, pak se dokument od podepsání nezměnil a podpis je platný.

Je třeba mít na paměti, že je zapotřebí použít stejné algoritmy jako při podepisování a veřejný klíč použitý k dešifrování musí být v páru se soukromým klíčem, který byl použit k tvorbě podpisu.




Obrázek 4: Zjednodušené schéma ověření elektronického podpisu

### 4.2.3 Elektronická pečeť

Kromě elektronického podpisu se můžeme setkat ještě s pojmem *elektronická pečeť*. Elektronický podpis je určen pouze fyzickým osobám, neexistuje tedy elektronický podpis pro právnické osoby, organizace, úřady apod. Naproti tomu elektronickou pečeť může vytvářet pouze právnická osoba (včetně organizační jednotky státu) a může ji připojit jen na to, čeho je sama původcem. Připojení elektronické pečeti není projevem vůle jako je tomu u podpisu, ale deklarací původu.

Po technické stránce se jedná o stejnou technologii, jaká je používána u elektronického podpisu. Rozdíl mezi elektronickým podpisem a pečetí je tedy čistě legislativní, nikoli technologický.

### 4.2.4 Digitální certifikát

Třetí zárukou elektronického podpisu (viz kapitola 4.2.1) je autentizace, která umožňuje ověřit identitu toho, komu elektronický podpis patří. Elektronický podpis vytváříme za pomoci soukromého klíče a pro jeho ověření protistrana používá klíč veřejný, který jí poskytneme. Jak si však může být protistrana jista, že veřejný klíč, který je jí k ověření poskytnut, opravdu náleží dané osobě a ne někomu, kdo se za ni pouze vydává? Tuto problematiku řeší certifikáty.

Digitální certifikát je elektronicky podepsaný veřejný klíč, který vydává certifikační autorita. Obsahuje informace o majiteli konkrétního veřejného klíče a vydavateli certifikátu (tj. certifikační autoritě). Současně je certifikátem stvrzeno, že ten, komu byl certifikát vydán, má v držení i odpovídající soukromý klíč. Můžeme pak říci, že „elektronický podpis je založen na certifikátu“. Jedny z nejpoužívanějších jsou certifikáty dle mezinárodního standardu X.509.

První verze standardu byla publikována v roce 1988, dnes je nejrozšířenější ve verzi 3. Specifikuje nejen formát certifikátů, ale taktéž třeba formát *seznamu odvolaných certifikátů*, ke kterým se dostaneme o něco později. Struktura certifikátu podle standardu X.509v3 například obsahuje:

- Verzi standardu X.509.
- Sériové číslo certifikátu, které mu přidělil vydavatel.
- Jméno certifikační autority, která certifikát vystavila.
- Začátek a konec řádné platnosti certifikátů.
- Údaje o vlastníkovi, kterému byl certifikát vystaven.
- Informace o veřejném klíči vlastníka: algoritmus veřejného klíče a samotný veřejný klíč (data).
- Elektronická pečeť certifikační autority společně s použitým algoritmem. Samotný certifikát je tedy podepsán (pečetěn) soukromým klíčem certifikační autority, aby byla zaručena integrita v něm uvedených informací.

Tyto informace jsou v certifikátu popsány pomocí jazyka ASN.1 (Abstract Syntax Notation One)[7]. Následně mohou být kódovány například binárně pomocí kódování DER, nebo pokud je DER certifikát zakódován pomocí Base64[8] a umístěn mezi řádky „—–BEGIN CERTIFICATE—–“ a „—–END CERTIFICATE—–“, můžeme říci, že je kódován v PEM.

### 4.2.5 Certifikační autorita

Ten, kdo vydává certifikáty, je nazýván certifikační autoritou (CA). Certifikační autoritu si můžeme provozovat i v rámci svého počítače a vydávat si certifikáty sami, hovoříme pak o tzv. *self-signed certifikátech*[9]. Certifikační autority si například často provozují banky pro potřeby zabezpečení svého internetového bankovnictví.

[7] Jazyk, který na základě souboru formálních pravidel umožňuje obecným a standardizovaným způsobem popsat struktury objektů a to nezávislé na konkrétním řešení.

[8] Kódování převádějící binární data na posloupnost tiskutelných znaků.

[9] Jedná se o specifický certifikát, který podepsal sám jeho tvůrce, který se tak zároveň stal certifikační autoritou. U podpisu, který je na takovém certifikátu založen, většinou probíhá jen ověření na neporušení integrity.

Certifikát, který si vydáme v rámci vlastní certifikační autority, nemá příliš velkou váhu, protože údaje v něm bychom mohli zfalšovat. Jednalo by se tak o stejný stav, jako když jsme o certifikátech neuvažovali. Informaci o tom, že se jedná o náš veřejný klíč, bychom například dopsali do e-mailu, ve kterém přílohou posíláme podepsaný elektronický dokument společně s veřejným klíčem. Existují tedy instituce, které certifikáty za poplatek vydávají a jejich úkolem je ověřit údaje o majiteli předloženého veřejného klíče. Mluvíme pak o *kvalifikovaném certifikátu*. Hlavní rozdíl mezi certifikátem a kvalifikovaným certifikátem je v tom, že kvalifikovaný certifikát jednoznačně identifikuje osobu a můžeme s jistotou říci, jaké osobě elektronický podpis patří. Kvalifikované certifikáty vydávají *kvalifikovaní poskytovatelé služeb vytvářejících důvěru*, což jsou certifikační autority, které musí splňovat zákonné požadavky na své vlastní fungování.

### 4.2.6 Kvalifikovaný poskytovatel služeb vytvářejících důvěru

Pojem *kvalifikovaný poskytovatel služeb vytvářejících důvěru* zavedlo nařízení eIDAS. Patří do něj certifikační autority, které splňují požadavky tohoto nařízení a mají oprávnění[10] vydávat kvalifikované certifikáty. Nařízení vyžadovalo nové posouzení toho, zda příslušná autorita splňuje vše, co se po ní požaduje, aby mohla vydávat kvalifikované certifikáty. V předchozí právní úpravě kvalifikované certifikáty vydávaly tzv. *akreditované certifikační autority*. Díky přechodným ustanovením dostaly všechny tři tuzemské akreditované certifikační autority (I.CA, PostSignum a eIdentity a.s.) dočasný statut kvalifikovaného poskytovatele služeb vytvářejících důvěru (do 1. 7. 2017) a dostaly tak rok na získání tohoto statutu podle nové právní úpravy a v mezidobí mohly řádně fungovat.

Kromě vydávání kvalifikovaných certifikátů mohou kvalifikovaní poskytovatelé dle eIDAS působit i v jiných oblastech. Například v provozování služeb pro ověřování platnosti kvalifikovaných elektronických podpisů. Čtenáře pro přehledné shrnutí všech kvalifikovaných služeb odkazuji na článek Jiřího Průšy [2].

### 4.2.7 Trusted Services List (TSL)

Jedná se o seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru, které v členských zemích EU poskytují své kvalifikované služby. Členské státy pak na základě eIDAS musí kromě tuzemských certifikátů uznávat i ty, které vydala jakákoliv certifikační autorita v rámci EU, jenž je zařazena do tohoto seznamu. Každý členský stát si spravuje svůj vlastní seznam, který publikuje na internetu. TSL za Českou republiku je zveřejněn na internetové adrese http://tsl.gov.cz/ a to ve dvou formátech: PDF a XML. Evropská unie poskytuje na adrese https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml rozcestník na TSL všech zemí. Zajímavostí může být přítomnost Islandu, Lichtenštejnska a Norska, což jsou sice státy, které nepatří mezi členské země EU, ale eIDAS do své legislativy zakomponovaly taktéž, protože patří mezi státy Evropského hospodářského prostoru (EHP).

[10] Oprávnění vydávají státem pověřené dohledové orgány, tzv. *subjekty posuzování shody* [2].

### 4.2.8 Kořenové a podřízené certifikační autority

Z praktických důvodů jsou certifikační autority často vnitřně členěny a každá certifikační autorita má svou vlastní vnitřní strukturu:

1. Kořenová autorita: měla by být nejdůvěryhodnějším typem certifikační autority v rámci organizace. Kořenové autority se nejčastěji používají výhradně pro vystavování certifikátů jiným certifikačním autoritám organizace, které se nazývají *podřízené certifikační autority*. Kořenové autority vše zastřešují.

2. Podřízená certifikační autorita (někdy též zprostředkující autorita): certifikační autorita, která získala certifikát od jiné certifikační autority organizace. Obvykle již vystavuje certifikáty koncovým zákazníkům ke konkrétním účelům. Vydává certifikáty k podepisování dokumentů, zabezpečení e-mailu nebo ověřování na webu. Podřízené certifikační autority však mohou vystavovat certifikáty i dalším certifikačním autoritám, které se nacházejí níže v hierarchii autorit.

### 4.2.9 Infrastruktura veřejného klíče (PKI)

V praxi existuje mnoho certifikačních autorit, dohromady pak hovoříme o *infrastruktuře veřejného klíče* (anglicky *Public Key Infrastructure*). Cílem PKI je zajistit důvěryhodný systém distribuce certifikátů a v nich přidružených veřejných klíčů.

Nejdůležitějším faktorem každého certifikátu je jeho důvěryhodnost. Tedy jestli a jak moc můžeme věřit tomu, co je v certifikátu uvedeno. Každý certifikát obsahuje veřejný klíč a identitu osoby, které klíč patří. Tato osoba má ve svém výlučném držení i odpovídající soukromý klíč. Certifikát nejčastěji získáme společně s podepsaným dokumentem. Pokud by tomu tak nebylo, musíme si jej dohledat sami.

Ověřením důvěryhodnosti certifikátu vyhodnocujeme i platnost elektronického podpisu, který je na certifikátu založen. Nejjednodušší způsob, jak bychom u certifikátu mohli posuzovat důvěryhodnost, by bylo samozřejmě individuální posouzení. Například pokud by nám náš obchodní partner, kterého dobře známe a máme v něj důvěru, sám osobně předal svůj certifikát, zařadili bychom ho mezi ty certifikáty, kterým budeme věřit. V praxi je však zapotřebí efektivnější řešení, protože se nemůžeme osobně a dopředu setkat se všemi osobami, od kterých chceme přijímat elektronické dokumenty nebo s nimi elektronicky komunikovat [3]. Je tedy zapotřebí využít důvěryhodného prostředníka, který se nám zaručí za autenticitu certifikátů. A tím i za identitu osob, kterým byly certifikáty vydány. Tímto prostředníkem je, jak již víme, certifikační autorita.

U certifikátů a certifikačních autorit využíváme *delegaci důvěry*. Když důvěřuji konkrétní certifikační autoritě, mohu důvěřovat i všem certifikátům, které tato certifikační autorita vydala. Důvěryhodnost certifikátu odvozujeme od důvěryhodnosti toho, kdo ho vydal.

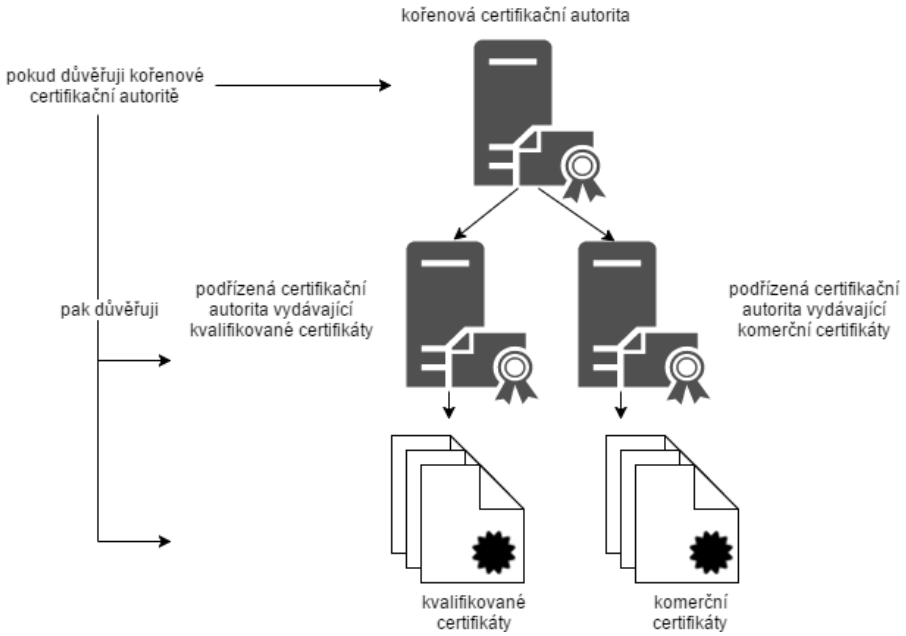
Certifikační autorita používá při vydávání certifikátů svůj vlastní certifikát. Každý vydaný certifikát opatří elektronickou pečetí, která je na jejím certifikátu založena. Připojením elektronické pečeti vyjádří, že ona je původcem vydaného certifikátu. Pokud vyjádříme důvěru certifikátu, na kterém je tato elektronická pečeť založena, pak vyjádříme důvěru certifikační autoritě a všem certifikátům, které vydala.

Vyjadřování důvěry můžeme dále řetězit. Pokud vyjádřím důvěru entitě A a ona pak vyjádří důvěru entitě B, pak i já mohou důvěřovat entitě B. Pokud to uvedeme v terminologii certifikačních autorit, tak pokud považuji za důvěryhodnou jednu certifikační autoritu, a ta prohlásí za důvěryhodné jiné certifikační autority, mohu i já považovat tyto certifikační autority za důvěryhodné.

#### 4.2.9.1 Strom důvěry

Zřetězení důvěry se dá zobecnit do tzv. *stromu důvěry*. V jeho kořeni se nachází *kořenový certifikát*, který odpovídá jedné *kořenové certifikační autoritě*. Z tohoto kořene se pak odvíjí důvěra v další certifikáty *podřízených certifikačních autorit* (vnitřní uzly stromu) a všechny certifikáty koncových uživatelů (listy stromu). Pokud někdo vyjádří svou důvěru kořenovému certifikátu, vyjadřuje tím důvěru v celý strom. Cílem je zjednodušení vyjadřování důvěry, kdy stačí vyjádřit důvěru v jeden kořenový certifikát a prostřednictvím něj projevit svou důvěru ve všechny certifikáty ve stromu.

V praxi pak existuje mnoho certifikačních autorit, a tedy i mnoho stromů důvěry, které jsou vždy založeny na svém vlastním kořenovém certifikátu.




Obrázek 5: Znázornění jednoho stromu důvěry

#### 4.2.9.2 Vyjádření důvěry certifikátu

Vyjádření důvěry, nebo nedůvěry certifikátu je nejdůležitější aspektem elektronického podpisu. Jak jsme si již řekli, elektronický podpis je založen na přiděruženém certifikátu. Od důvěry v certifikát se pak odvozuje důvěra a platnost elektronického podpisu. Pokud uživatel vyjádří důvěru konkrétnímu certifikátu či stromu certifikátů, pak on ponese následky, pokud bude považovat za důvěryhodné něco, co za důvěryhodné považovat neměl. Jestliže certifikát pochází od certifikační autority, která se nachází na TSL, tak můžeme předpokládat, že je důvěryhodný. Naopak pokud certifikát pochází od nám neznámé certifikační autority, pak musíme vždy prověřit jaké jsou na ni ohlasy.

Pokud vyhodnocujeme důvěryhodnost certifikátu, můžeme skončit s jednou ze tří možností:

1. Certifikát je důvěryhodný: certifikát byl prohlášen za důvěryhodný nebo patří do některého ze stromu důvěry, jehož kořenový certifikát byl prohlášen za důvěryhodný.

2. Certifikát není důvěryhodný: certifikát byl prohlášen za nedůvěryhodný nebo patří do některého ze stromu důvěry, jehož kořenový certifikát byl prohlášen za nedůvěryhodný.

3. O důvěryhodnosti certifikátu nelze rozhodnout: nemáme v okamžiku, kdy probíhá kontrola důvěryhodnosti, dostatek informací, abychom dokázali rozhodnout o důvěryhodnosti daného certifikátu.

Důvěru certifikátu, ať kořenovému nebo jinému, vyjádříme tím, že jej vložíme mezi důvěryhodné certifikáty v *úložišti certifikátu* (anglicky *certificate store*). Úložiště důvěryhodných certifikátů může mít v jednoduché podobě plochou strukturu. Každý certifikát, který je v něm vložený, je považován za důvěryhodný. Mohou být však i úložiště certifikátu s vnitřní strukturou v podobě složek, které mají odlišný význam. Tyto složky pak certifikáty kategorizují (například na osobní, kořenové, ...), ale mohou existovat i složky, kde naopak vložíme certifikáty, ke kterým důvěru nemáme.

Pokud certifikát v úložišti certifikátů chybí, nic to neříká o jeho důvěryhodnosti nebo nedůvěryhodnosti. Program, který s daným úložištěm pracuje, pouze nemá podle čeho posoudit důvěryhodnost tohoto konkrétního certifikátu. Jedná se tedy o třetí možnost z předchozího seznamu. Uživatel má možnost certifikát do úložiště, pokud jej neobsahuje, přidat. Toto typicky nastává u tuzemských certifikačních autorit, které často nebývají předvyplněny v zahraničních programech.

Úložišť certifikátů je možno mít několik. Každý program může používat své vlastní, případně jej může sdílet s ostatními programy. Kromě toho například operační systém Windows poskytuje jedno systémové úložiště certifikátů a programy pak mohou využívat kromě svých úložišť i toto. Úložiště certifikátů bývají velmi často předvyplněny takovými certifikáty, které autoři příslušných programů

považují za důvěryhodné. Tím však rozhodují za uživatele, co má považovat za důvěryhodné a ti s tímto vždy nemusí souhlasit. Je třeba vědět o existenci všech relevantních úložišť a jak jsou naplněny.

#### 4.2.9.3 Certifikační cesta

Abychom byli schopni v praxi pracovat s důvěrou v konkrétní certifikáty, je nezbytné umět odvodit jejich příslušnost od konkrétního stromu důvěry. A abychom toto uměli odvodit, musí každý certifikát obsahovat údaje, který nám to umožní. Pro spárování dvou certifikátů se nejčastěji používají atributy:

1. Identifikátor klíče autority (Authority Key Identifier) u podřízeného certifikátu.

2. Identifikátor klíče subjektu (Subject Key Identifier) u nadřízeného certifikátu.

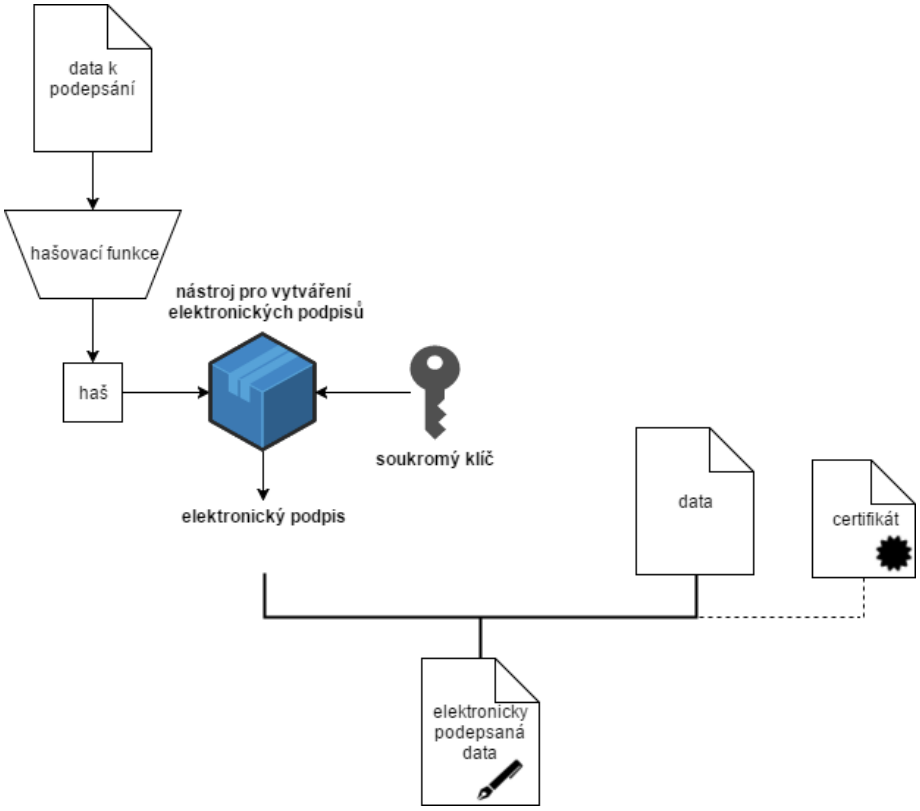
Jedná se o jednoznačný identifikátor, který je odvozen z otisku soukromého klíče, který je použit k vytvoření pečeti u podřízeného certifikátu. Pokud se hodnoty v těchto atributech u obou certifikátů shodují, je prostřednictvím nich možné vytvořit tzv. *certifikační cestu* až ke kořenovému certifikátu. Z kořenového certifikátu pak můžeme určit důvěryhodnost námi posuzovaného certifikátu. Kořenový certifikát je podepsán sám sebou (anglicky *self-signed*), a proto již nemá žádný nadřazený certifikát. U kořenového certifikátu jsou pak buď oba dva atributy prázdné, nebo se jejich obsahy shodují. Při budování certifikační cesty tedy postupujeme zdola nahoru. Jedná se o jeden z možných průchodů takovým stromem či lesem.

*RFC 3280*, které vytváření certifikační cesty popisuje, však upozorňuje, že ne každá certifikační autorita musí vypočítat tyto identifikátory stejný způsobem, proto by se nemělo výhradně usuzovat pouze z těchto dvou atributů, ale vzít v potaz i další atributy. Vybudování certifikační cesty je sice strojově lehce proveditelné, ale je zapotřebí komplexní algoritmus. Pro podrobnější informace čtenáře odkazuji na *RFC 3280*.

#### 4.2.9.4 Zjednodušené schéma s certifikátem

Na zjednodušeném schématu, které je velmi podobné 4.2.2.4, můžeme vidět použití digitálního certifikátu. Jediný rozdíl je, že certifikát obsahující veřejný klíč je přidán k elektronicky podepsaným datům (ať už přímo nebo formou URI[11]). Pokud se jedná o kvalifikovaný certifikát, tak zná ověřující strana s jistotou identitu toho, komu elektronický podpis patří. Zjednodušená ověřující část vypadá prakticky totožně jako v 4.2.2.4, jediný rozdíl je, že se veřejný klíč načítá z certifikátu, který zajišťuje jeho důvěryhodnost.

[11]URI (Uniform Resource Identifier) se skládá z řetězce znaků a identifikuje umístění zdroje informací.




Obrázek 6: Zjednodušené schéma tvorby elektronického podpisu s certifikátem

#### 4.2.9.5 Revokace certifikátů

*Revokace* (zneplatnění, odvolání) je možností, jak předčasně ukončit platnost konkrétního certifikátu. Jedná se o pojistku pro situace, kdy je například kompromitován soukromý klíč. K tomu může dojít při ukradení počítače, ale i prostým zkopírováním v nestřežené chvíli. Ve chvíli, kdy oprávněný vlastník už nemá nad soukromým klíčem výlučnou kontrolu, je nutné sáhnout k revokaci. Pokud by se tak nestalo, pak by ten, kdo klíč zcizil, mohl neoprávněně podepisovat. K revokaci se může sáhnout i v případech, kdy zaměstnanec opouští firmu a přestane vykonávat činnost, pro kterou byl certifikát vystaven. Jedná se o vhodnou prevenci proti případnému zneužití. Od okamžiku, kdy k revokaci dojde, se certifikát považuje za neplatný a vlastník soukromého klíče od této chvíle již nenese zodpovědnost za to, co je podepsáno soukromým klíčem založeném na tomto certifikátu.

Informace o revokaci, která obsahuje, zda certifikát byl nebo nebyl revokován a pokud byl, tak k jakému datu, zůstává u vydavatele certifikátu. Vydavatelem je příslušná certifikační autorita, která URI směřující na revokační informace zapisuje při vystavení přímo do jednoho z atributů v certifikátu. Revokaci vždy zpracovává ta certifikační autorita, která certifikát vydala. I při revokaci je ne-

zbytné spolehlivě ověřit identitu osoby, která o revokaci žádá. Ke spolehlivému ověření má dostatek informací pouze původní vydavatel certifikátu, který je navíc s tím, komu certifikát vystavil, ve smluvním vztahu. Tento smluvní vztah upravuje podobu žádosti o revokaci a v jakých lhůtách ji certifikační autorita zpracuje. Informaci o revokaci je šířena dvěma způsoby:

1. Se zpožděním: seznam revokovaných certifikátů neboli CRL (Certificate Revocation List).

2. V reálném čase: protokol OCSP (Online Certificate Status Procotol).

**Seznam revokovaných certifikátů (CRL)**

Každý CRL obsahuje časový interval (od-do), který udává dobu jeho řádné platnosti. Nejčastěji je to 12 nebo 24 hodin. CRL může být generován na dvou různých principech:

1. Na pravidelném principu: autorita vydá nový CRL, i když nedojde k žádné změně. Obvykle k tomu dochází v době kratší, než je samotná platnost CRL. Bývá to 4 nebo 8 hodin, horní hranicí je 24 hodin.

2. Ad-hoc: autorita vydá nový CRL kvůli žádosti o revokaci. Opět je horní hranicí 24 hodin, ale v praxi k tomu dochází v řádu sekund.

Pravidelnost aktualizací je v podmínkách certifikační autority, ta se však musí pohybovat v mantinelech, které vytyčil zákon. Může existovat více CRL, které mají překrývající se doby platnosti a jejich obsah se může lišit. Starší CRL pak neobsahuje nejaktuálnější revokační informace. Problém pak mohou mít programy, které si v cache udržují CRL po celou dobu jeho platnosti a až poté si stahují nejnovější verzi. Nemusí totiž reflektovat aktuální stav. Vedení CRL může probíhat dvěma způsoby:

1. Kumulativní: CRL je jen jeden, a dochází k jeho průběžné aktualizaci. Obsahuje celou historii revokovaných certifikátů.

2. Intervalový: existuje více CRL pokrývajících vždy jen určitý časový interval. Typicky v délce platnosti příslušného druhu certifikátu (např. 1 rok). V aktuální verzi lze nalézt jen informace o revokaci takových certifikátů, které by jinak byly stále platné. Pro starší informace je zapotřebí dohledat příslušný CRL.

Mohou nastat dva revokační stavy:

1. Zrušení (revoked): certifikát je nenávratně zrušen. Nejčastějším důvodem pro zrušení bývá ztráta nebo kompromitace soukromého klíče. Může k němu dojít i při zjištění, že byly použity zfalšované dokumenty při žádosti o vystavení certifikátu, nebo při porušení jakékoliv jiné podmínky stanovené certifikační autoritou.

2. Držení (hold): certifikát je dočasně neplatný. Nejčastějším důvodem je nejistota uživatel, zda mohl být soukromý klíč ohrožen. Certifikát může být odstraněn z CRL a znovu nabýt platnosti.

Výhodou je, že program nemusí být stále připojen k internetu, protože si CRL může stáhnout jednou denně a zbytek ověřování provádět v off-line režimu. Nevýhodou jsou pak ne vždy aktuální informace.

#### OCSP

OCSP je internetový protokol, který slouží stejně jako CRL k zjištění revokačního stavu. Byl vytvořen jako alternativa k CRL, která adresuje některé jeho problémy. Komunikace probíhá na HTTP protokolu na bázi „dotaz/odpověď". Serverům provozujícím OCSP se říká *OCSP Responder* a provozuje je certifikační autorita, která certifikát vystavila. Odpověď může být:

1. Good: certifikát není revokován.
2. Revoked: certifikát je revokován.
3. Unknown: stav certifikátu není znám.
4. Chybový kód: nelze zpracovat dotaz.

OCSP odpověď je typicky datově úspornější než CRL. Obsahuje i méně dat, která je nutná parsovat. Odpověď je navíc vždy aktuální. Nevýhodou je, že u OCSP probíhá dotaz na revokační status pro každý certifikát samostatně. Pokud chceme zkontrolovat $x$ certifikátů, musíme provést $n$ dotazů.

### 4.2.10 Kvalifikované a komerční certifikáty

V praxi se můžeme setkat s dvěma typy certifikátů, a to s certifikáty *kvalifikovanými* a *komerčními*. Jedná se stejně jako u elektronického podpisu a pečeti o rozdíl legislativní, ne technologický.

Požadavky na kvalifikované certifikáty jsou jasně vymezeny v zákoně. *Kvalifikované certifikáty* se používají pouze k podepisování dokumentů a mohou je vydávat pouze kvalifikovaní poskytovatelé služeb vytvářejících důvěru. Pro ostatní účely, kde se využívá asymetrické kryptografie, jako je přihlašování, šifrování, autentizace či zabezpečení, se používají certifikáty komerční. Pojem *komerční certifikát* zákon nezná a jejich podobu nijak nevymezuje.

Proč legislativa brání využívat kvalifikované certifikáty i k jiným účelům? Například při přihlašování k nějaké službě, která provádí autentizaci prostřednictvím certifikátu, posílá protistrana (server, na které služba běží) přihlašujícímu se uživateli *výzvu*. Jeho prohlížeč ji automaticky podepíše a vrací zpět, čímž se vůči serveru autentizuje. Avšak server by mohl uživateli v rámci *výzvy* podstrčit haš libovolného dokumentu a uživatel, pokud by k přihlašování používal kvalifikovaný certifikát, by mu jej závazně podepsal.

Novinkou, kterou přináší nařízení eIDAS, jsou kvalifikované SSL/TLS certifikáty pro autentizaci webových stránek, které představují jednu z kvalifikovaných služeb vytvářejících důvěru, a proto je mohou poskytovat pouze kvalifikovaní poskytovatelé. Této službě se však nedaří v současné chvíli (červen 2017) stále zaujmout širší veřejnost a zůstává tak pořád spíše na papíře. Čtenáře pro podrobnější informace odkazuji na článek Jiřího Průšy [4].

## 4.3 Časové razítko

Každý elektronický podpis obsahuje datum vzniku. Problém je, že tento časový údaj se přebírá ze systémových hodin zařízení, na kterém elektronických podpis vzniká. Systémové hodiny jsou však většinou lehce přenastavitelné. Takový časový údaj je nespolehlivý a nelze jej brát ve většině případů v potaz. Ke spolehlivému zakotvení v čase slouží *časové razítko*.

Stvrzuje, že to, co bylo orazítkováno, existovalo nejpozději okamžikem v něm uvedeným. Razítko však neříká nic o tom, kdy orazítkovaná data vznikla. Jestli to bylo před pěti sekundami, jednou hodinou či třeba třemi lety. Po technické stránce je časové razítko elektronickým podpisem, který neslouží k podepisování, ale k zafixování v čase. Nepředstavuje žádné vyjádření souhlasu k obsahu samotných dat, proto mluvíme o časovém razítku, ne o elektronickém podpisu.

*Kvalifikovaná elektronická časová razítka* vydává opět kvalifikovaný poskytovatel služeb vytvářejících důvěru, který splňuje požadavky nařízení eIDAS[12]. Často se také používá výraz *autorita časových razítek*, v angličtině *Time Stamp Authority* (TSA), nebo *poskytovatel časových razítek*. Jedná se opět o princip třetí důvěryhodné strany. Stejně jako elektronické podpisy, i časová razítka mohou být založena na certifikátu, který si sami vystavíme, ale takové časové razítko by nebylo o nic prokazatelnější než systémové hodiny.

### 4.3.1 Tvorba časového razítka

Časová razítka jsou popsána v *RFC 3161*. Je specifikována komunikace mezi klientem a poskytovatelem časových razítek či obsah a struktura žádosti a odpovědi o časové razítko. K popisu se používá ASN.1 syntaxe.

Časová razítka vznikají velmi podobným způsobem jako elektronické podpisy. Z dokumentu, který má být opatřen časovým razítkem, se vypočítá haš. Haš následně odešleme poskytovali časových razítek, který k němu přidá potřebné informace a vše opatří svou elektronickou pečetí. Časové razítko je poté připojeno k dokumentu.

Komunikace se skládá z *požadavku* a *odpovědi*. *Požadavek* obsahuje verzi protokolu a haš dat, která chceme razítkem opatřit. Další atributy jsou nepovinné a můžeme jimi například nastavit, zda chceme, aby v odpovědi byl i certifikát,

[12]Na rozdíl od kvalifikovaných certifikátů se na kvalifikovaná elektronická časová razítka nevztahovalo roční přechodobé období. Což však neznamenalo, že si s tím některé státy dělaly těžkou hlavu [5].

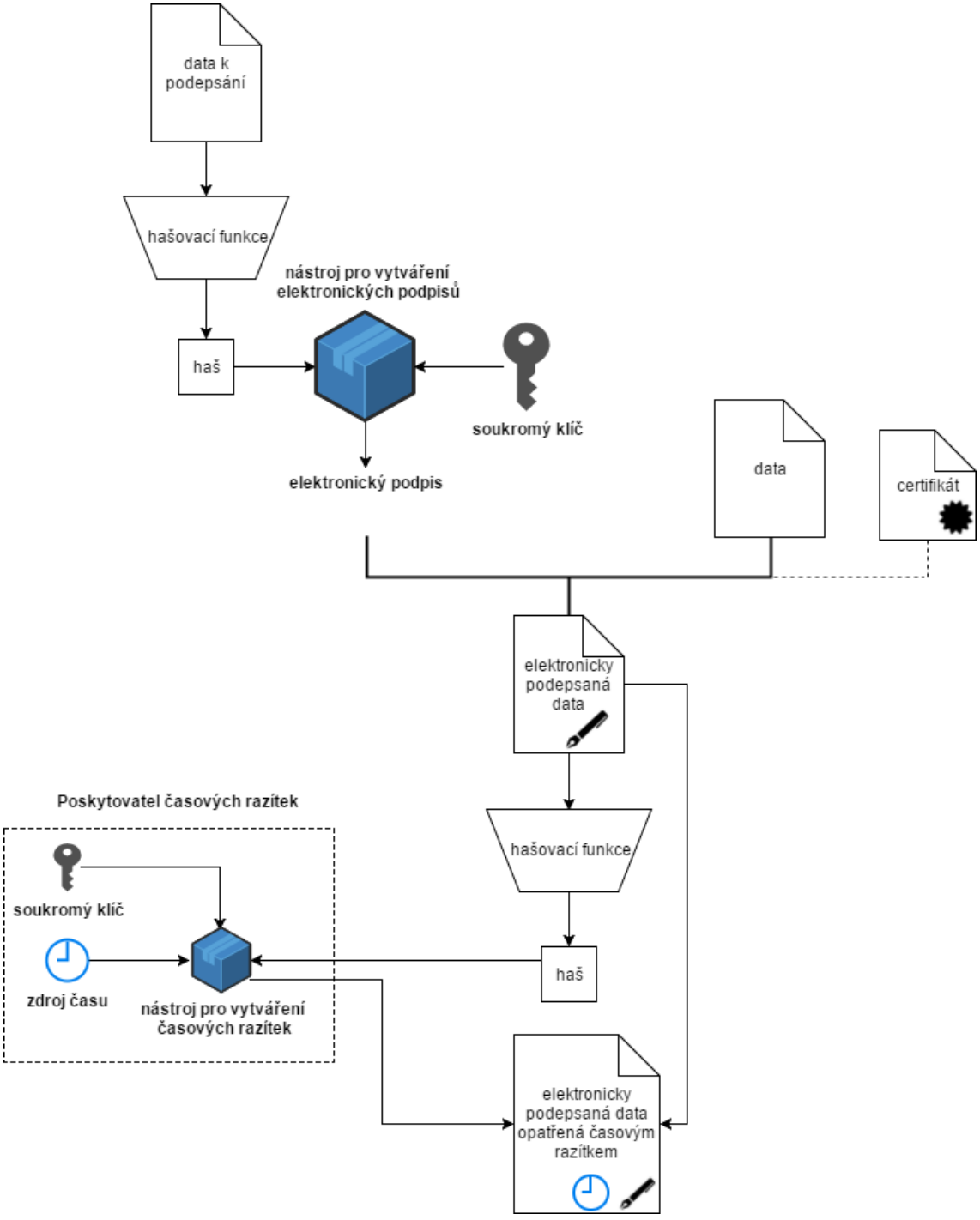
který poskytovatel při tvorbě používá. V *odpovědi* je pak status, zda časové razítko bylo přiděleno (případně informace o chybě) a časové razítko. Časové razítko se skládá z verze, politiky, podle které bylo přiděleno, haše, sériového čísla a času přidělení razítka. Mezi nepovinnými atributy pak například může být certifikát, který byl použit k vytvoření pečeti.

Jak bylo řečeno, využívá se stejné technologie jako u elektronických podpisů. Časové razítko proto například zajišťuje i integritu dokumentu, který fixuje v čase. Kdyby došlo k jakékoliv změně dat nebo k jejich neúmyslnému poškození, haš v časovém razítku by nesouhlasil.

Oproti elektronickému podpisu vyžaduje tvorba časového razítka přístup k internetu, protože uživatel, který chce dokument opatřit časovým razítkem, musí být schopen poskytovateli časových razítek poslat haš dokumentu a ten mu naopak musí v co nejkratším čase razítko vytvořit a poslat zpátky. Dalším rozdílem je, že za časová razítka se většinou neplatí jednorázově jako za certifikáty, kterými pak můžete vytvořit neomezený počet podpisů, ale průběžně, kdy je nutné platit za každé časové razítko zvlášť.

### 4.3.2 Zjednodušené schéma s časovým razítkem

Zjednodušené schéma dále rozvíjí obrázek 7. Můžeme vidět, že časové razítko potvrzuje existenci elektronického podpisu v čase. Je proto připojeno k dokumentu až po vytvoření elektronického podpisu. Na ověřování se v následující kapitole podíváme podrobněji.




Obrázek 7: Zjednodušené schéma tvorby elektronického podpisu s časovým razítkem

## 4.4 Zastarávání elektronických podpisů

V kapitole 4.2.2.3 bylo řečeno, že je zapotřebí průběžně a s předstihem posilovat použité hašovací funkce, abychom předcházeli nebezpečí, které představují kolizní dokumenty. Průběžné posilování se netýká jen hašovacích funkcí, ale i asymetrických šifrovacích algoritmů. Bezpečnost asymetrických šifer, jak jsme si uvedli v kapitole 4.1, je založena na předpokladu omezeného výpočetního výkonu, kterého lze v dané době dosáhnout. Růst výkonu, jak potvrzuje *Mooreův zákon*, je exponenciální. S rostoucím výpočetním výkonem a s objevy v oblasti kryptoanalýzy se zkracuje i doba potřebná k prolomení šifer. Je proto zapotřebí průběžně používat nové a silnější šifry. Posílení hašovacích i šifrovacích algoritmů lze aplikovat pouze u nových podpisů. Stávající elektronické podpisy není možné zpětně změnit a posílit.

Průběžné posilování se řeší na základě uměle navozeného *časového omezení*. K tomu je využita doba platnosti certifikátu, na kterém je elektronický podpis založen. Po uplynutí doby platnosti se již není možné spoléhat na informace, které certifikát stvrzuje a je zapotřebí si nechat vystavit certifikát nový. Elektronické podpisy, které byly s pomocí takového certifikátu vytvořeny, nepřestávající s jeho expirací platit. A to z důvodu, že elektronický podpis připojený k elektronickému dokument, který zakládá právní úkon, může mít důsledky, které nemusí být omezeny v čase. Nemohli bychom uzavírat smlouvy na dobu delší, než je doba platnosti certifikátu. Právní systém nezná nic jako *zastarávání podpisů* a jejich omezení v čase. Neomezujeme tak platnost elektronického podpisu, ale dobu, kdy je možné platnost elektronického podpisu ověřit. **Platnost** a **možnost ověřit platnost jsou dvě nezávislé věci**. To, že přijdeme o možnost ověření platnosti podpisu, neznamená, že platný není (a ani, že platný je). Můžeme pouze říci, že to nevíme.

Průběžné posilování hašovací a šifrovacích algoritmů není jediným důvodem, proč bylo zavedeno časové omezení:

- Pokud je uživateli zcizen podpisový klíč, tak je výrazně omezena doba jeho zneužitelnosti. Pokud by platnost neexistovala nebo byla příliš dlouhá, je poměrně velká šance, že se uživateli klíč „někde zatoulá“, zapomene na něj a jeho zcizení ani nezaznamená.

- Čím déle jakýkoliv soubor existuje, tím je pravděpodobnější, že bude rozkopírován na různá, a ne vždy bezpečná místa. To je u soukromých klíčů velmi nežádoucí.

- Je zapotřebí, aby informace v certifikátu byly čas od času přezkoumány a zůstaly co nejaktuálnější. Důvody jsou stejné jako například u cestovního pasu.

- Bez časového omezení by bylo velmi obtížné donutit uživatele k výměně starého certifikátu za nový. Platnost certifikátu velmi usnadňuje aktualizaci bezpečnostních standardů. Navíc je predikovatelná, protože uživatel zná dobu expirace svého certifikátu.

- Intervalové revokační seznamy, které pokrývají jen určitý časový interval, by ve své podobě neexistovaly a časem by byly velmi objemné.

U tuzemských certifikačních autorit je doba platnosti kvalifikovaných certifikátů jeden rok. U certifikátů, na kterých jsou založena časová razítka, to bývají roky čtyři. Dále platí, že čím výše jsme v hierarchii, tím delší platnost certifikáty mají. Kořenový certifikát PostSignum (PostSignum Root QCA 2) má platnost 15 let a certifikát podřízené autority (PostSignum Qualified QCA 2), která vydává kvalifikované certifikáty konečným zákazníkům, má platnost 10 let. Kořenové certifikáty mají výrazně delší platnost, protože by bylo nepraktické stále měnit vrcholové certifikáty. Jsou však podle toho chráněny (speciální hardware, dobře fyzicky chráněné umístění, ...).

## 4.5 Ověřování elektronických podpisů

Nyní se podíváme na to, jak se elektronické podpisy ověřují a prokazuje se jejich platnost. Ověřování a vyhodnocování platnosti je velmi složitou problematikou, která má technické i právní aspekty. Na začátku si ještě připomeňme, že ověření platnosti a samotná platnost jsou dvě nezávislé věci. Elektronický podpis může být stále platný, ale schopnost platnost ověřit už mít nemusíme. Ověření může skončit třemi způsoby:

1. Elektronický podpis je platný: jsme schopni ověřit a prokázat platnost podpisu.

2. Elektronický podpis je neplatný: jsme schopni ověřit a prokázat neplatnost podpisu.

3. Nevíme: nejsme schopni ověřit a prokázat platnost, nebo neplatnost podpisu.

Při ověřování musíme brát v potaz tzv. *posuzovaný okamžik*, tedy k jakému časovému okamžiku budeme platnost podpisu posuzovat. Pokud budeme posuzovat platnost k různým časovým okamžikům, můžeme obdržet různé výsledky. Například pokud má certifikát platnost do 1.7.2017 a my zvolíme jako posuzovaný okamžik 1.6.2017 a všechny bezpečnostní prvky jsou v pořádku, můžeme říci, že je elektronický podpis na něm založený platný. Pokud však jako posuzovaný okamžik zvolíme 1.8.2017, pak už můžeme pouze konstatovat, že to nejsme schopni rozhodnout. Pokud chceme provádět ověřování elektronického podpisu dle zákona, nemůžeme si vybrat posuzovaný okamžik podle toho, jak se nám to „hodí“, ale musíme vycházet z přesně daného postupu.

Pokud je podepsaný dokument fixován časovým razítkem, tak se za posuzovaný okamžik považuje čas uvedený v časovém razítku, protože podpis v té době již prokazatelně existoval. V případě existence více elektronických časových razítek pak uvažujeme čas připojení nejstaršího z nich. Pokud podepsaný dokument není opatřen časovým razítkem, který by jej fixoval v čase, pak za posuzovaný okamžik považujeme čas doručení dokumentu. V případě, že dokument

není opatřen časovým razítkem a neznáme čas doručení, posuzujeme platnost k aktuálnímu okamžiku. Ve chvíli, kdy víme, k jakému času budeme dokument posuzovat, můžeme přejít k samotnému ověřování.

### 4.5.1 Kontrola integrity

Kontrola integrity nám říká, zda došlo nebo nedošlo ke změně dat po jejich elektronickém podepsání. Pro tuto kontrolu je zapotřebí:

1. Vypočítat haš podepsaných dat, a to za pomocí stejného algoritmu, kterým spočítal haš podepisující.
2. Dešifrovat hodnotu elektronického podpisu pomocí veřejného klíče s využitím stejného algoritmu, který byl použit k šifrování a získaný haš porovnat s vypočteným hašem podepsaných dat.

Je-li integrita porušena, nebudou se námi vypočítaný a dešifrovaný haš shodovat. Pak můžeme rovnou konstatovat, že je podpis neplatný. Pokud se haše shodují, integrita nebyla porušena, ale nemůžeme zatím říci, že je podpis platný a přecházíme k dalšímu kroku.

### 4.5.2 Kontrola platnosti certifikátu

Kontrola platnosti certifikátu nám říká, zda byl certifikát, na kterém je podpis založen, k posuzovanému okamžiku platný. Tedy zda jsme ve chvíli, kdy jsme vytvářeli podpis na základě tohoto certifikátu, mohli vytvořit platný podpis. Kontrola zahrnuje:

1. Sestavení platné certifikační cesty posuzovaného certifikátu.
2. Ověření, zda okamžik podpisu spadá do intervalu platnosti certifikátu. Vycházíme z posuzovaného okamžiku.
3. Ověření platnosti elektronické pečeti, kterou vydavatel certifikát opatřil.
4. Ověření, zda certifikát nebyl k posuzovanému okamžiku revokován (pomocí CRL nebo OCSP).
5. Ověření platnosti elektronické pečeti, kterou je opatřen seznam zneplatněných certifikátů (CRL) nebo odpověď OCSP.
6. Stejným způsobem musí být ověřena platnost nadřazených certifikátů v rámci celé certifikační cesty.

V případě, že již uplynula doba platnosti certifikátu a podepsaný dokument nebyl nijak fixován v čase, nedokážeme ověřit, zda okamžik podpisu spadá do platnosti certifikátu a ten je tak platný, nebo neplatný. Jelikož jsou v České republice kvalifikované certifikáty, které jediné mohou být použity k podpisu

elektronických dokumentů (viz 4.2.10), vydávány pouze na dobu 1 roku (viz 4.4), ztrácíme nejpozději do 1 roku od vzniku podpisu možnost ověřit platnost podpisu, který není doplněn o časové razítko. Může to být i mnohem kratší doba, záleží na tom, kdy byl vystaven certifikát, který jsme k podpisu použili. Naše neschopnost prokázat platnost nás neopravňuje tvrdit, že zkoumaný podpis je neplatný.

Dále je třeba vzít v potaz, jestli nedošlo k zneplatnění certifikátu certifikační autoritou (viz CRL nebo OCSP v kapitole 4.2.9.5). To se nejčastěji stane, pokud je kompromitován soukromý klíč a uživatel požádá certifikační autoritu o revokaci. V případě, že byl k posuzovanému okamžiku certifikát revokován, je elektronický podpis neplatný. Pokud nebyl podpis fixován v čase, pak i když došlo k revokaci až po jeho vzniku, musíme podpis považovat za neplatný, protože nevíme, kdy vznikl. Jestli před, nebo až po revokaci.

Pokud je po technické stránce elektronický podpis platný, začneme vyhodnocovat stránku legislativní. Jestliže není elektronický podpis založen na kvalifikovaném certifikátu (kontrolujeme proti TSL a ověřujeme, zda obsahuje všechny zákonem stanovené náležitosti), ale na certifikátu, který si někdo sám vygeneroval, můžeme se na něj i přes technickou platnost v kupní smlouvě na nemovitost jen těžko spoléhat.

Výše popsaný postup vychází z metodického návodu Ministerstva vnitra České republiky [6], který jsem zjednodušil pro potřeby objasnění problematiky ověřování podpisů. Čtenáře, kterého zajímají všechny legislativní i technické postupy, které je potřeba splnit, aby v souladu s českou legislativou mohl o elektronickém podpisu prohlásit, že se jedná o nejvyšší a nejdůvěryhodnější typ (tzv. *uznávaný elektronický podpis*, podrobněji v kapitole 5), na něj odkazuji, protože je to dle mého názoru velmi kvalitně zpracovaný materiál. Na závěr chci ještě čtenáře upozornit, že se jedná o obecný pohled na ověřování elektronických podpisů, který není závislý na konkrétním formátu.

## 4.6 Dlouhodobě ověřitelný elektronický podpis

Dosud jsme pracovali s předpokladem, že s plynutím času ztrácíme schopnost ověřit platnost elektronického podpisu. Připomeňme si, že toto časové omezení je způsobeno uměle omezenou platností certifikátů, na kterých jsou elektronické podpisy založeny. Důvody jsou podrobně rozebrány v kapitole 4.4. Z legislativního pohledu však podpis neztrácí v průběhu času svou platnost a právní systém nezná u podpisů pojem *zastarávání*.

Část řešení je postavena na myšlence zafixování původního dokumentu a podpisu v čase. K tomu se používá časové razítko, které se připojí k podepsanému dokumentu dříve, než skončí platnost certifikátu, na kterém je podpis založen. Pokud bychom promeškali nejzazší možný okamžik pro přidání časového razítka, pak nám pozdější přidání už nebude nic platné. Nepůjde totiž ověřit, že je elektronický podpis připojený k dokumentu platný. Byl by totiž fixován až k okamžiku, kdy certifikát, na kterém byl založen, už nebyl platný. Nejlepší je připojit ča-

sové razítko k dokumentu co nejdříve po jeho podepsání. V budoucnu pak může ověřující strana rozhodovat o platnosti podpisu k tomuto okamžiku, protože ví, že podpis v této době již existoval. A nebude za *posuzovaný okamžik* považovat například až aktuální čas kdy probíhá ověření, ve kterém mohou mít certifikáty už dávno vypršenou řádnou dobu platnosti nebo být dokonce revokovány.

Připojovat časová razítka musíme opakovaně, protože i časové razítko je založeno na certifikátu s omezenou platností. Tomuto procesu říkáme *přerazítkování*. Přerazítkováním můžeme průběžně reagovat na zastarávání kryptografických algoritmů a využívat nové, silnější šifry a hašovací funkce.

V praxi však narážíme na další problémy. Správně aplikovaná posloupnost časových razítek nám sice fixuje dokument v čase a zajišťuje, že se od dané chvíle nezměnil, ale integrita podepsaného dokumentu nám nestačí k tomu, abychom mohli spolehlivě ověřit platnost podpisu (viz předchozí kapitola 4.5). K ověření platnosti jsou zapotřebí i další informace:

- Certifikát, na kterém je podpis založen.
- Všechny nadřazené certifikáty v certifikační cestě.
- Revokační informace o všech certifikátech.
- Certifikáty, na kterých jsou založeny elektronické pečeti, které pečetí CRL nebo OCSP odpovědi.

Největší problém způsobují informace o revokaci, ať už v podobě CRL nebo OCSP odpovědí. Pokud k ověřování dochází až po delší době od vzniku podpisu, nemusí být tyto informace již k dispozici. Například u intervalových CRL, o kterých jsme se zmiňovali v kapitole 4.2.9.5, jsou tyto informace nedostupné ihned poté, co skončí řádná platnost certifikátu. Dají se sice získat i jinými způsoby (obvykle z archivu dané certifikační autority), ale také jen po určité časové období. A co budeme dělat například za 100 let?

Řešením je k podepsanému dokumentu přibalit všechny informace potřebné k pozdějšímu ověření. Tomuto řešení se říká *Long Term Validation* (LTV), česky *dlouhodobé ověření*. Díky tomu můžeme platnost elektronických podpisů ověřovat i desítky let poté, co podpisy vznikly, což je velmi důležité pro digitální kontinuitu. Pro praktickou implementaci LTV je zapotřebí standardizovaný a jednotný formát, který všechny potřebné informace důvěryhodně a spolehlivě pojme, aby pak tyto informace mohly být použity k pozdějšímu ověření. A především, aby ověření splnilo všechny požadavky kladené zákony. eIDAS definuje tři referenční formáty, které specifikuje a spravuje Evropský institut pro telekomunikační standardy:

1. CAdES (*CMS Advanced Electronic Signatures*): elektronický podpis umožňující podepsat jakákoliv data. Je reprezentován binárně.
2. XAdES (*XML Advanced Electronic Signatures*): elektronický podpis umožňující podepsat jakákoliv data. Je reprezentován značkovacím jazykem XML.

3. PAdES (*PDF Advanced Electronic Signatures*): elektronický podpis umožňující podepsat dokumenty ve formátu PDF. Je založen na formátu CAdES.

Každý formát je ještě odstupňován podle toho, co a jak je k samotnému podpisu přibaleno. Základní úroveň je klasicky elektronický podpis, o kterém jsme mluvili doteď. Vyšší úrovně pak přibalují časová razítka, certifikáty z certifikační cesty, informace o revokaci a další informace:

1. Základní podpis (*Basic Signature*): elektronický podpis bez fixace v čase. Jeho platnost lze ověřit do té doby, dokud korespondující certifikáty nejsou revokovány, nebo nevypršela jejich platnost.

2. Podpis s časem (*Signature with Time*): elektronický podpis s fixací v čase pomocí časového razítka. Jeho platnost lze ověřit, i když korespondující certifikáty byly revokovány, pokud byly revokovány až poté, co byl podpis fixován v čase. Lze ověřit platnost i po vypršení platnosti certifikátů.

3. Podpis s možností dlouhodobého ověření (*Signature with Long-Term Validation Material*): elektronický podpis, ke kterému jsou začleněny všechny validační materiály (certifikáty, CRL, OCSP odpovědi) nebo odkazy na tyto materiály, potřebné pro ověření platnosti podpisu.

4. Podpis s možností dlouhodobého ověření se zajištěním integrity validačních materiálů (*Signature providing Long Term Availability and Integrity of Validation Material*): cílí na dlouhodobou dostupnost a integritu validačních materiálů elektronického podpisu pro potřeby dlouhodobého ověření a umožňuje ověřit platnost i v případě událostí jako je použití slabých kryptografických algoritmů nebo vypršení platnosti validačních materiálů.

Všechny tři formáty splňují standard AdES (Advanced Electronic Signature) a poskytují tak několik záruk:

1. Jsou spojeny s daty takovým způsobem, že detekujeme jakoukoliv změnu.

2. Jsou jednoznačně spojeny s podepisujícím a jsme schopni identifikovat osobu, které podpis patří.

3. Podepisující má výhradní kontrolu nad tvorbou podpisu.

Jak si můžeme všimnout, záruky popisované standardem AdES kopírují záruky pro elektronický podpis, které jsme si definovali v kapitole 4.2. Standard AdES totiž popisuje „klasický“ elektronický podpis, se kterým se můžeme běžně setkat, a o kterém jsme dosud mluvili. Nařízení eIDAS však definuje jasné požadavky, které musí formát podpisu patřící do tohoto standardu splňovat. V kapitole 4.2 jsme si řekli, že se takový „klasický“ elektronický podpis dle české legislativy nazývá *zaručený*. Jedná se o nepříliš šťastný překlad slovního spojení *Advanced*

*Electronic Signature*, který je často kritizován [7], ale je v rámci české legislativy používán již dlouho. Jako lepší překlad se často uvádí *pokročilý elektronický podpis*. Čtenář by měl mít na paměti, že se může v nejrůznější literatuře setkat se zaměňováním pojmů *elektronický podpis*, *zaručený elektronický podpis*, *pokročilý elektronický podpis* nebo dokonce *digitální elektronický podpis*. Všechny tyto pojmy odkazují na elektronický podpis, který je založený na asymetrické kryptografii a infrastruktuře veřejného klíče (PKI). My pro potřeby této práce budeme nadále používat pojem *elektronický podpis*, protože máme objasněno, jaký elektronický podpis máme na mysli.

Nyní již upusťme od obecného popisu elektronického podpisu a pojďme se podívat na konkrétní formáty elektronického podpisu, které splňují standard AdES a eIDAS je předkládá jako referenční formáty. Proč referenční? Jednotlivé členské státy totiž mohou pro přeshraniční transakce implementovat i své vlastní formáty elektronického podpisu, ale ty musí splňovat stejné požadavky jako standardy referenční a zároveň by bylo nutné vybudovat k neomezenému a bezplatnému použití aplikaci, která umožní okamžité ověření takového elektronického podpisu a je přístupná po internetové síti.[8]

## 4.7 XML Advanced Electronic Signatures (XAdES)

XAdES (XML Advanced Electronic Signatures) je formát elektronického podpisu definovaný v normě *ETSI EN 319 132-1* [9]. Je postaven na technologii PKI a digitálních certifikátech.

Jedná se o sadu rozšíření a omezení standardu XML-DSig (XML Digital Signature), který definuje elektronické podpisy reprezentované pomocí značkovacího jazyka XML. Zatímco XML-DSig je obecný standard pro podepisování elektronických dokumentů, XAdES definuje přesné schéma elektronického podpisu, které je kompatibilní s nařízením eIDAS.

### 4.7.1 XML Digital Signature (XML-DSig)

XML-DSig je standardem [10] konsorcia W3C[13] a popisuje syntaxi a zpracování elektronického podpisu, který je postaven na značkovacím jazyce XML. Standard popisuje XML strukturu, kterou lze podepsat libovolná data. A to jednotlivě i hromadně s využitím jediného elektronického podpisu.

#### 4.7.1.1 Struktura podpisu

Struktura elektronického podpisu vypadá následovně:

```
<Signature ID?>
   <SignedInfo ID?>
      <CanonicalizationMethod Algorithm/>
      <SignatureMethod Algorithm/>
      (<Reference ID? URI? Type?>
         (<Transforms Algorithm>)?
         <DigestMethod Algorithm>
         <DigestValue>
      </Reference>)+
   </SignedInfo>
   <SignatureValue ID?>
   (<KeyInfo ID?>)?
   (<Object ID? MimeType? Encoding?>)*
</Signature>
```

Elementy a atributy bez označení se musí vyskytnout právě jednou. Symbol „?“ za elementem a atributem značí, že nemusí být přítomen, ale pokud je, tak maximálně jednou. Symbol „+“ za element značí, že musí být přítomen alespoň jednou. Symbol „*“ značí, že element nemusí být přítomen, ale pokud je, může být přítomen i opakovaně.

[13] Mezinárodní sdružení, jehož hlavním úkolem je dohlížet na vývoj internetových standardů. Zabývá se především vysokoúrovňovými internetovými protokoly.

Každý element má svůj význam:

1. Signature: kořenový element elektronického podpisu. Atribut *ID* slouží k identifikaci konkrétního podpisu, pokud jich existuje v rámci podepisovaných dat několik.

2. SignedInfo: element, který je kryptograficky podepsán. Obsahuje nebo odkazuje na podepsaná data a specifikuje použité algoritmy. Atribut *ID* slouží k tomu, aby na tento podpis mohly odkazovat jiné podpisy.

   (a) CanonicalizationMethod: element popisující použitý kanonizační algoritmus. XML je jednoznačně transformováno na jednu zvolenou reprezentaci. Bez kanonizace by mohla podepisující a ověřující strana vypočítat odlišné haše[14]. Atribut *Algorithm* specifikuje použitý algoritmus.

   (b) SignatureMethod: algoritmus použitý k vytvoření a pro ověření podpisu. Atribut *Algorithm* specifikuje použitý algoritmus (např. RSA-SHA256).

   (c) Reference: jedna nebo více referencí jednoznačně identifikující data, která podepisujeme. Může se jednat o aktuální XML dokument, jeho část nebo externí zdroj identifikovaný pomocí URI. Atribut *ID* slouží k identifikaci konkrétní reference, pokud jich existuje několik. Atribut *URI* odkazuje na příslušná data a *Type* popisuje, jakého typu data jsou.

      i. Transforms: transformace aplikované na data před výpočtem haše. Transformací může být XPath[15], který vybírá jen tu část dat, kterou chceme podepsat. Atribut *Algorithm* specifikuje použitý algoritmus.

      ii. DigestMethod: použitý hašovací algoritmus. Atribut *Algorithm* specifikuje použitý algoritmus (např. SHA256).

      iii. DigestValue: vypočítaný haš. Jedná se o výstup hašovací funkce, která byla aplikována na transformovaná data. Haš je zakódován v Base64.

3. SignatureValue: hodnota elektronického podpisu vypočítaná z elementu *SignedInfo* pomocí algoritmu z elementu *SignatureMethod* z dat kanonizovaných pomocí algoritmu z elementu *CanonicalizationMethod*. *SignedInfo* obsahuje elementy *Reference*, což jsou reference na podepsaná data včetně jejich hašů. Změna dokonce i jediného bitu v tomto řetězci způsobí, že

[14] XML dává po stránce syntaktického zápisu poměrně velkou volnost. Pořadí atributů nebo použité uvozovky nehrají roli. Například „<a foo='yes' boo='no'/>“ a „<a boo="no" foo='yes'></a>“ je z pohledu softwaru pracujícího s XML ekvivalentní. Vypočtený haš by se však u podepisující a ověřující strany lišil. Data by mohla být považována za změněná i když změněná nebyla, protože by je algoritmy XML zpracovaly odlišným způsobem.

[15] Jazyk, pomocí kterého lze adresovat části XML dokumentu.

podpis nebude považován za validní, protože bude porušena integrita elektronického podpisu. Hodnota podpisu je zakódována v Base64.

4. KeyInfo: nepovinný element, který umožňuje podepisující straně přiložit veřejný klíč pro ověření elektronického podpisu. Většinou se jedná o elektronicky podepsaný veřejný klíč uložený ve formátu X.509. Pokud element není vyplněn, musí ověřující strana získat veřejný klíč pro ověření podpisu jiným způsobem.

5. Object: nepovinný element s libovolným obsahem. Může například obsahovat časové razítko nebo podepsaná data (pak se jedná o tzv. *obalující podpis*). Atribut *ID* slouží k identifikaci konkrétního elementu *Object*, pokud jich podpis obsahuje několik. Atribut *MimeType* identifikuje formát souboru dle standardu MIME[16]. Poslední atribut *Encoding* obsahuje informaci o použitém kódování.

#### 4.7.1.2 Formy podpisu

Podpis může mít tři formy:

1. Zabalený podpis (*Enveloped Signature*): podpis je součástí podepsaných dat. Kořenový element *Signature* je potomkem elementu, který sám podepisuje. Odkazuje na něj některá z referencí, která musí obsahovat transformaci, která vyjme samotný element *Signature* z výpočtu. Opačně by nebylo možné zabalený podpis vytvořit, protože by byl jeho výstup závislý sám na sobě.

2. Obalující podpis (*Enveloping Signature*): podpis obaluje podepsaná data. Data, která se podepisují, jsou umístěna v elementu *Object*.

3. Odpojený podpis (*Detached Signature*): podpis a data, která podepisuje, jsou v samostatných souborech nebo ve stejném souboru jako sourozenecké elementy.

#### 4.7.1.3 Tvorba podpisu

Tvorba podpisu probíhá ve dvou krocích. V prvním jsou vytvořeny reference, ve druhém pak samotný podpis.

**Tvorba referencí**

Pro každý datový objekt, který budeme podepisovat:

1. Provedeme požadovanou transformaci.

2. Vypočítáme haš pomocí zvolené hašovací funkce.

[16]Dvoudílný identifikátor formátu souboru na internetu. Skládá se z typu, podtypu a jednoho čí více nepovinných parametrů. Například *application/pdf* označuje PDF dokument.

3. Vytvoříme element *Reference*, do kterého vložíme hašovací algoritmus, haš a dle potřeby další nepovinné atributy a elementy.

**Tvorba podpisu**

Jednu nebo více referencí použijeme v druhém kroku pro tvorbu elektronického podpisu:

1. Vytvoříme element *SignedInfo*, do kterého vložíme elementy *CanonicalizationMethod*, *SignatureMethod* a *Reference*. Element *Reference* se může vyskytovat vícekrát, pokud podepisujeme více datových objektů.

2. Kanonizujeme a spočítáme hodnotu elektronického podpisu a hodnotu vložíme do elementu *SignatureValue*.

3. Vytvoříme element *Signature*, do kterého vložíme *SignedInfo*, *SignatureValue* a dle potřeby další nepovinné atributy a elementy.

#### 4.7.1.4 Ověření podpisu

Ověření podpisu probíhá ve dvou krocích. V prvním jsou ověřeny reference, ve druhém pak samotný podpis.

**Ověření referencí**

1. Element *SignedInfo* kanonizujeme algoritmem uvedeným v elementu *CanonicalizationMethod*.

2. Pro každou referenci v *SignedInfo*:

   (a) Dereferencujeme data, na která reference odkazuje. Následně aplikujeme, pokud existují, transformace uvedené v elementu *Transforms*.

   (b) Vypočítáme haš pomocí hašovací funkce uvedeného v elementu *DigestMethod*.

   (c) Haš se srovná s hodnotou v elementu *DigestValue*. Pokud se hodnoty shodují, pak nebyla porušena integrita a reference je považována za platnou.

**Ověření podpisu**

1. Dohledáme veřejný klíč, který může být uložen v elementu *KeyInfo*, případně jej musíme získat jiným způsobem.

2. Spočítáme hodnotu elektronického podpisu z kanonizovaného elementu *SignedInfo* na základě algoritmu specifikovaného v elementu *SignatureMethod*. Tu pak srovnáme s hodnotou elementu *SignatureValue*, která byla dešifrována veřejným klíčem.

Pokud jsou všechny reference úspěšně ověřeny a je úspěšně ověřen i samotný podpis, je podpis formátu XML-DSig považován za platný. V opačném případně je považován za neplatný.

Zde popsané ověření je kontrolou integrity, která je obecně popsána v kapitole 4.5.1. Pokud by však měl mít podpis i právní váhu bylo by následně zapotřebí provést kontrolu platnosti certifikátu (viz kapitola 4.5.2). Kontrola platnosti certifikátu je nezávislá na formátu elektronického podpisu, protože probíhá vždy nad certifikátem a pracuje s jeho atributy. Jediným rozdílem je maximálně načtení certifikátu ze struktury elektronického podpisu pro potřeby ověření. Čtenář by měl mít od této chvíle na paměti, že toto bude platit u všech formátů, které si představíme.

#### Manifest

Zajímavý element, který si v rámci XML-DSig ještě představíme, je *Manifest*, který se ve výše popsané struktuře nenachází, ale obvykle bychom ho našli uvnitř některého z elementů *Object*. *Manifest* použijeme ve chvíli, kdy předpokládáme, že některá externí data, která chceme podepsat, mohou být v budoucnu smazána. Stejně jako *SignedInfo* obsahuje jednu nebo více referencí na data, která chceme podepsat a haše těchto dat. Některá reference elementu *SignedInfo* pak odkazuje na *Manifest* a jako haš má spočítaný element *Manifest*, ne samotná data, na která *Manifest* odkazuje. Pokud jsou některá data, na která *Manifest* odkazuje, smazána, nic se nestane, protože jeho haš zůstává stejný. A zůstává platný i podpis. Pokud by byla stejná data referencována přímo ze *SignedInfo*, tak by jejich nedostupnost způsobila neplatnost celého podpisu. *SignedInfo* tedy data podepisuje nepřímo.

### 4.7.2 Výhody XAdES oproti XML-DSig

Standard XML-DSig neříká, jakým způsobem bude identifikována podepisující strana, nedefinuje bezpečnostní politiku, neobsahuje podrobnější metadata a nepodporuje možnost dlouhodobého ověření bezpečnostních prvků. Formát XAdES adresuje nedostatky XML-DSigu následovně:

- Určuje, jak bude identifikována podepisující strana. U elektronického podpisu je téměř vždy zapotřebí znát identitu podepisujícího. Bez identity může být elektronický podpis použit pouze k ověření integrity. XML-DSig umožňuje certifikát přiložit do elementu *SignedInfo*, ale nepožaduje, aby tato informace byla podepsána (a tím pádem zabezpečena). XAdES toto požaduje a k identifikaci se používají certifikáty ve formátu X.509.
- Definuje bezpečnostní politiku například tím, že omezuje přípustné kryptografické algoritmy.
- Obsahuje metadata podepsaného datového objektu a jasně určuje, jak mají být použita.

- Podporuje dlouhodobou archivaci (LTV), tedy možnost dlouhodobého ověření bezpečnostních prvků.

XML-DSig řeší některé nedostatky volitelným elementem *SignatureProperties*[17], který slouží k uložení libovolných metadat, ale XAdES k řešení nedostatků přistupuje systematicky. XML-DSig rozšiřuje o tzv. *kvalifikované vlastnosti*. Což jsou metadata daného elektronického podpisu. Dále definuje čtyři úrovně elektronického podpisu a jasně určuje, které *kvalifikované vlastnosti* mají být přítomny pro splnění příslušné úrovně. Rozdělení na čtyři úrovně jsme si už přiblížili v kapitole 4.6. Pro tento účel je definováno nové XML schéma popisující, jak mají být *kvalifikované vlastnosti* sestaveny a zapojeny do základního XML-DSig podpisu.

### 4.7.3 Kvalifikované vlastnosti a struktura

Elektronický podpis ve formátu XAdES rozšiřuje XML-DSig o *kvalifikované vlastnosti* (anglicky *qualifying properties* nebo *QP*), dále *vlastnosti*. Jedná se o sadu metadat, která jsou uložena v nově definovaných elementech. Do podpisu můžeme vložit například identitu podepisující strany, revokační informace nebo časové razítko. Vlastnosti jsou rozděleny na:

- Podepsané vlastnosti (*Signed Properties*): skupina vlastností, která **je** podepsána stejným podpisem společně s podepisovanými daty. *Podepsané vlastnosti* se dále dělí na *podepsané vlastnosti podpisu* (*Signed Signature Properties*) a *podepsané vlastnosti datových objektů* (*Signed Data Object Properties*). Podpis je chrání proti změně.

- Nepodepsané vlastnosti (*Unsigned Properties*): skupina vlastností, která **není** podepsána stejným podpisem společně s podepisovanými daty. *Nepodepsané vlastnosti* mohou vkládat a podepsat jiné subjekty, které pracují s již existujícím podpisem. Kdyby nově přidané vlastnosti nebyly podepsány, hrozilo by jejich podvržení. *Nepodepsané vlastnosti* se dále dělí na *nepodepsané vlastnosti podpisu* (*Unsigned Signature Properties*) a *nepodepsané vlastnosti datových objektů* (*Unsigned Data Object Properties*). V současné verzi standardu nejsou *nepodepsané vlastnosti datových objektů* specifikovány, proto je nebudeme dále uvažovat.

#### Struktura

XAdES schéma je vloženo do elementu *Object* v původním XML-DSigu. To umožňuje, aby byl do jisté míry interoperabilní s již existujícími nástroji, které pracují s XML-DSigem. Může být ověřován jako XML-DSig podpis, avšak přichází se tím o výhody, které přináší, protože nástroje, které umí jen pracovat s XML-DSigem nedokáží zpracovat rozšiřující informace, jako jsou například přiložené revokační seznamy nebo časová razítka.

Struktura podpisu ve formátu XAdES vypadá následovně:

[17] SignatureProperties je případně umístěn v elementu *Object*.

```
<ds:Signature ID?>
   <ds:SignedInfo ID?>
     <ds:CanonicalizationMethod Algorithm/>
     <ds:SignatureMethod Algorithm/>
     (<ds:Reference ID? URI? Type?>
          (<ds:Transforms Algorithm>)?
          <ds:DigestMethod Algorithm>
          <ds:DigestValue>
     </ds:Reference>)+
   </ds:SignedInfo>
   <ds:SignatureValue ID?>
   (<ds:KeyInfo ID?>)?
   (<ds:Object ID? MimeType? Encoding?>
     <xades:QualifyingProperties>
          <xades:SignedProperties>
            <xades:SignedSignatureProperties/>
            <xades:SignedDataObjectProperties/>
          </xades:SignedProperties>
          <xades:UnsignedProperties>
            <xades:UnsignedSignatureProperties/>
          </xades:UnsignedProperties>
     </xades:QualifyingProperties>
   </ds:Object>)*
</ds:Signature>
```

Vlastnosti jsou vkládány do elementu *xades:QualifyingProperties*. Elementy vnořené do elementu *xades:SignedProperties* představují *podepsané vlastnosti*. Jsou referencovány z XML-DSig podpisu, aby byly podepsány, musí být proto vytvořeny dříve, než je podpis vygenerován. Naopak elementy vnořené v elementu *xades:UnsignedProperties* představují *nepodepsané vlastnosti* a nejsou kryty podpisem, takže mohou být k podpisu přidány i po vygenerování podpisu, aniž by narušily jeho integritu. Přidat je může třetí strana, která s podpisem pracuje a bez účasti toho, kdo podpis vytvořil.

Úroveň určuje, které vlastnosti jsou povinné, nepovinné nebo zakázané. Podpis formátu XAdES, který chce splňovat příslušnou úroveň, musí tyto požadavky respektovat. Vlastnosti mohou být součástí stejného XML dokumentu nebo se mohou nacházet ve stejném XML dokumentu mimo tělo podpisu (sourozenecké elementy), nebo ve zcela jiném souboru a být odkazovány nepřímo pomocí URI.

Jak bylo uvedeno na začátku kapitoly 4.7.3, podepsané a nepodepsané vlastnosti se dále dělí. V rámci těchto elementů se již nachází samotná metadata.

#### 4.7.3.1 Podepsané vlastnosti podpisu

Rozšiřují původní XML-DSig informacemi o podpisu:

- Čas vytvoření podpisu (*xades:SigningTime*): čas pochází ze systémových

hodin zařízení, na kterém byl podpis vytvořen.

- Podpisový certifikát (*xades:SigningCertificateV2*): certifikát, který byl použit k vytvoření podpisu a případně další certifikáty v rámci certifikační cesty. Certifikát použitý k podpisu je povinný, zbylé certifikáty jsou volitelné.

- Podpisová politika (*xades:SignaturePolicyIdentifier*): sada pravidel pro vytváření a ověřování podpisu. Podepisující strana na základě nich podpis vytváří a ověřující strana ověřuje. Pokud je při ověřování zjištěno porušení pravidel dané politiky, nebo se politiku nepodaří identifikovat, je podpis neplatný i přesto, že by bez ní platný byl.

- Místo podpisu (*xades:SignatureProductionPlaceV2*): fyzické místo, o kterém podepisující strana tvrdí, že se v něm ve chvíli podpisu nacházela.

- Role podepisujícího (*xades:SignerRoleV2*): například podle zastávané pozice v organizaci, ve které podpis vzniká.

#### 4.7.3.2 Podepsané vlastnosti dat

Rozšiřují původní XML-DSig informacemi o podepsaných datech:

- Formát dat (*xades:DataObjectFormat*): metadata podepisovaných dat. Formát dat dle standardu MIME, informace o kódování a slovní popis.

- Typ závazku (*xades:CommitmentTypeIndication*): závazky, které vyplývají podepisující straně z vytvoření podpisu a za které přijímá zodpovědnost. Například že podepsaná data sama vytvořila a podepsala nebo pouze přejala a podepsala.

- Časové razítko nad všemi daty (*xades:AllDataObjectsTimeStamp*): časové razítko spočítané nad všemi podepsanými daty s výjimkou *xades:SignedProperties*, protože by jinak byl podpis závislý sám na sobě. Dokazuje, že podepsaná data vznikla před určitým časovým okamžikem.

- Časové razítko nad konkrétními daty (*xades:IndividualDataObjectsTimeStamp*).

#### 4.7.3.3 Nepodepsané vlastnosti podpisu

Vlastnosti podpisu, které nejsou pokryty původním podpisem podepisujícího:

- Úložiště podpisové politiky (*xades:SignaturePolicyStore*): místo, kde se nachází politika, která se používá v rámci vlastnosti *xades:SignaturePolicyIdentifier*. Buď formou URI nebo je přiložen samotný dokument pro ověřování off-line.

- Podpis podpisu (*xades:Countersignature*): nejedná se o spolupodpis, jak by se dle anglického názvu mohlo nabízet, ale o podpis původního podpisu, který se nachází v elementu *ds:SignatureValue*. Může se jednat o XML-DSig nebo další XAdES. Podepisující díky tomu nemůže v budoucnu přepočítat hodnotu *ds:SignatureValue*, protože by došlo k porušení integrity podpisu v *xades:Countersignature*.

- Časové razítko pro podpis (*xades:SignatureTimeStamp*): libovolné množství časových razítek, které fixují podpis.

- Kompletní seznam odkazů na všechny revokační informace (*xades:CompleteRevocationRefs*): obsahuje odkazy na revokační informace (CRL nebo OCSP odpovědi) pro certifikát použitý k podpisu a pro všechny certifikáty v rámci certifikační cesty s výjimkou kořenového certifikátu. Ten je z principu důvěryhodný. Seznam může obsahovat i odkazy na revokační informace pro certifikáty, na kterých jsou založena časová razítka (i pro všechny certifikáty na certifikační cestě) i revokační informace pro certifikáty, kterými byly podepsány CRL nebo OCSP odpovědi (i pro všechny certifikáty na certifikační cestě).

- Kompletní seznam odkazů na všechny certifikáty (*xades:CompleteCertificateRefsV2*): obsahuje odkazy na certifikáty, které se nachází v certifikační cestě podpisového certifikátu. Certifikát použitý k podpisu není zahrnut, nachází se ve vlastnosti *xades:SigningCertificateV2*. Seznam může obsahovat i odkazy na certifikáty, na kterých jsou založena časová razítka (vč. všech certifikátů na certifikační cestě) i certifikáty, kterými byly pečetěny revokační informace (vč. všech certifikátů na certifikační cestě).

- *xades:RefsOnlyTimeStampV2*: časové razítko, které mimo jiné pokrývá *xades:CompleteRevocationRefsV2* a *xades:CompleteCertificateRefsV2*.

- Všechny revokační informace (*xades:RevocationValues*): samotné revokační informace potřebné k ověření podpisu, ne pouze odkazy na ně.

- Všechny certifikáty (*xades:CertificateValues*): samotné certifikáty potřebné k ověření podpisu, ne pouze odkazy na ně.

- Archivní časové razítko (*xades:ArchiveTimeStamp*): libovolné množství časových razítek, které metodou *přerazítkování* posilují původní podpis. Pokrývají celý podpis a umožňují dlouhodobé ověření podpisu.

Jak vidíme, standard definuje mnoho vlastností, některé z nich dokonce mají i druhou verzi (např. *SigningCertificateV2*), první byla označena za *zastaralou* a neměla by se u nových podpisů používat. Tento výčet by měl čtenáři posloužit k vytvoření představy o tom, jakými způsoby XAdES zajišťuje proklamované schopnosti. Pro podrobný popis všech vlastností čtenáře odkazuji na normu *ETSI EN 319 132-1*.

### 4.7.4 XAdES Baseline Profile

XAdES definuje mnoho volitelných *vlastností*, které nesou informace o podpisu a podepisovaných datech. Z toho důvodu může být pro aplikace obtížná jeho interpretace, protože podpisy se mohou značně lišit ve vlastnostech, které mají vyplněny. Z toho důvodu ETSI zavedlo čtyři základní úrovně XAdES podpisů. Této specifikaci se říká *XAdES Baseline Profile* (česky *Výchozí XAdES Profil*) a jejím cílem je omezit volnost při vytváření podpisů ve formátu XAdES, kterou zavedla původní specifikace a usnadnit tak interoperabilitu. Podpisy vytvořené pomocí této specifikace zůstávají plnohodnotnými XAdES podpisy, a navíc jsou označovány jako *baseline conformant* (česky *vyhovující základu*). Každá vyšší úroveň splňuje všechny požadavky předchozí úrovně. Rozdělení na úrovně jsme si obecně představili v kapitole 4.6, nyní si ukážeme konkrétní rozdělení u XAdESu:

- Úroveň B-B (*B-B Level*): poskytuje základní úroveň elektronického podpisu, která definuje, jakým způsobem bude podepisující identifikován (prostřednictvím X.509 certifikátu) a zabezpečení této informace (umístění do *podepsaných vlastností*).
- Úroveň B-T (*B-T Level*): přidává časové razítko, které důvěryhodně prokazuje existenci podpisu v čase. Rozšíření o vlastnost *xades:SignatureTimeStamp*.
- Úroveň B-LT (*B-LT Level*): rozšiřuje úroveň B-T o všechny certifikáty, revokační stavy těchto certifikátů a další informace potřebné pro ověření platnosti podpisu. Cílem je umožnit dlouhodobého ověření podpisu. Rozšíření například o vlastnosti *xades:CertificateValues*, *xades:RevocationValues*.
- Úroveň B-LTA (*B-LTA Level*): rozšiřuje úroveň B-LT o archivní časové razítko, čímž vytváří archivní elektronický podpis, který je chráněn před hrozbou oslabení použitých kryptografických funkcí a před expirací nebo zneplatněním některého z certifikátů v certifikační cestě. Rozšíření například o vlastnost *xades:ArchiveTimeStamp*.

*XAdES Baseline Profile* klade na vytváření a ověřování nejrůznější požadavky:

#### Požadavky na algoritmy

Použité algoritmy a jejich parametry (např. délka klíče) musí splňovat právní požadavky daného státu, jinak nebude možné považovat elektronický podpis z legislativní pohledu za platný. Dále specifikace doporučuje množinu preferovaných algoritmů pro kanonizaci a transformaci, ale jedná se pouze o doporučení, podepisující se nimi nemusí řídit. Z algoritmů je zakázáno pouze použití hašovacího algoritmu MD5.

### Umístění vlastností

Všechny vlastnosti musí být umístěny v elementu *xades:QualifyingProperties*, který je potomkem *ds:Object*. Žádná vlastnost nesmí být umístěna externě.

Kromě těchto společných požadavků, které musí splňovat všechny profily, pak *Baseline Profile* klade poměrně mnoho požadavků na profily samotné. Jaké vlastnosti mohou a nemohou obsahovat, jakým způsobem mají být tyto vlastnosti vyplněny a kde mají být umístěny. Pro další informace o *XAdES Baseline Profile* čtenáře odkazuji na normu *ETSI EN 319 132-1, kapitola 6: XAdES baseline signatures*. XAdES kromě *základních úrovní* popsaných v *Baseline Profile* nabízí ještě *rozšířené úrovně*, které vyžadují pro splnění jiné kombinace vlastností. Pro více informací o *rozšířených úrovních* čtenáře odkazuji na normu *ETSI EN 319 132-2* [11].

## 4.8 CMS Advanced Electronic Signatures (CAdES)

CAdES (CMS Advanced Electronic Signatures) je formát elektronického podpisu definovaný v normě *ETSI EN 319 122-1* [12]. Stejně jako XAdES je postaven na technologii PKI a digitálních certifikátech.

Jedná se o sadu rozšíření a omezení standardu CMS (Cryptographic Message Syntax), který definuje elektronické podpisy reprezentované pomocí ASN.1, kódované převážně s využitím BER a částečně DER kódování. Nejčastěji má binární reprezentaci. Zatímco CMS je obecný standard pro kryptograficky chráněné zprávy, který lze použít k elektronickým podpisům, ověřování či šifrování jakýchkoliv digitálních dat, CAdES určuje přesnou ASN.1 definici a činí jej kompatibilní s nařízením eIDAS.

### 4.8.1 Cryptographic Message Syntax (CMS)

CMS je standardem organizace *Internet Engineering Task Force* (IEFT)[18]. Byl odvozen ze standardu PKCS#7 verze 1.5, se kterým se snaží zachovat zpětnou kompatibilitu. Standard PKCS#7 byl vyvinut roku 1993 v *RSA Laboratories*. Plánovaný PKCS#7 verze 1.6, který měl být vydán v roce 1997, již nebyl dokončen. Nejnovějším dokumentem popisujícím CMS je *RFC 5652* [13] z roku 2009. Dnes je CMS klíčovou kryptografickou součástí mnoha dalších kryptografických standardů jako je například S/MIME (zabezpečení elektronické pošty), PKCS#12 (formát pro uchovávání kryptografických objektů) či CAdES.

#### 4.8.1.1 Struktura podpisu

Objekty jsou v CMS jednoznačně identifikovány pomocí OID (*Object ID*, česky *identifikátor objektu*), což je globálně jednoznačný identifikátor objektu. OID je tvořeno posloupností čísel, které jsou odděleny tečkou, tvoří tak stromovou strukturu[19]. Každý uzel ve stromu je spravován autoritou, která může definovat podřízené uzly a taktéž pověřit autoritu, která tyto podřízené uzly bude spravovat. Struktura elektronického podpisu vypadá následovně:

```
ContentInfo ::= SEQUENCE {
  contentType ContentType,
  content [0] EXPLICIT ANY DEFINED BY contentType
}

SignedData ::= SEQUENCE {
  version CMSVersion,
  digestAlgorithms DigestAlgorithmIdentifiers,
  encapContentInfo SEQUENCE {
```

[18]Organizace, která vyvíjí a podporuje internetové standardy. Zabývá se především nízkoúrovňovými internetovými protokoly.

[19]Příkladem může být *1.2.840.113549.1.7.2*, což je OID pro jeden z mnoha objektů standardu PKCS#7.

```
    eContentType ContentType,
    eContent [0] EXPLICIT OCTET STRING OPTIONAL
  },
  certificates [0] IMPLICIT CertificateSet OPTIONAL,
  crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
  signerInfos SET OF SEQUENCE {
    version CMSVersion,
    sid SignerIdentifier,
    digestAlgorithm DigestAlgorithmIdentifier,
    signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF SEQUENCE {
      attrType OBJECT IDENTIFIER,
      attrValues SET OF AttributeValue
    } OPTIONAL,
    signatureAlgorithm SignatureAlgorithmIdentifier,
    signature OCTET STRING,
    unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF SEQUENCE {
      attrType OBJECT IDENTIFIER,
      attrValues SET OF AttributeValue
    } OPTIONAL
  }
}
```

**ContentInfo**

Základní objektem CMS je *ContentInfo*. Jedná se o obálku obsahující dvě pole:

1. contentType: OID, který identifikuje *typ obsahu*.
2. content: obsah.

CMS v rámci *RFC 3852* definuje šest základních *typů obsahu*, které lze aplikovat na libovolná data:

- Data (*data*): 8bitové řetězce dat. Například v kódování ASCII. Na tomto *typu obsahu* staví další *typy*.
- Podepsaná data (*signed-data*): data s žádným nebo libovolným počtem podpisů. Tomuto *typu* se jako jedinému budeme dále věnovat, protože se jedná o elektronický podpis.
- Zabalená data (*enveloped-data*): zašifrovaná data s libovolným počtem zašifrovaných šifrovacích klíčů pro jednoho nebo více příjemců.
- Hašovaná data (*digested-data*): data a haš vypočítaný z těchto dat pomocí hašovacího algoritmu.
- Zašifrovaná data (*encrypted-data*): zašifrovaná data. Oproti *enveloped-data* neobsahuje informace o příjemcích a nejsou ani přiloženy šifrovací klíče.

- Autentizovaná data (*authenticated-data*): data, jejich MAC (*Message Authentication Code*) a zašifrované autentizační klíče pro jednoho nebo více příjemců. MAC funkce je velmi podobná hašovacím funkcím, rozdíl je, že funkce je výsledkem zpracovávaných dat a navíc i klíče (*Otisk = f(text, klíč)*). Příjemce kombinací MAC a zašifrovaného autentizačního klíče ověřuje integritu původního obsahu.

Další *typy obsahu* jsou definovány v jiných RFC dokumentech. Aplikace, které chtějí splnit *RFC 5652*, musí podporovat alespoň *ContentInfo* a *ContentType*: *signed-data*, *enveloped-data* a *data*.

**SignedData**

Ukázali jsme si, že *RFC 5652* definuje šest základních *typů obsahu*. My se zaměříme na typ *signed-data*, který nás i standard CAdES, zajímá nejvíce. Obsahem objektu *SignedData* jsou libovolná data s žádným nebo libovolným počtem podpisů. Když zpráva neobsahuje žádný elektronický podpis, používá se k distribuci certifikátů nebo CRL. Objekt *SignedData* se skládá z:

1. version: verze syntaxe. Může nabývat hodnot 1 až 5. PKCS#7 používá číslo 1, CMS pak nejčastěji číslo 3. Podrobnější informace pro správný výběr verze najde čtenář v *RFC 5652*.

2. digestAlgorithms: množina identifikátorů hašovacích algoritmů použitých pro výpočet haše včetně příslušných parametrů.

3. encapContentInfo: podepisovaný obsah. Jedná se o dvojici, kterou tvoří OID identifikující *typ* podepisovaných dat a případně data samotná. Data nejsou povinná, máme tedy možnost vytvořit externí podpis.

   (a) eContentType: OID, který identifikuje *typ obsahu* podepisovaných dat.

   (b) eContent: podepisovaná data.

4. certificates: množina certifikátů, ze kterých může ověřující strana sestavit certifikační cestu až ke kořenovému certifikátu. Podepisující strana nemá povinnost vložit všechny certifikáty, které ověřující strana bude při ověřování potřebovat. Předpokládá se, že si ověřující strana bude schopna opatřit potřebné certifikáty i jiným způsobem.

5. crls: množina CRL, které se vztahují k certifikátům z pole *certificates*. Opět platí, že podepisující strana nemá povinnost vložit všechny CRL, které bude ověřující strana potřebovat. Předpokládá se, že si ověřující strana bude schopna opatřit potřebné CRL i jiným způsobem.

6. signerInfos: množina elektronických podpisů.

(a) version: verze syntaxe. V případě, že je podepisovaný certifikát identifikován *jedinečným jménem certifikační autority* a *sériovým číslem certifikátu*, pak se použije verze 1. V případě, že je podepisovaný certifikát identifikován *identifikátorem klíče subjektu*, pak se použije verze 3.

(b) sid: obsahuje identifikaci podepisující strany, přesněji jejího certifikátu. K identifikaci může být použito buď *jedinečné jméno certifikační autority* a *sériové číslo certifikátu* nebo *identifikátor klíče subjektu*.

(c) digestAlgorithm: množina identifikátorů hašovacích algoritmů použitých pro výpočet haše včetně příslušných parametrů. Haš je vypočítán buď pouze ze samotných vstupních dat, tedy z pole *eContent*, nebo ze vstupních dat a *podepsaných atributů* v poli *signedAttrs* pokud se tam nějaké nachází (analogie k *podepsaným vlastnostem* v XAdES).

(d) signedAttrs: *podepsané atributy*, které se zahrnují do výpočtu elektronického podpisu.

   i. attrType: typ atributu.

   ii. attrValues: hodnota atributu.

(e) signatureAlgorithm: identifikace algoritmu použitého k vytvoření elektronickému podpisu včetně jeho příslušných parametrů.

(f) signature: hodnota elektronického podpisu.

(g) unsignedAttrs: *nepodepsané atributy*, které se nezahrnují do výpočtu elektronického podpisu.

   i. attrType: typ atributu.

   ii. attrValues: hodnota atributu.

#### 4.8.1.2 Formy podpisu

Podpis může mít dvě formy:

1. Obalující podpis (*Enveloping Signature*): podpis obaluje podepsaná data. Data, která se podepisují, jsou umístěna v poli *eContent*.

2. Odpojený podpis (*Detached Signature*): data, která chceme podepsat, nejsou obalena podpisem. Nenachází se tedy v poli *eContent*.

#### 4.8.1.3 Atributy podpisu

Stejně jako má XAdES *vlastnosti*, což jsou metadata o podpisu a podepisovaných datech, má CMS *atributy*.

**Podepsané atributy podpisu (*Signed Attributes*)**

Ukázka některých podepsaných atributů:

- Kontrolní součet zprávy (*Message Digest*): haš podepisované zprávy. Počítá se z položky *eContent*. Identifikátor atributu je *id-messageDigest*.
- Datum a čas (*Signing Time*): datum a čas podpisu. Identifikátor atributu je *id-signingTime*.

**Nepodepsané atributy podpisu (*Unsigned Attributes*)**

Ukázka nepodepsaného atributu:

- Spolupodpis (*Countersignature*): atribut se skládá ze struktury *SignerInfo*, která opět obsahuje položku *sid*, ze které se identifikuje certifikát nutný k ověření spolupodpisu. Vstupními daty pro výpočet spolupodpisu je elektronický podpis uložený v atributu *signature*. Identifikátor atributu je *id-countersignature*.

Pro podrobný podpis všech atributů čtenáře odkazuji na *RFC 5652*.

#### 4.8.1.4 Tvorba podpisu

Výpočet elektronického podpisu může mít dvě podoby:

1. Zpráva neobsahuje *podepsané atributy podpisu*: haš se spočte ze vstupních dat, tedy z pole *eContent* pomocí algoritmu specifikovaného v poli *digestAlgorithm*. Následně se z něj vytváří elektronický podpis s využitím algoritmu specifikovaného v poli *signatureAlgorithm*. Výsledný podpis je uložen v poli *signature*.
2. Zpráva obsahuje *podepsané atributy podpisu*: haš se spočte ze vstupních dat, tedy z pole *eContent* společně s *podepisovanými atributy* v poli *signedAttrs* pomocí algoritmu specifikovaného v poli *digestAlgorithm*. Následně se z něj vytváří elektronický podpis s využitím algoritmu specifikovaného v poli *signatureAlgorithm*. Výsledný podpis je uložen v poli *signature*.

#### 4.8.1.5 Ověření podpisu

Pro ověření je zapotřebí samotná hodnota elektronického podpisu, tu načteme z pole *signature*, a veřejný klíč. Veřejný klíč lze získat z pole *certificates*, do kterého může podepisující vložit certifikát použitý k podpisu, ale předpokládá se, že jej bude ověřující strana schopna získat i jiným způsobem, protože jej podepisující nemá povinnost přiložit. Ověření platnosti podpisu může být založeno na certifikační cestě, která se také skládá z certifikátů vložených do pole *certificates*, ale předpokládá se, že si bude ověřující schopen získat materiály k ověření i jiným způsobem. To samé platí pro CRL, které mohou být uloženy v poli *crls*.

Samotný proces ověření je velmi podobný tomu, co jsme si už v rámci práce ukazovali a nepopisuje jej do hloubky ani *RFC 5652*.

### 4.8.2 Výhody CAdES oproti CMS

Stejně jako XML-DSig, i CMS dává poměrně značnou volnost v možnostech tvorby elektronického podpisu. Vytvořené podpisy mohou být velmi jednoduché a nemusí obsahovat ani certifikát, kterým je identifikována podepisující strana. Nedefinuje bezpečnostní politiku, jeho atributy nepodporují možnost dlouhodobého ověření a není jasně určeno, jak a kdy mají být použity. Za tímto účelem bylo u CMS vydáno mnoho doplňující specifikací, které potřebné informace přidávají (například *RFC 2634* nebo *RFC 5035*). Využití těchto doplňujících specifikací bylo záležitostí jednotlivých států.

CAdES k tomuto problému přistupuje systematicky a stanovuje jasná pravidla pro elektronický podpis založený na standardu CMS, aby jej bylo možné považovat za elektronický podpis, který bude mít právně nezpochybnitelné účinky v rámci všech států EU. Jedná se o analogii k tomu, což jsme již probírali u XML-DSig a XAdESu. Velká část kapitoly 4.7, jako jsou například *kvalifikované vlastnosti*, *podepsané* a *nepodepsané vlastnosti* platí i v této kapitole. Liší se sice například v tom, že *vlastnostem* se říká *atributy* a pracuje se v binární oproti XML formě, ale cíl, kterého se snaží CAdES dosáhnout, a postupy jakými to dělá, jsou při srovnání s XAdESem velmi podobné.

Ve zkratce nyní zmíním nedostatky, které CAdES adresuje, protože valná většina z nich se kryje s tím, co XAdES řeší u XML-DSig (viz kapitola 4.7.2):

- Určuje, jak bude identifikována podepisující strana. CMS umožňuje certifikát přiložit do pole *certificates*, ale nepožaduje, aby tato informace byla podepsána (a tím pádem zabezpečena). CAdES toto požaduje a k identifikaci se používají certifikáty ve formátu X.509.
- Definuje bezpečnostní politiku.
- Rozšiřuje metadata.
- Podporuje dlouhodobou archivaci (LTV).

### 4.8.3 Atributy a struktura

Pokud jde o rozšíření, tak CAdES rozšiřuje CMS o nové datové struktury a atributy. Formát XAdES nazývá sadu metadata pro podpis a data *vlastnostmi*. *Vlastnosti* rozděluje na *podepsané* a *nepodepsané* a uchovává je v elementech *SignedProperties* a *UnsignedProperties*. Tyto elementy dále člení na *podepsané vlastnosti podpisu/dat* (*SignedSignatureProperties*, *SignedDataObjectProperties*) a nepodepsané vlastnosti podpisu/dat (*UnsignedSignatureProperties*, *UnsignedDataObjectProperties*). CAdES (stejně jako CMS) nazývá sadu metadat pro podpis a data *atributy*, taktéž je rozděluje na *podepsané* a *nepodepsané* a uchovává je v polích *signedAttrs* a *unsignedAttrs*.

Jak již bylo řečeno, CAdES i XAdES se sice liší v názvech těchto metadat, ale mají stejný cíl, kterého se snaží dosáhnout podobnými prostředky. Například v CAdESu *nepodepsaný atribut complete-revocation-references*, který ob-

sahuje odkazy na všechny CRL potřebné k validaci podpisu, má svou analogii v XAdESu jako *nepodepsaná vlastnost xades:CompleteCertificateRefsV2*. Atributy a vlastnosti jsou si velmi podobné, proto zde atributy nebudeme podrobně vypisovat jako vlastnosti v kapitole o XAdESu. Přehled toho, co všechno musí formát elektronického podpisu obsahovat pro splnění nařízení eIDAS si čtenář může udělat v kapitole 4.7.3. Pro podrobný popis všech atributů pak čtenáře odkazuji na normu *ETSI EN 319 122-1*.

#### Struktura

V kapitole 4.8.1.1 jsme si představili strukturu, která představuje elektronický podpis dle formátu CMS. Stejná struktura platí i pro CAdES. To je poměrně zásadní rozdíl oproti XAdESu, který původní strukturu XML-DSig značně rozšířil kvůli přidání metadat v podobě *kvalifikovaných vlastností*. Každý objekt a pole má svůj význam, pro jejich připomenutí čtenáře odkazuji na kapitolu 4.8.1.1.

### 4.8.4 CAdES Baseline Profile

Stejně jako formát XAdES i CAdES definuje mnoho volitelných atributů, které obsahují informace o podpisu a podepisovaných datech. Ze stejného důvodu jsou zavedeny čtyři základní úrovně CAdES podpisů, jejichž cílem je omezit volnost a zjednodušit tak jejich interpretaci. Jsou to:

- CAdES-B-B,
- CAdES-B-T,
- CAdES-B-LT,
- CAdES-B-LTA.

Úrovně jsou u XAdESu a CAdESu totožné, čtenáře proto odkazuji na kapitolu 4.7.4, kde jsou podrobně popsány. CAdES kromě *základních úrovní* popsaných v *Baseline Profile* nabízí ještě *rozšířené úrovně*, které vyžadují pro splnění jiné kombinace atributů. Pro více informací o *rozšířených CAdES úrovních* čtenáře odkazuji na normu *ETSI EN 319 122-2* [14].

#### Požadavky na algoritmy

Stejně jak XAdES, i CAdES zakazuje použití algoritmu MD5 a doporučuje množinu preferovaných algoritmů.

### 4.8.5 Srovnání XAdES a CAdES formátu

Pokud srovnáváme XAdES a CAdES, pak srovnáváme technologie, na kterých jsou vybudovány. U XAdES je to XML-DSig, který je postaven na značkovacím jazyce XML, a u CAdES zase binární CMS.

### Výhody XAdESu

- S využitím XPath můžeme podepisovat vybrané části dokumentu.
- Transformace umožňují odmazat části, které nechceme zahrnout do podpisu, například bílé mezery.
- Pro každý rozšířený programovací jazyk existuje spousta hotových knihoven, které umožňují snadnou manipulaci s XML.
- XML je člověkem čitelný formát, což se může hodit ve chvílích, když podpis chceme ručně prozkoumat nebo zobrazit.

### Výhody CAdESu

- Pracuje s binárními daty a zpracování je proto rychlejší než u XML, které vyžaduje značnou režii. Například výpočet haše u CMS typicky znamená pouze přímou manipulaci s bajtovým polem, XML-DSig musí provést kanonizace, transformace, kódování z/do Base64, ... A to vše nad XML elementy, jejichž zpracování trvá déle než práce přímo na bajtové úrovni.
- XML-DSig je například díky kanonizaci a XPath náchylnější na problémy s interoperabilitou[20]. Podepisující i ověřující strana totiž musí XML zpracovat zcela totožným způsobem a čím více technologií je do tvorby podpisu zapojeno, tím větší je šance, že se dvě implementace budou lišit.
- Potřebuje méně paměti. Navíc pokud obsahuje XML-DSig rozměrná data (*obalující podpis*), tak nástroje pro jeho generování, které nejprve načtou celé XML do paměti a až poté ho zpracovávají, mohou skončit na nedostatek paměti[21].

Vždy je zapotřebí posoudit výhody a nevýhody jednotlivých formátů a vybrat ten, který je pro danou situaci nejvhodnější.

[20] Schopnost různých systémů vzájemně spolupracovat.

[21] Příkladem může být *DOM Parser* v Javě, který celé XML nejprve načte do paměti a následně z něj vytváří objektově orientovanou reprezentaci XML.

## 4.9 PDF Advanced Electronic Signatures (PAdES)

PAdES (PDF Advanced Electronic Signature) je formát elektronického podpisu definovaný v normě *ETSI EN 319 142-1* [15]. Stejně jako XAdES a CAdES je postaven na technologii PKI a digitálních certifikátech.

Jedná se o sadu rozšíření a omezení ke standardu *ISO 32000-1* [16], ve kterém jsou kromě samotného formátu PDF řešeny i elektronické podpisy. Tento standard by měl být v polovině roku 2017 nahrazen novou verzí *ISO 32000-2*. Ta řeší posílení šifrovacích algoritmů (zavedení AES-256), vypuštění mnoha implementačních detailů a funkcí, které se považují za zastaralé, přidává plnou podporu UTF-8 a mnoho dalšího. Čtenáře pro zjištění všech nových funkcionalit odkazuji na standard *ISO 32000-2*. V době psaní diplomové práce (červen 2017) tento standard ještě nebyl vydán.

PDF podporuje elektronické podpisy již mnoho let. Zatímco *ISO 32000-1* popisuje obecný standard pro elektronicky podepsaná PDF, PAdES určuje přesnou definici a činí tyto podpisy kompatibilní s nařízením eIDAS.

Hlavní rozdíl PAdESu oproti XAdESu a CAdESu je, že se dá použít pouze na podepsání dokumentů ve formátu PDF. PAdES navíc definuje fungování softwaru pracujícího s elektronickými podpisy v PDF dokumentech. Naproti tomu XAdES i CAdES definují technologie, které lze použít při vývoji jakékoliv aplikace, která potřebuje pracovat s elektronickými podpisy standardizovaným způsobem.

Jelikož se jedná o standard, který pracuje s dokumenty čitelnými pro člověka, definuje i grafické znázornění podpisů a jejich integrování s funkcemi pro vyplňování formulářů, které PDF podporuje.

### 4.9.1 Portable Document Format (PDF)

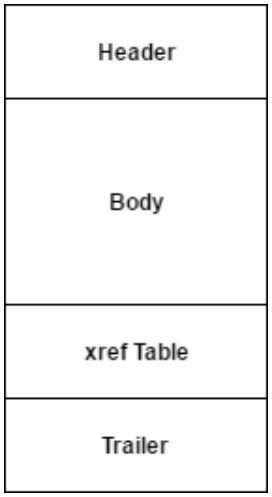
PDF je souborový formát pro ukládaní a zobrazování dokumentů nezávisle na softwaru i hardwaru a zajišťuje, že se na všech zařízeních zobrazí stejně. Může obsahovat text, obrázky, odkazy, multimediální prvky a mnoho dalšího. Podporuje funkce jako je textové vyhledávání, záložky, poznámky či náhodný přístup k datům. Důležitá je také možnost dokumenty komprimovat nebo elektronicky podepsat.

PDF je založen na podmnožině jazyka PostScript[22]. Některé funkce jazyka jsou vypuštěny (např. *if*, *loop*), jiné přidány nebo implementovány mírně odlišně. PDF dokumenty jsou obecně menší než dokumenty založené na jazyce PostScript a jejich struktura je předvídatelnější, což je důležité při modifikaci dokumentu nebo během vyhledávání informací, které se v něm nachází.

[22]Programovací jazyk vyvinutý pro popis tisknutelných dokumentů. Stejně jako formát PDF byl vyvinut firmou Adobe Systems Incorporated. Jednou z jeho hlavních předností je nezávislost na zařízení, na kterém se má dokument zobrazit nebo tisknout. Je založen na souřadnicovém systému, který určuje polohu objektů a je nezávislý na zobrazovacím prostoru, které zařízení poskytuje.

#### 4.9.1.1 Struktura PDF dokumentu

Zjednodušená struktura PDF dokumentu vypadá následovně:




Obrázek 8: Základní struktura PDF dokumentu

**Header (Hlavička)**

Skládá se z *magického čísla*[23] a verze formátu.

Například: *%PDF-1.7*

**Body (Tělo)**

V těle se nachází všechna data (texty, obrázky, ...), která jsou prezentována uživateli. Tvoří jej osm základních objektů, které lze jednoznačně poznat podle počátečního a koncového řetězce, který se skládá z ASCII znaků.

- Pravdivostní hodnoty (*Booleans*): klíčové slovo *true*, *false*.
- Čísla (*Numbers*): celá nebo reálná s omezeným rozsahem a přesností podle počítače, na kterém se PDF zpracovává.
- Řetězce (*Strings*): řetězce ASCII znaků, alternativně v hexadecimální nebo oktalové soustavě. Jsou obaleny kulatými nebo špičatými závorkami. Mezi kulatými závorkami mohou být libovolné tisknutelné znaky. Lze taktéž použít tzv. *escape sequence* jako je například „\n“ pro nový řádek. Maximální délka řetězce je omezena danou implementací.

  Například: *(text)*

[23] Číselná nebo textová konstanta, která identifikuje konkrétní souborový formát. U PDF má hodnotu v hexadecimálním vyjádření 25 50 44 46, v kódování ISO/IEC 8859-1 vyjádřeno jako *%PDF*.

- Jména (*Names*): slouží k pojmenování objektů. Jmenné objekty složené ze stejné sekvence znaků reprezentují stejný objekt a jsou uvozeny lomítkem.

  Například: */Example*

- Pole (*Arrays*): kolekce objektů. Jedno pole může obsahovat objekty více typů a je obaleno v hranatých závorkách.

  Například: *[42.0 15 true /Example]*

- Slovníky (*Dictionaries*): asociativní tabulka. Klíč musí být jmenný objekt a hodnota může být jakýkoliv objekt včetně dalšího slovníku. Slovník je obalen zdvojenými špičatými závorkami.

  Například:

  ```
  <<
  /Example (text)
  /Version 1.5
  /AnotherDictionary << /Example2 (text2) >>
  >>
  ```

- Proudy (*Streams*): velká data reprezentovaná sekvencí bajtů. Nejsou oproti řetězcům velikostně omezeny. Používají se například k uložení obrázků. Na rozdíl od řetězců nemusí být přečteny celé najednou. Informace o proudu v sobě obsahuje slovník, který je k němu přičleněn. Obsahuje například délku dat či filtr, který má být na proud dat aplikován při jeho zpracování[24].

  Například:

  ```
  << ... >>
  stream
  data
  endstream
  ```

- Null: prázdný objekt.

Každý objekt v rámci PDF může být označen jako tzv. *nepřímý objekt* (*indirect object*) prostřednictvím obalení do značek *obj* a *endobj*, kdy úvodní značce *obj* předchází dvě čísla určující číslo objektu a generaci. Toto označení přiřadí objektu jedinečný identifikátor, kterým se na něj ostatní objekty mohou odkazovat. Identifikátor je uložen v tabulce křížových odkazů a lze ho znovu použít na jakékoliv stránce a v jakémkoliv *slovníku*. Přístup k objektu prostřednictvím tabulky křížových odkazů je velmi rychlý. Pokud budeme odkazovat na nedefinovaný objekt, výsledkem bude *null*. Příklad definování nepřímého objektu:

[24]Filtrem může být například algoritmus zajišťující dekomprimaci, pokud jsou data komprimována

```
5 0 obj
(example)
endobj
```

Objekty jsou obvykle číslovány sekvenčně a při vytvoření mají číslo generace 0. Při změně se pak toto číslo navyšuje, udává tedy, o jakou verzi objektu se jedná. Na objekt se pak můžeme odkazovat pomocí tzv. *indirect reference*, která se skládá z čísla objektu, generace a znaku *R*:

```
5 0 R
```

### xref Table (Tabulka křížových odkazů)

Tabulka křížových odkazů, která obsahuje odkazy na všechny *nepřímé objekty* v dokumentu. Jejím účelem je umožnit náhodný přístup k objektům v dokumentu, aniž by bylo nutné sekvenčně procházet celé PDF pro nalezení konkrétního objektu.

### Trailer

Na konci každého dokumentu se nachází *Trailer*. Ten obsahuje slovník *trailer dictionary* uvozený klíčovým slovem *trailer*, jehož položky popisují dokument. Například celkový počet záznamů v tabulce křížových odkazů nebo kde se nachází důležité části dokumentu. Není pak zapotřebí sekvenčního procházení celého dokumentu. Před koncem dokumentu se pak nachází klíčové slovo *startxref*, které určuje posun tabulky s křížovými odkazy oproti začátku dokumentu, což umožňuje její rychlé nalezení. Poslední řádek pak tvoří znak *%%EOF*, který označuje konec dokumentu. Aplikace zobrazující PDF by proto měly číst PDF vždy od konce.

Ukázka struktury reálného PDF dokumentu s tučně zvýrazněnými popisky, které slouží pro lepší orientaci a nejsou normálně součástí PDF:

**Hlavička**

```
%PDF-1.4
```

**Tělo**

```
6 0 obj<</H[516 141]/Linearized 1/E 4534/L 8357/N 1/O 9/T
8191>>
endobj
```

**Tabulka křížových odkazů**

```
xref
6 11
0000000016 00000 n
0000000657 00000 n
0000000516 00000 n
0000000733 00000 n
0000000860 00000 n
```

```
0000000970 00000 n
0000001327 00000 n
0000001548 00000 n
0000001582 00000 n
0000004251 00000 n
0000004458 00000 n
```

**Trailer**

```
trailer
<</Size 17/Prev 8181/Root 7 0 R/Info 5 0 R
/ID[<db7775cce227f6b30c440df4221dc390>
<b0b3638dea568846897460db50f305e8>]>>
startxref
0
%%EOF
```

Pro detailní popis struktury čtenáře odkazuji na standard *ISO 32000-1*, případně *ISO 32000-2*.

#### 4.9.1.2 Přírůstkové aktualizace

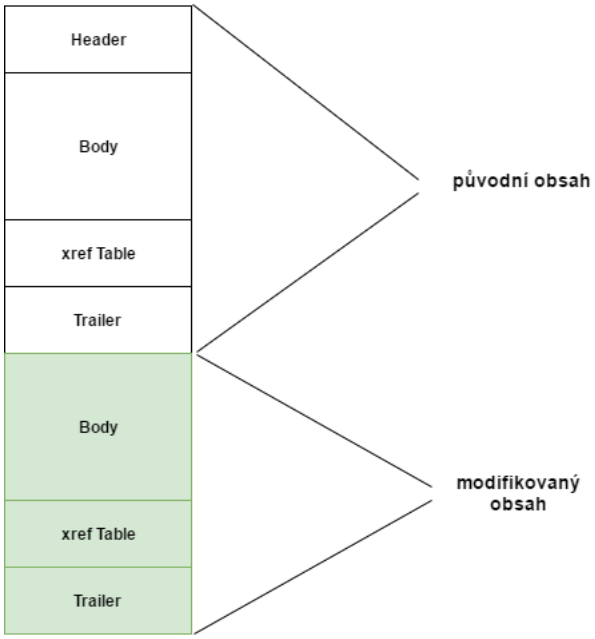
Formát PDF podporuje tzv. *přírůstkové aktualizace*. Ty umožňují provádět změny v dokumentu a zároveň zachovat původní obsah. Přírůstková aktualizace je realizována přidáním modifikovaných informací na konec dokumentu (viz obrázek 9). Je tak zachován celý původní obsah a na konec dokumentu se přidá nové *tělo*, *tabulka křížových odkazů* a *trailer*. U předchozí verze souboru nejsou vyžadovány žádné změny. Při zpracování dokumentu se pak berou v potaz jen nejnovější verze všech objektů. Díky přírůstkovým aktualizacím mohou aplikace zobrazit, jak vypadala konkrétní verze dokumentu před určitou změnou, nebo například porovnat dvě verze mezi sebou.

#### 4.9.1.3 Struktura podpisu

*ISO 32000-1* popisuje dvě operace s elektronickými podpisy a to vytvoření elektronického podpisu a jeho pozdější ověření. Podpis lze vytvořit dvěma způsoby:

1. Standardní aktualizace: podpis přidáváme do aktuálního dokument a měníme tím jeho obsah. Původní objekty se nahrazují novými, přidávají se nové objekty a je nutné přepočítat odkazy v tabulce křížových odkazů a aktualizovat všechny další informace, jako jsou například posuny.

2. Přírůstková aktualizace: nejčastěji se při tvorbě podpisu používá přírůstková aktualizace. Podpis vždy fixuje konkrétní verzi dokumentu a nástroje, které pracují s PDF, mohou zobrazit, jak vypadala konkrétní podepsaná verze. Díky tomu můžeme PDF opatřit novým podpisem bez změny jakýchkoliv dat pokrytých starším podpisem. Můžeme tak modifikovat PDF, aniž by došlo ke znehodnocení stávajících podpisů.




Obrázek 9: Přírůstková aktualizace

Informace o podpisu jsou uloženy v tzv. *podpisovém slovníku* (*Signature Dictionary*), což je objekt typu *slovník*, který podpis popisuje. *Podpisový slovník* obsahuje:

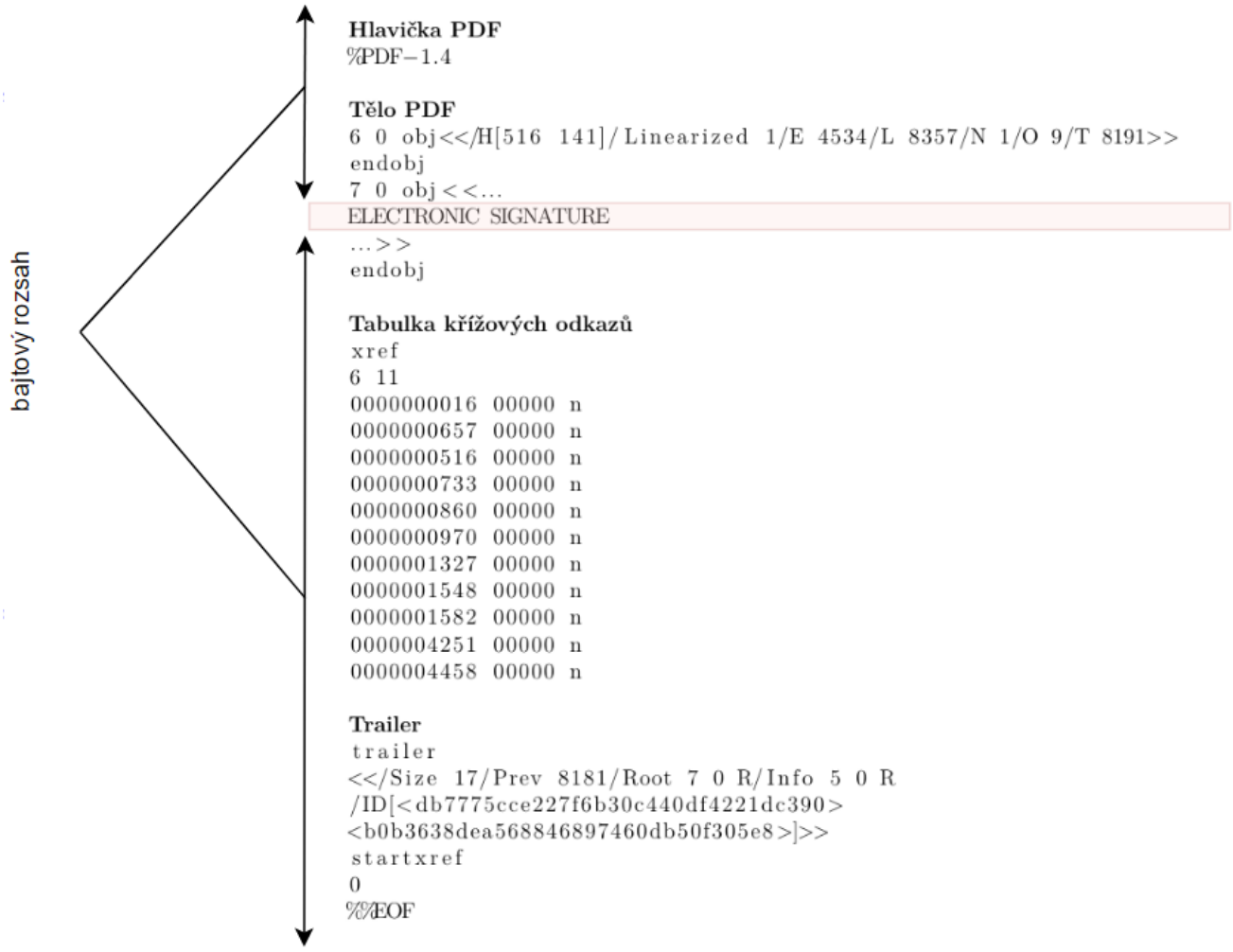
- Type: typ objektu, který slovník popisuje. V případě elektronického podpisu hodnota *Sig*.
- Filter: jméno handleru, který by měl být použit k ověření podpisu. Například *Adobe.PPKLite*.
- SubFilter: udává, jak jsou kódována data podpisu a informace o klíči v rámci *podpisového slovníku*. Například *adbe.pkcs7.detached*.
- Contents: hodnota elektronického podpisu. Obsahuje data ve formátu PKCS#1 nebo PKCS#7/CMS. Je doporučeno používat PKCS#7/CMS.
- Cert: certifikát použitý k vytvoření elektronického podpisu a certifikáty v rámci certifikační cesty.
- ByteRange: pole dvojic celých čísel, které určují všechny intervaly, kde se nachází data, která chceme podepsat. První číslo udává posun prvního bajtu intervalu od začátku dokumentu, druhé pak délku intervalu. Intervaly nejčastěji pokrývají celý dokument s výjimkou samotného elektronického podpisu.

- Reference: specifikuje určité přípustné transformace, které lze provést na podepsaném dokumentu, při kterých nebude porušena integrita podpisu. Může jít například o možnost přidání komentáře.
- Changes: popisuje změny, které byly nad dokumentem mezi tímto a předchozím podpisem provedeny.
- Name: jméno podepisujícího.
- M: čas vytvoření podpisu.
- Location: místo podpisu.
- Reason: důvod podpisu.
- ContactInfo: kontaktní informace na podepisující osobu.
- R: verze handleru, který byl při tvorbě podpisu použit.
- V: verze *podpisového slovníku*.
- Prop_Build: informace o zařízení, které podpis vytvořilo (například operační systém).

Pro podrobný popis všech hodnot *podpisového slovníku* čtenáře odkazuji na *ISO 32000-1*.

Elektronické podpisy jsou u PDF dokumentů založeny na fyzickém uspořádání bajtů. Podpis definuje bajtový rozsah (offset a délku) v rámci PDF dokumentu, který bude použit k vytvoření a ověření podpisu. V PDF obvykle nejsou žádné bajty, které by nebyly podpisem pokryty kromě hodnoty podpisu samotného. Je pokryt celý dokument, nikoliv jednotlivé stránky, jak by se mohlo zdát z grafické vizualizace softwarových nástrojů, které zobrazí podpis na konkrétní stránce. *ISO 32000-1* umožňuje pouze sériové, a ne paralelní přidání podpisu. Každý další podpis tedy podepisuje i všechny předchozí podpisy. Jak můžeme vidět na obrázku 10, podepisuje se vše kromě červené části, kde se nachází hodnota podpisu. Struktura samotného pak podpisu vypadá následovně:

```
7 0 obj <<...
/Type /Sig
/Filter /Adobe.PPKLite
/SubFilter /adbe.pkcs7.detached
/Contents <330821e4906092a...000>
/ByteRange [0 67449 84727 318560]
/Name (Bc. Petr Freiberg)
/M (D:20170506144430+02'00')
/R 1116416
...>>
endobj
```




Obrázek 10: Bajtový rozsah, ze kterého se počítá haš

#### 4.9.1.4 Tvorba a ověření podpisu

Podepsání PDF dokumentu probíhá následovně:

1. Dokument se převede na proud bajtů.
2. Pokud se podepisuje celý dokument, což je nejčastější způsob, pak se nejprve v rámci *přírůstkové aktualizace* uloží na disk všechny objekty s dodatečným místem navíc pro samotná data podpisu a pole *ByteRange*. *ByteRange* určuje, ze kterých částí se má haš spočítat. Na obrázku 10 je definice dvou proudů znázorněna šipkami. Horní šipka vždy udává, kde proud začíná a dolní, kde končí.
3. Ve chvíli, kdy je známa pozice v rámci provedené přírůstkové aktualizace, je pole *ByteRange* přepsáno správnými hodnotami. Jelikož se posun nesmí změnit, je dodatečné místo přepsáno nulovými hodnotami.
4. Je spočítán haš z bajtů, které jsou určeny hodnotami pole *ByteRange* pomocí hašovacího algoritmu (např. SHA-256).
5. Haš je podepsán soukromým klíčem a je vygenerován hexadecimální PKCS#7/CMS objekt.
6. PKCS#7/CMS objekt je umístěn do položky *Contents*, která se nachází mezi prvním a druhým proudem bajtů. Nevyužitý prostor je opět vyplněn nulami, protože se posun nesmí změnit.

Ověření podpisu spočívá v opětovném výpočtu haše z bajtů, které jsou určeny dvojicemi v poli *ByteRange* a porovná se s hašem, který je s pomocí veřejného klíče získán z hodnoty elektronického podpisu, která je uložena v položce *Contents*.

### 4.9.2 Výhody PAdES oproti podpisům dle ISO 32000-1

Standard PAdES vychází ze standardu *ISO 32000-1*, který specifikuje elektronické podpisy PDF dokumentů založené na formátu PKCS#1 a PKCS#7/CMS. V rámci PAdES je však povolen pouze PKCS#7/CMS. PAdES zavádí alternativní kódování, které podporuje formát elektronické podpisu, který odpovídá formátu CAdES. Elektronický podpis formátu CAdES je tedy během procesu podepisování vložen do PDF struktury, kterou podepisuje. PAdES využívá CAdES jako základ, na kterém dále staví.

Stejně jako CAdES či XAdES, i PAdES stanovuje jasná pravidla pro elektronický podpis, aby byl uznán napříč státy EU. Taktéž zavádí čtyři základní úrovně podpisů, s tím, že každá vyšší úroveň splňuje všechny požadavky úrovně, která jí předchází.

### 4.9.3 Struktura

Požadavky na strukturu jsou následující:

- Objekt *SignedData*, který je specifikován v CAdESu, tvoří elektronický podpis PDF dokumentu a je umístěn v položce s klíčem *Contents* v rámci *podpisového slovníku* (*Signature Dictionary*) jak je popsáno v *ISO 32000-1*. V rámci PDF podpisu může figurovat vždy jen jeden podepisující (jeden objekt typu *SignerInfo* v poli *signerInfos*).
- Požadavky na zpracování PDF podpisu jsou specifikovány v normě *ISO 32000-1*. Výjimkou jsou pouze případy, kde je nahrazuje norma *ETSI EN 319 142-1* (PAdES).
- Některé atributy popsané v CAdESu mají stejný nebo podobný význam jako klíče *podpisového slovníku*. V takových situacích je použit pouze jeden z nich podle požadavků, které PAdES pro danou úroveň stanovuje.

PAdES využívá:

- Atributy definované v CMS a CAdES. Ty tvoří objekt *SignedData*, který je umístěn do položky s klíčem *Contents* v *podpisovém slovníku*. PAdES z nich využívá například: *signing-certificate-v2* (typ podepsaného obsahu) nebo *signature-policy-identifier* (podpisová politika).
- Atributy definované v *ISO 32000-1*, které tvoří *podpisový slovník*. PAdES z nich využívá například: *Contents* (místo pro uložení elektronického podpisu) nebo *Reason* (důvod podpisu).
- Atributy validačních dat a archivních validačních dat, které slouží k dlouhodobému ověření elektronického podpisu formátu PAdES. Jedná se o nové atributy, které PAdES zavádí.

Pro podrobný seznam využívaných atributů čtenáře odkazuji na normu *ETSI EN 319 142-1*.

#### 4.9.3.1 Validační data a atributy pro archivní validační data

PAdES definuje způsob, jak přidat k elektronickému podpisu, který podepisuje PDF dokument, dodatečná validační data. Zavádí *slovník Document Security Store* (DSS), který obsahuje data potřebná k validaci: certifikáty, CRL či OCSP odpovědi. DSS může dále obsahovat *slovník Validate Related Information* (VRI), který propojuje validační data s konkrétním podpisem.

Dále PAdES přináší rozšíření v podobě *slovníku Document Time-stamp*, který definuje nový podpis *Time stamp signature*. Vychází ze standardního *podpisového slovníku*, jehož strukturu jsme si ukazovali v kapitole 4.9.1.3, a zavádí na něj následující omezení:

1. Typ: musí být *DocTimeStamp*.

2. SubFilter: musí být *ETSI.RFC3161*.

3. Contents: musí obsahovat časové razítko.

4. Nesmí obsahovat položky: *Cert*, *Reference*, *Changes*, *R*, *Prop_AuthTime*, *Prop_AuthType*.

5. Neměl by obsahovat položky: *Name*, *M*, *Location*, *Reason*, *ContactInfo*.

Důvod, proč by některé položky neměly být ve slovníku, je ten, že se již nachází v rámci obsahu položky *Contents*. Všechny tyto rozšíření slouží k dlouhodobému ověření elektronického podpisu formátu PAdES.

### 4.9.4 PAdES Baseline Profile

Stejně jako formát XAdES a CAdES i PAdES zavádí čtyři základní úrovně PAdES podpisů, jejichž cílem je omezit volnost a zjednodušit tak jejich interpretaci: Jsou to:

- PAdES-B-B,
- PAdES-B-T,
- PAdES-B-LT,
- PAdES-B-LTA.

Úrovně jsou totožné, čtenáře proto odkazuji na kapitolu 4.7.4, kde jsou podrobně popsány. PAdES kromě *základních úrovní* popsaných v *Baseline Profile* nabízí ještě další dodatečné profily. Pro více informací čtenáře odkazuji na normu *ETSI EN 319 142-2* [17].

### 4.9.5 XAdES zanořený v PAdES

V rámci PAdESu se mohou nacházet i XML data podepsána elektronickým podpisem ve formátu XAdES, který je vložen do PDF společně s podepsanými daty. XAdES může být rozšířen tak, aby byl dlouhodobě ověřitelný. XML je podepsán nezávisle na PDF kontejneru a následně do něj spolu s podpisem vložen. XML data samozřejmě mohou být podepsána i bez XAdESu s použitím klasického PDF podpisu společně se zbytkem PDF.

Je třeba mít na paměti, že pokud PDF po vložení XAdESu znovu podepíšeme klasickým PDF podpisem, nelze již do XAdESu přidávat další informace, protože by došlo k porušení integrity podpisu. Pokud je XAdES umístěn v místě, kde jsou povoleny změny, je do něj možné přidávat dodatečné informace i po podepsání dokumentu.

Pro více informací čtenáře odkazuji na normu *ETSI EN 319 142-2*.

## 4.10 Ověřování elektronických podpisů standardu AdES

Technická specifikace *ETSI EN 319 102-1* [18] popisuje, jak probíhá ověřování a vyhodnocování platnosti elektronického podpisu splňující standard AdES, co vše je zapotřebí vzít v úvahu a jak mají být výsledky reprezentovány ověřující straně. Tato specifikace důsledně zohledňuje všechny aspekty elektronického podpisu: jeho formát, úroveň, použité certifikáty či podpisovou politiku. Proces ověření platnosti podpisu demonstruje formou abstraktních algoritmů, které je zapotřebí implementovat. Ty se v upravených variantách využívají pro ověření všech referenčních formátů nařízení eIDAS, kam patří XAdES, CAdES a PAdES. U vyšších úrovní elektronických podpisů je zapotřebí vzít do úvahy dodatečné informace, které mají k dispozici. Například u podpisů úrovně T, tedy takových, které jsou fixovány časovým razítkem, se ověřování provádí k okamžiku připojení časového razítka. S narůstající komplexitou, kterou sebou vyšší úrovně přináší, narůstá i složitost jejich ověření a vyhodnocení. Pro splnění specifikace *ETSI EN 319 102-1* není vyžadováno implementování těchto abstraktních algoritmů, ale požadují se případně takové algoritmy, které s nimi budou funkčně kompatibilní.

Jak probíhá ověření elektronického podpisu jsme si přiblížili v kapitole 4.5 a i na dalších místech v rámci celé čtvrté kapitoly. Popis ověření platnosti konkrétního formátu elektronického podpisu, například XAdESu úrovně B-LT, je nad rámec této práce. Čtenáři, který by měl o tuto problematiku zájem, doporučuji jako první zdroj informací zmiňovanou technickou specifikaci *ETSI EN 319 102-1* [18], která problematiku popisuje abstraktně a nezávisle na použitém programovacím jazyce.

# 5 Legislativa v ČR a EU

Česká i evropská legislativa prošla v minulém roce s přijetím nařízení eIDAS poměrně zásadními změnami. Ty mimo jiné pro státní i soukromý sektor znamenají nutnost přehodnocení způsobu práce s elektronickými dokumenty (a jejich elektronickými podpisy) a mají vliv i na software, který se dnes v České republice, ale i v ostatních státech EU, tvoří a tvořit bude.

Značný informační přínos při zpracování této kapitoly měla série článků [19] od autora RNDr. Ing. Jiřího Peterky, nezávislého konzultanta, vysokoškolského pedagoga, publicisty a od roku 2015 člena Rady ČTÚ. V současné době se jedná o jednoho z největších odborníků na eIDAS a přidruženou problematiku. Kapitola je shrnutím legislativních změn, které mají vliv na práci s důvěryhodnými elektronickými dokumenty. Nebudu tedy popisovat vše, co eIDAS mění, protože šíře tohoto nařízení dalece přesahuje rozsah této práce. Čtenáře je taktéž na místě upozornit, že kapitola není odborným právním rozborem.

## 5.1 Předchozí právní úprava v ČR

Předchozí právní úprava byla poměrně letitá, pocházela z roku 2000 a byla tvořena především zákonem č. 227/2000 Sb. *o elektronickém podpisu*, který sám vycházel z ještě starší unijní směrnice 1999/93/ES *o zásadách Společenství pro elektronické podpisy*. V rámci něj byly definovány elektronické podpisy. Během následujících let po roce 2000 docházelo k určitému vývoji, například přidáním elektronických značek, které v původní podobě zákona nebyly a mohly je používat pro podepisování jak fyzické, tak právnické osoby. Elektronická značka byla do legislativy zavedena pro potřeby nejrůznějších výstupů z informačních systémů, které neprochází lidskýma rukama, generuje je automaticky systém a je zapotřebí na nich vyznačit původ. Jednalo se však o evoluční, ne revoluční změny. Velký problém byl také v tom, že si jednotlivé státy EU vytvářely svůj vlastní legislativní rámec.

Kupříkladu český *zaručený elektronický podpis* byl diametrálně odlišný od slovenského *zaručeného elektronického podpisu*. Přívlastek „zaručený“ se vztahuje k právní úpravě a co všechno s takovým podpisem můžeme dle legislativy podepsat. Českým zaručeným elektronickým podpisem se šlo podepsat jménem kohokoli (i někoho reálně neexistujícího), zatímco u slovenské formy elektronického podpisu se mohla podepsat jen a pouze příslušná fyzická osoba. Důvodem bylo, že česká podoba nemusela být založena na kvalifikovaném certifikátu. Tento problém byl zmíněn již v kapitole 4.6, a je způsoben ne příliš šťastným překladem slovního spojení *Advanced Electronic Signature*. [7]

Takových rozdílů a nejasností bychom napříč státy EU našli mnoho, což bylo způsobeno i tím, že původní česká legislativa okolo elektronických podpisů vznikala v době, kdy jsme ještě ani nebyli součástí evropského společenství.

## 5.2 Nová právní úprava v ČR (eIDAS)

V druhé polovině roku 2016 nabylo účinnost nařízení Evropského parlamentu a Rady (EU) č. 910/2014, plným názvem *o elektronické identifikaci a službách vytvářejících důvěru na vnitřním trhu a o zrušení směrnice 1999/93/ES* (eIDAS). Záměrem tohoto nového unijního nařízení je snaha vytvořit jednotné celoevropské prostředí, v němž bude rutinně v rámci členských států EU fungovat elektronická identifikace (elektronické prokazování totožnosti) a další služby vytvářející důvěru pro elektronické transakce na vnitřním trhu EU (například vytváření a ověřování elektronických podpisů, pečetí a časových razítek) [20]. To by mělo zajistit bezpečnou a snadnou elektronické interakce mezi občany, podniky a veřejnou správou, a to i napříč státy EU. Zavedlo tak mimo jiné i společný rámec pro bezpečnostní prvky digitálních dat ve všech členských státech EU.

Jedná se o nařízení, a nikoli směrnicí. To znamená, že je přímo účinné. Platí od okamžiku své účinnosti (1.7.2016) a má aplikační přednost před národními zákony a dalšími právními předpisy. Do českého práva byl zakomponován adaptačním zákonem č. 297/2016 Sb. (*Zákon o službách vytvářejících důvěru pro elektronické transakce*) a doprovodným změnovým zákonem č. 298/2016 Sb., které připravily existující národní právní úpravu na dopady tohoto nařízení. Byl zrušen a nahrazen původní zákon č. 227/2000 Sb. (o elektronickém podpisu) a taktéž byla provedena řada změn i v mnoha jiných zákonech. Pokud nařízení eIDAS něco vynechává nebo to nechává na dopracování na národní úrovni, pak záleží, jak je to upraveno v české právní úpravě. Pokud však nařízení něco řeší, pak má přednost před národní právní úpravou a činí ji neúčinnou.

## 5.3 Přechodové období

Po dobu dvou let bude platit ještě tzv. *přechodové období*, které dává čas přizpůsobit se nové legislativě. Po tuto dobu zůstane například zachován ryze český výdobytek v podobě elektronické značky. eIDAS se v našem řešení inspiroval a zavádí elektronické pečeti. Hlavními legislativními rozdíly je, že elektronickou značku mohla jak fyzická, tak právnická osoba připojit na jakýkoliv dokument bez ohledu na to, jestli byla jeho původcem. Elektronickou pečeť může vytvářet jen právnická osoba (včetně organizační složky státu) a připojit ji může jen na to, čeho je sama původcem. Pečeť nedeklaruje projev vůle (v právním slova smyslu) jako například podpis (podepsat můžete klidně i cizí dokument, například smlouvu), ale deklarujeme pomocí ní, že jsme původcem toho, co je pečetí opatřeno. Na pozadí jsou samozřejmě stále kryptografické metody vycházející z asymetrické kryptografie, avšak zásadně se liší právní výklad.

## 5.4 Novinky v elektronických podpisech

Elektronické podpisy se dají po legislativní stránce nyní rozčlenit do čtyř kategorií:

- „prostý“ elektronický podpis: cokoli, co má elektronickou podobu a co někdo použije jako svůj podpis. Může se jednat i o scan vlastnoručního podpisu, který formou obrázku vložíme do PDF.
- zaručený elektronický podpis (AdES): na certifikát, na kterém je podpis založen, nejsou kladeny žádné požadavky. Může to být jakýkoli certifikát, třeba i *self-signed*, který si můžeme sami vytvořit a napsat do něj cokoli.
- zaručený elektronický podpis (AdES) založený na kvalifikovaném certifikátu: certifikát je jednoznačně spojen s podepisující osobou a umožňuje její identifikaci.
- kvalifikovaný elektronický podpis (QES, Qualified Electronic Signature): zaručený elektronický podpis musí být založen na kvalifikovaném certifikátu pro elektronický podpis a musí být vytvořen pomocí kvalifikovaného prostředku pro vytváření elektronických podpisů. Typicky čipová karta nebo USB token s příslušnou certifikací. Podepisování probíhá přímo ve kvalifikovaném prostředků a soukromý klíč potřebný pro podepsání nelze z takového prostředku exportovat.

Jedná se o legislativní pohled, který určuje, jaké technologie mají být pro splnění legislativy použity. V České republice existuje ještě *uznávaný elektronický podpis*. *Uznávaným elektronickým podpisem* se rozumí *zaručený elektronický podpis založený na kvalifikovaném certifikátu* nebo *kvalifikovaný elektronický podpis*. Jedná se tak o legislativní zkratku za dva různé druhy elektronických podpisů. Nařízení eIDAS nezná *uznávaný elektronický podpis* v podobě *zaručeného elektronického podpisu založeného na kvalifikovaném certifikátů*, ale ani jej nezakazuje. Jedná se o výjimku, kterou Česká republika využívala jak v předchozí, tak i v současné právní úpravě. Byla zavedena z toho důvodu, aby občané nemuseli používat při komunikaci se státem kvalifikované prostředky. Nebude však moci těžit z hlavního benefitu, kterým je jednotný způsob uznávání v rámci EU. Oproti elektronické značce bude existovat i po přechodovém období. U té bylo rozhodnuto, že je již nepotřebná a bude z české legislativy vypuštěna. Pokud jde o využití, pak státní orgány musí do dvou let používat pouze kvalifikované elektronické podpisy, u soukromých subjektů je to volitelné.

eIDAS jako referenční formáty elektronického podpisu vymezil formáty XAdES, CAdES a PAdES. A ty, jak víme naprosto detailně určují jakým způsobem má být vytvořen elektronický podpis. eIDAS připouští možnost používání i jiných formátů, ale ukládá řadu dodatečných povinností každému, kdo by tak chtěl činit.

## 5.5 Princip nediskriminace

Jedním ze sloganů, které doprovázejí nástup nového unijního nařízení, je tvrzení, že poprvé zrovnoprávňuje elektronickou a listinnou (papírovou) podobu. V novém nařízení je zmíněn požadavek reprezentovaný jako zákaz diskriminace

dokumentů v elektronické podobě: „Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.“

Příkladem může být, když na úřadě či soudu sedí referent, který nechce pracovat s čímkoliv elektronickým. Jakékoliv elektronické vstupy apriorně odmítá a požaduje, aby vše bylo předkládáno v listinné formě. To od nabytí účinnosti eIDAS již není možné. Musí se takovým vstupem začít zabývat a zkoumat, zda má všechny požadované náležitosti. Například pokud se jedná o právní úkon, kde je povinný podpis, pak zda je takový elektronický dokument řádně podepsán. A pokud ano, tak jestli je opatřen podpisem takového druhu, který je pro dané právní jednání požadován. Dokument v elektronické podobě může být odmítnut například právě na základě toho, že je opatřen podpisem špatného druhu nebo není podepsán vůbec. Nemůže však být již odmítnout pouze z toho důvodu, že má elektronickou podobu.

# 6 Úložiště důvěryhodných dokumentů

Cílem kapitoly je přiblížit technické řešení úložiště důvěryhodných dokumentů, které je v souladu s předchozími kapitolami. Popsat benefity, které jeho používání přináší, jaké mají být jeho základní vlastnosti a funkcionality a na jakém formátu patřícím do standardu AdES může být vybudováno. V závěru kapitoly bude v krátkosti shrnuto komerční řešení, na jehož vývoji jsem se z pozice vedoucího programátora firmy M.I.T. Consulting, s.r.o., podílel.

## 6.1 Proč používat úložiště?

Jak již bylo řečeno v úvodu práce, míra využívání elektronických dokumentů se jednoznačně odvíjí od jasných pravidel, jak s takovými dokumenty zacházet, aby si zachovaly svou důvěryhodnost. V České republice jednoznačně chybí povědomí o koncepci *důvěryhodného elektronického dokumentu* a tím i o pravidlech, jak s dokumentem zacházet, aby neztratil svou důvěryhodnost. Jedním z příkladů může být dlouhá diskuze o tzv. *vyvratitelné domněnce pravosti*[25], kterou představoval dnes již zrušený paragraf[26], který byl některými využíván jako záminka k odmítání aktivní péče o elektronické dokumenty. To, jak byl paragraf vykládán, šlo zcela proti tomu, co jsme si řekli v kapitolách 4.4 a 4.6, které se týkaly *zastarávání elektronických podpisů*. Vyvratitelná domněnka pravosti je složitější konstrukce, proto čtenáře odkazuji na článek doktora Peterky [22], který ji řeší a uzavřu to citací ze stejného článku [22]:

*Chcete-li mít možnost pracovat se svými elektronickými dokumenty, až dosud jste mohli volit mezi dvěma přístupy:*

- *dát na slova „lidí od počítačů a technických standardů“ a jednou za určitou dobu (dnes cca 5 let) ke svým el. dokumentům připojit časové razítko (a v tomto smyslu se o své dokumenty aktivně starat), nebo*
- *dát na slova archivářů (lidí z oboru archivnictví) a spoléhat se na to, že jeden el. podpis a jedno časové razítko vystačí na libovolně dlouho. Tedy že není třeba „přerazítkovávat“ (pravidelně přidávat další časová razítka), protože to prý nikdo nedělá a je to celkově hloupost.*

...

*No, teď už je vše rozhodnuto: vyvratitelná domněnka pravosti byla dnešním dnem zrušena, a odpůrci aktivní péče a o elektronické dokumenty tak přišli o svůj hlavní, a vlastně jediný argument.*

*Horší je, že smůlu má nyní ten, kdo se na jejich výklad spoléhal. Pokud promeškal nejzazší možný okamžik pro přidání dalšího časového razítka na nějaký svůj*

[25] Právní domněnka je konstrukce užívaná v právu, jíž se za určitých okolností v zájmu právní jistoty presumuje (předpokládá) právní skutečnost, o níž není jisto, zda nastala.[21]

[26] Zákon č. 499/2004 Sb. *o archivnictví a spisové službě*

*starší elektronický dokument, dnes už jej nebude moci využít. Protože elektronický podpis na dokumentu již nepůjde ověřit...*

Úložiště by před takovými situacemi mělo uživatele chránit a pracovat na základě technologických standardů a detailní znalosti dané problematiky, kterou do něj samozřejmě musí někdo naprogramovat. Prvním z důvodů, proč používat úložiště je tedy **bezpečnost**.

Problematika, jak již víme, je to velmi rozsáhlá, proto se nedá předpokládat, že by běžní uživatelé například detailně chápali důvody pro nutnost pravidelného *přerazítkování*. Úložiště by proto mělo poskytovat takový uživatelský komfort, aby je od těchto složitostí odstínilo. Pokud bude začleněno do již stávající infrastruktury, ve které je v rámci firmy dedikován server, na který mají všichni přístup a ukládají do něj firemní dokumenty, tak uživatelé ani nemusí vědět, že se na pozadí nějaké úložiště vůbec nachází. Druhým důvodem je tak **uživatelský komfort**. V ideálním případě uživatel nemusí řešit, jakým způsobem bude zajišťována dlouhodobá ověřitelnost a z toho vyplývající důvěryhodnost jeho elektronicky podepsaného dokumentu. Vše je řešeno na pozadí automaticky a jediné, co musí vědět je, že má elektronické dokumenty ukládat na nějaké konkrétní místo, které firma určila. Typicky je možnost dlouhodobého ověření velmi důležitá u dokumentů jako jsou:

- faktury,
- smlouvy,
- dopisy,
- objednávky.

Třetím důležitým důvodem pro úložiště je **legislativa**. Z kapitoly 5.2, která probírala nové nařízení eIDAS, můžeme usuzovat, kam se bude legislativní vývoj dále ubírat. Klade se důraz na sjednocení legislativy a technologií na poli digitální ekonomiky a je snaha maximalizovat použitelnost a přenositelnost elektronických služeb napříč státy EU. Úložiště by proto mělo poskytovat standardizované řešení postavené na standardu AdES a nařízení eIDAS, aby měl uživatel jistotu, že je po legislativní stránce vše v pořádku a jeho dokumenty bude jakýkoliv členský stát považovat za důvěryhodné (ač není tento pojem v české legislativě zakotven).

## 6.2 Základní vlastnosti úložiště

Úložiště by mělo mít určitou sadu vlastnosti, abych dokázalo splnit svůj cíl, kterým je udržet dokument dlouhodobě ověřitelný:

- Fixace dokumentu pomocí časového razítka.
- Uchovávání všech potřebných validačních materiálů (certifikáty, CRL, OCP odpovědi, TSL). Musí být také fixovány v čase.

- Udržování adekvátní síly používaných kryptografických mechanismů.
- Aktivní ochrana elektronického dokumentu proti podvrhu nebo poruše v úložišti.
- Automatické ověřování platnosti bezpečnostních prvků (typicky detekce chvíle, kde je nutné dokument přerazítkovat).
- Splnění legislativních požadavků ČR i EU.
- Auditování událostí, při kterých dochází k manipulaci s elektronickým dokumentem.
- Možnost napojení na jiné systémy, typicky DMS[27], které pak do něj mohou ukládat data.

Kromě softwarové ochrany je samozřejmě zapotřebí i ochrana hardwarová, jako je například volba vhodných zálohovacích mechanismů. Analýza této problematiky je mimo rozsah této práce.

## 6.3 Na jakém formátu úložiště vybudovat?

eIDAS jak dobře víme, určuje tři referenční formáty: XAdES, CAdES a PAdES. PAdES pro potřeby úložiště, které umožňuje uložit jakýkoliv typ dokumentu, můžeme zavrhnout rovnou. Výběr mezi zbývajícími dvěma formáty už není tak snadný a jako vodítko může posloužit srovnání, které se nachází v kapitole 4.8.5. Já zde představím řešení postavené na formátu XAdES, který umožňuje:

- Podepsat libovolné dokumenty bez ohledu na jejich typ.
- Podepsat více dokumentů jedním podpisem.
- Podepsat dokumenty skrze element *Manifest*, díky kterému bude podpis závislý na podepisovaných datech nepřímo.
- Vytvořit odpojený podpis (*detached signature*), kdy jsou podpis a dokumenty uloženy samostatně. Podpis obsahuje pouze odkazy na dokumenty a pro každý z nich má vypočítaný haš.
- Pro každý rozšířený programovací jazyk existuje mnoho knihoven umožňující snadnou manipulaci s XML.

Díky těmto možnostem, které XAdES nabízí, bude úložiště umožňovat:

[27] Systém určený ke správě elektronických dokumentů.

- Spojení dokumentů do jednoho balíčku, který bude opatřen jedním podpisem a jedním časovým razítkem. To značně optimalizuje proces razítkování a přerazítkování, protože jak bylo řečeno v kapitole 4.3, časová razítka jsou placená od kusu. Pokud bychom dokumenty podepisovaly každý zvlášť, tak bychom potřebovali pro každý z nich jedno časové razítko. To by enormně zvýšilo cenu za provoz úložiště.

- Mazaní dokumentů, protože jsou podepsány nepřímo skrze element *Manifest*. Viz kapitola 4.7.1.4.

- Stažení důkazních materiálů k dokumentu, aniž bychom vyzradili obsah zbylých dokumentů. Odpojený podpis obsahuje pouze haše dokumentů, na které odkazuje.

## 6.4 Příjem, čtení a důkazní materiály

Jedná se o základní operace, které musí úložiště poskytovat. Nyní se na ně podíváme podrobněji.

### Příjem dokumentu

Příjem dokumentu do úložiště by měl minimálně splňovat:

1. Kontrolu konzistence dokumentu, kdy ukládající na základě stanovené hašovací funkce spočítá haš dokumentu a ten společně s ukládaným dokumentem posílá do úložiště. Úložiště na vstupu vypočítá pro dokument stejnou hašovací funkcí haš a srovná ho se zaslaným hašem. Jedná se o všeobecně známý *kontrolní součet*, který zajistí, že do úložiště dorazil neporušený dokument. Pokud se haše neshodují, je na to ukládající upozorněn a dokument není přijat.

2. Kontrolu na bezpečnostní prvky, kdy je zkontrolováno, zda dokument není opatřen jedním nebo více elektronickými podpisy nebo jinými bezpečnostními prvky. Pokud je, tak proběhne proces ověření platnosti (viz kapitola 4.5). Je pak na nastavení úložiště, zda přijímá jen dokumenty s platnými bezpečnostními prvky nebo přijímá všechny. Pokud však přijímá všechny, tak u těch, které ověřením neprojdou, už není schopno zpětně zajistit důvěryhodnost. Úložiště by mělo podporovat všechny referenční formáty, aby je na příjmu dokázalo ověřit.

   V této chvíli je vrácen jedinečný identifikátor dokumentu a poslední krok již probíhá asynchronně.

3. Úložiště pro každý podpis/pečeť načte použitý certifikát a všechny certifikáty v certifikační cestě. Pro každý z nich získá revokační informace v podobě CRL nebo OCSP odpovědí. Zde je potřeba myslet na to, že pokud je podpis/pečeť na dokumentu mladší 24 hodin a pro získání revokačních informací používáme CRL, tak v něm revokace ještě nemusí být zanesena.

Je proto zapotřebí počkat 24 hodin a až poté CRL stáhnout. Stejné načtení informací musí proběhnout i pro pečeti, kterými jsou opatřeny revokační informace (viz kapitola 4.5).

Tímto způsobem úložiště zpracuje každý dokument. Po uplynutí stanoveného časového intervalu nebo po dosažení určitého počtu dokumentů je vytvořen XAdES úrovně B-LT s referencemi na všechny přijaté dokumenty.

#### Čtení dokumentu

Čtení dokumentu z úložiště je přímočará operace. Na konci procesu ukládání dokumentu do úložiště je vrácen jedinečný identifikátor dokumentu. Tento identifikátor poslouží uživateli k tomu, aby mohl dokument z úložiště znovu načíst. Běžně by uživatel s tímto identifikátorem vůbec neměl přijít do styku, protože bude odstíněn grafickou nadstavbou například v podobě ikonek. Dle implementace samozřejmě mohou být nastaveny i další podmínky jako jsou oprávnění nebo dodatečná autentizace pomocí PIN kódu.

#### Poskytnutí důkazních materiálů

Pokud uživatel potřebuje prokázat důvěryhodnost uloženého dokumentu, je zapotřebí, aby mu úložiště vydalo všechny důkazní materiály, které má. Ty představuje XAdES. Uživatel zašle jedinečný identifikátor dokumentu a úložiště mu pošle XAdES, který jej podepisuje. Je zapotřebí mít na paměti, že XAdES vzniká až po určité době od přijetí dokumentu. Po uplynutí časového intervalu nebo po dosažení určitého počtu dokumentů, jak jsme si řekli výše. Proto pokud by uživatel o důkazní materiál žádal dříve, než XAdES vznikl, tak úložiště musí vrátit zprávu, že dokument ještě nebyl podepsán a fixován v čase. Volba parametrů, které určují, jak brzo nebo pozdě bude dokument podepsán a fixován, je velmi důležitá a musí se volit dle prostředí, kde úložiště běží.

## 6.5 Smazání dokumentu

Při návrhu úložiště musíme myslet na to, že uživatel může chtít jednou uložený dokument smazat. To může mít řadu důvodů jako je nahrazení starého dokumentu za novější verzí nebo uvolnění místa v úložišti. Jak víme z kapitoly 4.7.1.4, taková věc by mohla u XAdESu, na kterém je úložiště postaveno, způsobit problém, protože by při ověřování referencí, které odkazují na dokumenty, nebylo možné všechny vyhodnotit. Řešení jsou dvě:

- Dokument reálně nesmazat, ale jen nastavit příznak, že je smazaný a na uživatelské straně k němu zamezit přístup.
- Vytvořit XAdES s využitím elementu *Manifest*, který umožnuje, aby XAdES podepisoval dokumenty nepřímo, jak jsme si řekli v kapitole 4.7.1.4, a tím mít možnost dokument opravdu fyzicky odstranit z úložiště se zachováním platnosti XAdESu.

Výběr jedné nebo druhé varianty závisí na prostředí, kde je úložiště nasazeno.

## 6.6 Pravidelná kontrola

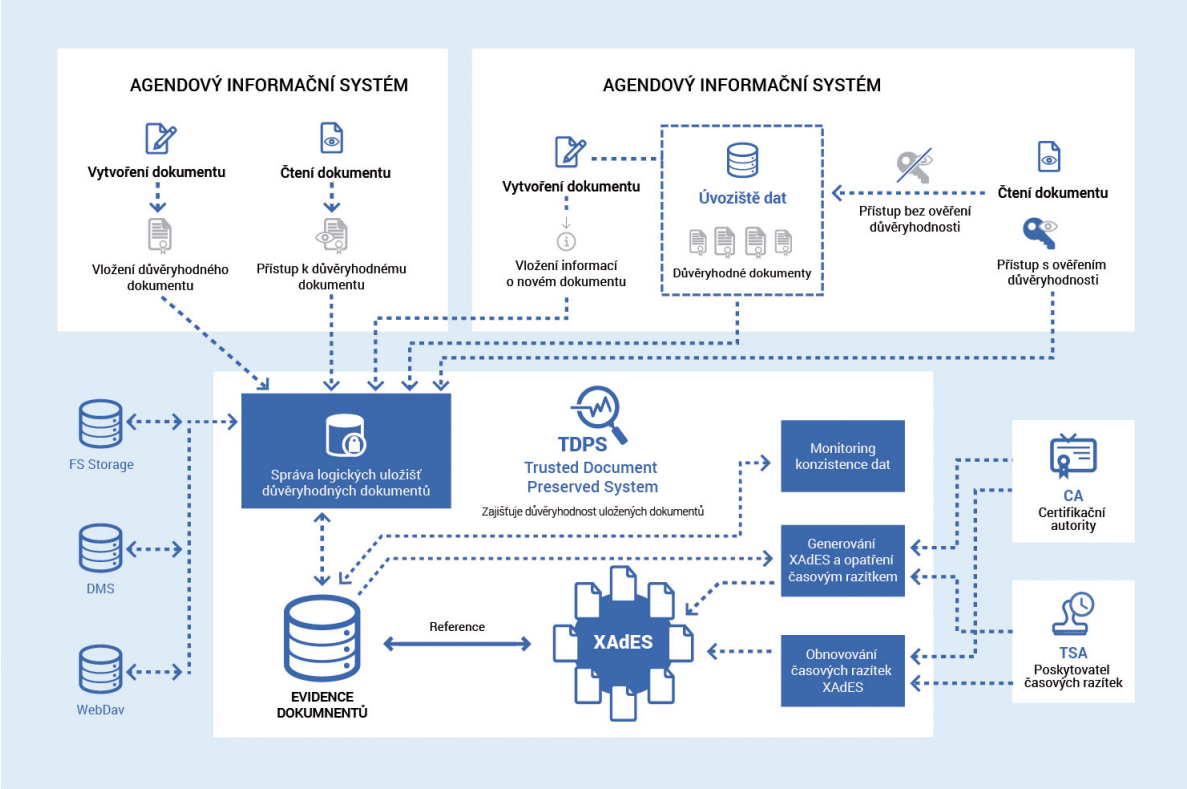
Úložiště by mělo v rámci pravidelných kontrol minimálně poskytovat:

1. Kontrolu konzistence všech uložených dokumentů. Každý dokument by měl být ve stanovených intervalech (jejich nastavení opět závisí na implementaci) zkontrolován, zda nebyla narušena jeho konzistence. Tato kontrola probíhá na základě srovnání hašů.

2. Kontrolu, zda nekončí platnost certifikátu, na kterém je založeno časové razítko, kterým je XAdES opatřen. Kontrola by měla probíhat každý den a provádět přerazítkování XAdESů s určitým předstihem pro případ neočekávaných problémů (např. výpadku časové autority). Tímto budou docíleno dlouhodobé ověřitelnosti.

## 6.7 Komerční řešení

Na závěr bych v krátkosti představil komerční řešení, na kterém jsem se podílel. Systém pro správu důvěryhodných dokumentů je komerční aplikací firmy M.I.T. Consulting, s.r.o, která jej nabízí pod obchodním názvem *Trusted Document Preserved System* (TDPS). [23]




Obrázek 11: Schéma TDPS [23]

Slouží k zachovaní důvěryhodnosti všech typů elektronických dokumentů. Úložiště splňuje všechny požadavky, které jsme si zde představili a dále k nim přidává: antivirovou kontrolu, notifikační upozornění v případě narušení konzistence uložených dokumentů nebo například napojení DMS pomocí CMIS. Jedná se o standard umožňující různým DMS komunikovat a spolupracovat prostřednictvím internetu.

## 6.8 Navazující diplomová práce

V této kapitole jsme si ukázali úložiště, které dokáže dlouhodobě udržovat důvěryhodnost elektronických dokumentů tím, že udržuje v ověřitelném stavu jejich bezpečnostní prvky. Pro potřeby digitální archivace, kdy chceme archivovat elektronické dokumenty vysoké informační hodnoty, je však zapotřebí více. Například čitelnost zajišťovat konverzí do formátů vhodných pro dlouhodobé uchovávání, aby nedošlo k situaci, že v horizontu desítek let nebudeme schopni elektronický dokument přečíst, protože nebude mít software, který by formát uměl interpretovat. K čemu nám pak bude zjištění, že má dokument platné elektronické podpisy, když ho nedokážeme přečíst.

Touto problematikou se bude v horizontu jednoho roku zabývat diplomová práce mého kolegy Bc. Jana Pavlovského, která na tuto práci bude navazovat. Jádro digitálního archivu bude tvořit komponenta námi popsaného úložiště pro správu důvěryhodných dokumentů, která se bude starat o udržování bezpečností prvků u dokumentů, které budou v archivu uloženy. Nad tímto úložištěm pak budou vystavěny další komponenty, které budou tvořit samotnou funkcionalitu digitálního archivu.

# Závěr

Cílem práce bylo popsat technologickou a legislativní stránku, na které může být vystavěno úložiště pro dlouhodobou a důvěryhodnou správu elektronických dokumentů. Formou, která bude pro čtenáře snadno uchopitelná a k dané problematice od něj neočekává žádné znalosti. Zároveň postupně půjde do dostatečné hloubky, aby zodpověděla co nejvíce otázek a poskytla co nejucelenější pohled.

Jednou z největších výzev bylo nastudování a pochopení této rozsáhlé a komplikované problematiky, ve které se prolíná technologický a legislativní svět. V České republice se tímto tématem veřejně zabývá pouze několik jednotlivců a velká část práce stojí pouze na oficiálních normách a zahraničních zdrojích. Normy ETSI i fundované rešerše firem jako Adobe Systems pak sice poskytují detailní popis konkrétní technologie nebo části řešené problematiky, ale obtížně se z nich vyvozuje širší kontext. Zcela chybí zdroje, které by již problematiku zpracovaly uceleně a do hloubky. To je způsobeno faktem, že se jedná o zatím málo prozkoumanou oblast, která se teprve nedávno začala více řešit společně s nařízením eIDAS. V následujících letech, pokud nedojde k obratu v nastoleném legislativním směru, očekávám poměrně razantní zvýšení povědomí u širší společnosti, která bude zákony nucena se touto problematikou zabývat.

Práce čtenáře nejprve seznamuje se základními pojmy jako jsou elektronický podpis a jeho platnost, a postupně k nim přidává složitější konstrukce typu zaručeného elektronického podpisu (AdES) nebo důvěryhodného úložiště. Stranou nezůstává ani legislativní rámec, kterému je věnována samostatná kapitola. V rámci celé práce je snaha vysvětlit nový pojem ve chvíli, kdy jej čtenář potřebuje znát a neodkazovat ho na budoucí sekce, dále zvolit přiměřenou úroveň detailu, aby vše podstatné bylo řečeno, a nakonec provázat jednotlivé pojmy do jednoho celku, ze kterého jsou vyvozeny podložené závěry.

Věřím, že práce poskytne čtenářům, kteří mají o tuto problematiku zájem, odrazový můstek, který jim usnadní orientaci v této dynamicky se rozvíjející se oblasti a případně ji použijí jako základ, na kterém budou moci dále stavět.

# Conclusions

The aim of the thesis is to describe the technological and legislative aspects on which a repository can be built for long-term and trustworthy administration of electronic documents. It pertains to a format that is readily grasped by the reader without the need for additional knowledge and/or expertise. At the same time, it gradually ventures deep into answering as many questions as possible in order to render the most complete view.

One of the biggest challenges was to study and understand this extensive and complicated issue in which the technological and legislative world is intermingled. Only a few individuals are publicly involved in this topic in the Czech Republic and the thesis is mostly based only on official standards and foreign sources. ETSI standards and research reviews from companies of the likes of Adobe Systems provide detailed description of a technology or parts of a solved issue, but it's difficult to derive a wider context from it. There is a lack of resources that would already process this subject completely in a comprehensive and in-depth manner. This is due the fact that it is still a marginally explored area that has only recently gained attention pursuant to the entry of the eIDAS regulation. In the years to come, if there is no change in the established legislative direction, I expect a rather vigorous increase in awareness among the wider society that will be forced to deal with this issue.

The reader first learns about the basic concepts such as electronic signature and its validity, and gradually learns more complex constructions like an advanced electronic signature (AdES) or a trusted repository. Legislative framework is also not forgotten and has one devoted chapter. Throughout the thesis, effort is made toward explaining the new concept at a time when the reader needs to know it and not refer him to future sections. Also, a suitable level of detail and linking individual concepts is essential.

I believe that the thesis will provide a good basis for readers interested in this issue and shall facilitate in their orientation in this dynamically developing field.

# A Obsah přiloženého CD

Součástí diplomové práce je přiložené CD s následující strukturou:

**`doc/`**
: Adresář obsahuje text práce ve formátu PDF a všechny soubory potřebné pro vygenerování PDF dokumentu (v ZIP archivu).

**`readme.txt`**
: Textový soubor obsahující informace o struktuře CD.

# Seznam použitých zkratek

**AdES** Advanced Electronic Signature

**ASCII** American Standard Code for Information Interchange

**ASN.1** Abstract Syntax Notation One

**BER** Basic Encoding Rules

**CA** Certifikační autorita

**CAdES** CMS Advanced Electronic Signatures

**CMS** Cryptographic Message Syntax

**CRL** Certificate Revocation List

**DER** Distinguished Encoding Rules

**ETSI** European Telecommunications Standards Institute

**HTTP** Hypertext Transfer Protocol

**IEFT** Internet Engineering Task Force

**LTV** Long Term Validation

**MAC** Message Authentication Code

**MIME** Multipurpose Internet Mail Extensions

**OCSP** Online Certificate Status Procotol

**PAdES** PDF Advanced Electronic Signatures

**PDF** Portable Document Format

**PEM** Privacy-enhanced Electronic Mail

**PKCS** Public Key Cryptographic Standards

**PKI** Public Key Infrastructure

**RFC** Request for Comments

**URI** Uniform Resource Identifier

**SHA** Secure Hash Algorithm

**TSA** Time Stamp Authority

**TSL** Trusted Services List

**W3C** World Wide Web Consortium

**XAdES** XML Advanced Electronic Signatures

**XML** eXtensible Markup Language

**XML-DSig** XML Digital Signature

# Literatura


[1] WIKISOFIA.CZ. Dokument, informační pramen a informační zdroj. [online]. 2017, [cit. 2017-06-01]. Dostupný z: ⟨https://wikisofia.cz/wiki/Dokument,_informa%C3%84%C2%8Dn%C3%83%C2%AD_pramen_a_informa%C3%84%C2%8Dn%C3%83%C2%AD_zdroj⟩.

[2] J., PRŮŠA. eIDAS: Česko má první subjekt posuzování shody. Jak je na tom Evropa? [online]. 2017, [cit. 2017-06-01]. Dostupný z: ⟨https://www.lupa.cz/clanky/eidas-cesko-ma-prvni-subjekt-posuzovani-shody-jak-je-na-tom-evropa/⟩.

[3] J., PETERKA. *Báječný svět elektronického podpisu.* První vyd. 2011. 438 s. ISBN 978-80-904248-3-8.

[4] J., PRŮŠA. eIDAS: Jak evropské nařízení (ne)ovlivní webové certifikáty? [online]. 2016, [cit. 2017-06-01]. Dostupný z: ⟨https://www.lupa.cz/clanky/eidas-jak-evropske-narizeni-ne-ovlivni-webove-certifikaty/⟩.

[5] J., PRŮŠA. eIDAS a problémy s důvěryhodností kvalifikovaných certifikátů. [online]. 2017, [cit. 2017-07-21]. Dostupný z: ⟨https://www.lupa.cz/clanky/eidas-a-problemy-s-duveryhodnosti-kvalifikovanych-certifikatu/⟩.

[6] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Metodický návod pro ověřování platnosti uznávaných elektronických podpisů a elektronických pečetí. [online]. 2016, [cit. 2017-06-01]. Dostupný z: ⟨http://www.mvcr.cz/soubor/metodicky-navod-pro-overovani-platnosti-uznavanych-podpisu-a-peceti.aspx⟩.

[7] J., PETERKA. eIDAS: Elektronické značky a pečetě a rekviem za datovou zprávu. [online]. 2016, [cit. 2017-06-01]. Dostupný z: ⟨https://www.lupa.cz/clanky/eidas-elektronicke-znacky-a-pecete-a-rekviem-za-datovou-zpravu/⟩.

[8] ÚŘEDNÍ VĚSTNÍK EVROPSKÉ UNIE. PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2015/1506 ze dne 8. září 2015. [online]. 2015, [cit. 2017-06-01]. Dostupný z: ⟨http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32015D1506&from=CS⟩.

[9] ETSI. ETSI EN 319 132-1 v1.1.1: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures. [online]. 2016, [cit. 2017-06-01]. Dostupný z: ⟨http://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/en_31913201v010101p.pdf⟩.

[10] W3C. XML Signature Syntax and Processing (Second Edition). [online]. 2008, [cit. 2017-06-01]. Dostupný z: ⟨https://www.w3.org/TR/xmldsig-core/⟩.

[11] ETSI. ETSI EN 319 132-2 V1.1.1: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures. [online]. 2016, [cit. 2017-06-01]. Dostupný z: ⟨http://www.etsi.org/deliver/etsi_en/319100_319199/31913202/01.01.01_60/en_31913202v010101p.pdf⟩.

[12] ETSI. ETSI EN 319 122-1 V1.1.1: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures. [online]. 2016, [cit. 2017-06-01]. Dostupný z: ⟨http://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.01.01_60/en_31912201v010101p.pdf⟩.

[13] NETWORK WORKING GROUP. RFC 5652: Cryptographic Message Syntax (CMS). [online]. 2009, [cit. 2017-06-01]. Dostupný z: ⟨https://tools.ietf.org/html/rfc5652⟩.

[14] ETSI. ETSI EN 319 122-2 V1.1.1: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures. [online]. 2016, [cit. 2017-06-01]. Dostupný z: ⟨http://www.etsi.org/deliver/etsi_en/319100_319199/31912202/01.01.01_60/en_31912202v010101p.pdf⟩.

[15] ETSI. ETSI EN 319 142-1 V1.1.1: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures. [online]. 2016, [cit. 2017-06-01]. Dostupný z: ⟨http://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/en_31914201v010101p.pdf⟩.

[16] ADOBE SYSTEMS INCORPORATED. ISO 32000-1. [online]. 2008, [cit. 2017-06-01]. Dostupný z: ⟨https://www.adobe.com/content/dam/Adobe/en/devnet/pdf/pdfs/PDF32000_2008.pdf⟩.

[17] ETSI. ETSI EN 319 142-2 V1.1.1: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles. [online]. 2016, [cit. 2017-06-01]. Dostupný z: ⟨http://www.etsi.org/deliver/etsi_en/319100_319199/31914202/01.01.01_60/en_31914202v010101p.pdf⟩.

[18] ETSI. ETSI EN 319 102-1 V1.1.1: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation. [online]. 2016, [cit. 2017-06-01]. Dostupný z: ⟨http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf⟩.

[19] J., PETERKA. Seriál eIDAS, elektronické podpisy a služby vytvářející důvěru. [online]. 2016, [cit. 2017-06-01]. Dostupný z: ⟨https://www.lupa.cz/serialy/eidas-elektronicke-podpisy-a-sluzby-vytvarejici-duveru/⟩.

[20] GORDIC. eIDAS není strašák, uživatelé GINISu se ho obávat nemusí. [online]. 2015, [cit. 2017-06-01]. Dostupný z: ⟨https://www.gordic.cz/zpravy-gordic/2015/eidas-neni-strasak,-uzivatele-ginisu-se-ho-obavat/⟩.

[21] WIKIPEDIA.CZ. Právní domněnka. [online]. 2017, [cit. 2017-06-01]. Dostupný z: ⟨https://cs.wikipedia.org/wiki/Pr%C3%83%C2%A1vn%C3%83%C2%AD_domn%C3%84%C2%9Bnka⟩.

[22] J., PETERKA. Po 16 letech své existence přestává platit zákon o el. podpisu. [online]. 2016, [cit. 2017-06-01]. Dostupný z: ⟨http://www.earchiv.cz/b16/b0919001.php3⟩.

[23] MIT. TDPS – DŮVĚRYHODNÉ ULOŽIŠTĚ DOKUMENTŮ. [online]. 2017, [cit. 2017-06-01]. Dostupný z: ⟨http://www.mit-consulting.cz/produkty/tdps-duveryhodne-uloziste-dokumentu/⟩.

[24] CRUELLAS J. C. KARLINGER G., PINKAS D. a ROSS J. XML Advanced Electronic Signatures (XAdES). [online]. 2003, [cit. 2017-06-01]. Dostupný z: ⟨https://www.w3.org/TR/XAdES/⟩.

[25] HLOUŠKOVÁ V. LUBAS J., ROSOL I. a BOBČÍK B. Důvěryhodný digitální dokument. Stanovisko ICT UNIE k problematice právně validního dokumentu. [online]. 2014, [cit. 2017-06-01]. Dostupný z: ⟨http://www.ictu.cz/fileadmin/user_upload/documents/Pozicni_dokumenty/Duveryhodny_digitalni_dokument.pdf⟩.

[26] LUBAS J. KUBÍČEK P., TEJCHMAN J. Správa a ukládání důvěryhodných dokumentů. [online]. 2016, [cit. 2017-06-01]. Dostupný z: ⟨http://www.ictu.cz/fileadmin/user_upload/documents/Pracovni_skupiny/Archivnictvi/2016/Sprava_a_ukladani_duveryhodnych_dokumentu.pdf⟩.

[27] ADOBE SYSTEMS INCORPORATED. The AdES family of standards: CAdES, XAdES, and PAdES. [online]. 2009, [cit. 2017-06-01]. Dostupný z: ⟨https://blogs.adobe.com/security/91014620_eusig_wp_ue.pdf⟩.

[28] J., PATTYNOVÁ. Důvěryhodný dokument v kontextu digitální kontinuity: právní aspekty. [online]. 2016, [cit. 2017-06-01]. Dostupný z: ⟨http://www.ictu.cz/fileadmin/user_upload/documents/Pracovni_skupiny/Archivnictvi/2016/Duveryhodny_dokument_Jana_Pattynova.pdf⟩.

[29] M.I.T. CONSULTING, S.R.O. Důvěryhodný dokument. [online]. 2017, [cit. 2017-06-01]. Dostupný z: ⟨http://www.mit-consulting.cz/wp-content/uploads/MIT_Duveryhodny_Document_TDPS_ERMS.pdf⟩.

[30] GEMINI SECURITY SOLUTIONS. XML Advanced Electronic Signatures (XAdES). [online]. [Cit. 2017-06-01]. Dostupný z: ⟨http://geminisecurity.com/wp-content/uploads/tools/xades-overview.pdf⟩.

[31] J., PETERKA. Problém digitální kontinuity, alias dlouhověkost elektronických dokumentů. [online]. 2013, [cit. 2017-06-01]. Dostupný z: ⟨http://www.earchiv.cz/papers/p66/index.php3⟩.

[32] ADOBE SYSTEMS INCORPORATED. Digital Signatures in a PDF. [online]. [Cit. 2017-06-01]. Dostupný z: ⟨https://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/Acrobat_DigitalSignatures_in_PDF.pdf⟩.