Ondřej Ševeček | PM Windows Server | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security |
ondrej@sevecek.com | www.sevecek.com |

KVALIFIKOVANÉ CERTIFIKÁTY

1

Slovníček

Česky	Anglicky
veřejný / soukromý klíč	public / private key
otisk	hash
podepsat / podpis / značka	sign / signature
kvalifikovaný	qualified
akreditovaný poskytovatel certifikačních služeb	accredited certification service provider
časové razítko	timestamp

2

Zákon

- Zákon č. 227/2000 Sb., o elektronickém podpisu
- Primitiva
  - (kvalifikovaný) (akreditovaný) poskytovatel certifikačních služeb
  - (zaručený) elektronický podpis
  - elektronická značka
    - "zaručená" se nepíše, i když to tak je
  - (kvalifikovaný) (systémový) certifikát
  - (kvalifikované) časové razítko

Zákon

- (zaručený) elektronický podpis
  - non repudiation, podepisuje jen fyzická osoba
  - nemusí být kvalifikovaný, nepotřebujeme SSCD
- elektronická značka
  - signature, podepisuje fyzická nebo právnická osoba, jen kvalifikovaný systémový certifikát
- (kvalifikovaný) (systémový) certifikát
  - fyzická osoba, právnická osoba
- (kvalifikované) časové razítko
  - bez identifikace podepisující osoby
  - jedná se sice o podpis, ale nesmí být brán jako vyjádření souhlasu

Poskytovatel certifikačních služeb

- poskytovatel certifikačních služeb
  - certifikační autorita
- kvalifikovaný poskytovatel certifikačních služeb
  - CA, která vydává kvalifikované certifikáty, nebo kvalifikované systémové certifikáty, nebo kvalifikovaná časová razítka
  - ohlašovací povinnost
- akreditovaný poskytovatel certifikačních služeb
  - kvalifikovaný poskytovatel certifikačních služeb, který byl akreditován podle tohoto zákona
  - vydává uznávané kvalifikované certifikáty, které je možné použít k podepisování a značkování dokumentů, jejichž prostřednictvím se činí úkony vůči "státu"
- vůči státu je možné použít v EU cizíně akreditované CA, které jsou "důvěryhodné", což definuje ministerstvo

5

Ministerstvo

- uděluje a odnímá akreditace
- vede evidenci vydaných kvalifikovaných systémových certifikátů, které používá kvalifikovaný poskytovatel certifikačních služeb
- průběžně uveřejňuje přehled udělených akreditací, přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb a kvalifikované systémové certifikáty, a to i způsobem umožňujícím dálkový přístup

6

Kvalifikovaný certifikát

- kvalifikovaným certifikátem [se rozumí] certifikát, který má náležitosti podle §12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb
- Kvalifikovaný certifikát musí obsahovat
  - označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona
  - v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen
  - jméno, popřípadě jména, a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym
  - zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu
  - data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby
  - elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný certifikát vydává
  - číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb
  - počátek a konec platnosti kvalifikovaného certifikátu
  - případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití
  - případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít

Kvalifikovaný systémový certifikát

- kvalifikovaným systémovým certifikátem certifikát, který má náležitosti podle §12a a byl vydán kvalifikovaným poskytovatelem certifikačních služeb
- Kvalifikovaný systémový certifikát musí obsahovat
  - označení, že je vydán jako kvalifikovaný systémový certifikát podle tohoto zákona
  - v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen
  - jednoznačnou identifikaci označující osoby, případně prostředku pro vytváření elektronických značek
  - data pro ověřování elektronických značek, která odpovídají datům pro vytváření elektronických značek, jež jsou pod kontrolou označující osoby
  - elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný systémový certifikát vydává
  - číslo kvalifikovaného systémového certifikátu unikátní u daného kvalifikovaného poskytovatele certifikačních služeb
  - počátek a konec platnosti kvalifikovaného systémového certifikátu
  - omezení pro použití kvalifikovaného systémového certifikátu, přičemž tato omezení musí být zjevná třetím stranám.

Kvalifikované časové razítko

- kvalifikovaným časovým razítkem [se rozumí] datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem
- Kvalifikované časové razítko musí obsahovat
  - číslo kvalifikovaného časového razítka unikátní u daného kvalifikovaného poskytovatele certifikačních služeb,
  - označení pravidel, podle kterých kvalifikovaný poskytovatel certifikačních služeb kvalifikované časové razítko vydal,
  - v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,
  - hodnotu času, která odpovídá koordinovanému světovému času při vytváření kvalifikovaného časového razítka,
  - data v elektronické podobě, pro která bylo kvalifikované časové razítko vydáno,
  - elektronickou značku kvalifikovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal.

Prostředky pro (bezpečné) vytváření el. podpisů

- prostředkem pro (bezpečné) vytváření elektronických podpisů [se rozumí] technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů
- bezpečné:
  - data pro vytváření podpisu se mohou vyskytnout pouze jednou a že jejich utajení je náležitě zajištěno
  - data pro vytváření podpisu nelze při náležitém zajištění odvodit ze znalosti způsobu jejich vytváření a že podpis je chráněn proti padělání s využitím existující dostupné technologie
  - data pro vytváření podpisu mohou být podepisující osobou spolehlivě chráněna proti zneužití třetí osobou
- Prostředky pro bezpečné vytváření podpisu nesmí měnit data, která se podepisují, ani zabraňovat tomu, aby tato data byla předložena podepisující osobě před vlastním procesem podepisování
- Prostředek pro bezpečné ověřování podpisu musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, aby
  - data používaná pro ověření podpisu odpovídala datům zobrazeným osobě provádějící ověření,
  - podpis byl spolehlivě ověřen a výsledek tohoto ověření byl řádně zobrazen,
  - ověřující osoba mohla spolehlivě zjistit obsah podepsaných dat,
  - pravost a platnost certifikátu při ověřování podpisu byly spolehlivě zjištěny,
  - výsledek ověření a totožnost podepisující osoby byly řádně zobrazeny,
  - bylo jasně uvedeno použití pseudonymu,
  - bylo možné zjistit veškeré změny ovlivňující bezpečnost

(obecný) Elektronický podpis

- elektronickým podpisem [se rozumí] údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě

Zaručený elektronický podpis

- zaručeným elektronickým podpisem [se rozumí] elektronický podpis, který splňuje následující požadavky
  - je jednoznačně spojen s podepisující osobou
  - umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě
  - byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou
  - je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat
- Poznámka: explicitně se zde nezmiňuje kvalifikovaný certifikát, ale i ten je identifikací osoby

Podepisující osoba

- podepisující osobou [se rozumí] fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby

Elektronická značka

- elektronickou značkou [se rozumí] údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky
  - jsou jednoznačně spojené s označující osobou
  - umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu
  - byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou
  - jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat

Označující osoba

- označující osobou [se rozumí] fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou

Prostředky pro vytváření elektronických značek

- Prostředek pro vytváření elektronických značek musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, že
  - data pro vytváření elektronických značek jsou dostatečným způsobem utajena a jsou označující osobou spolehlivě chráněna proti zneužití třetí osobou,
  - označující osoba je informována, že zahajuje používání tohoto prostředku
- Prostředek pro vytváření elektronických značek musí být nastaven tak, aby i bez další kontroly označující osoby označil právě a pouze ty datové zprávy, které označující osoba k označení zvolí

Držitel certifikátu

- držitelem certifikátu [se rozumí] fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu pro sebe nebo pro podepisující nebo označující osobu a které byl certifikát vydán

Podepsání zprávy a seznámení

- Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem. Pokud se neprokáže opak, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila.

MVČR

- http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx
- Seznam kvalifikovaných poskytovatelů certifikační služeb
- Seznam nástrojů (SSCD), u nichž byla prověřena shoda
  - není povinné ukládání kvalifikovaných certifikátů
- Seznam otisků certifikátů kvalifikovaných CA

NBÚ SK

- Povinně ukládat kvalifikované certifikáty na otestovaných zařízeních (SSCD)
  - http://www.nbusr.sk/sk/elektronicky-podpis/certifikacia-produktov-pre-zep/zoznam-certifikovanych-produktov/certifikovane-produkty-pre-pouzivate-ov-zep.html

Kvalifikované CA

- Poskytovatel certifikačních služeb
- Audit podle ČSN ISO/IEC 27001 – Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky

CZ/SK Akreditované Kvalifikované CA

- http://www.ica.cz
  - 2002
  - kvalifikovaná časová razítka 2006
  - MSRootCAProg 2008
- http://www.postsignum.cz
  - 2005
  - MSRootCAProg 2011
- http://www.eidentity.cz
  - 2005
  - not on MSRootCAProg as of May 2013
- http://www.dtca.sk
  - I.CA dceřiná společnost na Slovensku
  - stejné certifikáty
  - 2006
  - MSRootCAProg 2008
- http://www.disig.sk
  - 2005
  - MSRootCAProg 2009
- http://www.psca.sk
  - not on MSRootCAProg as of May 2013

EU Směrnice

- Směrnice EP a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy
- Uznávané elektronické podpisy a elektronické značky

EU certifikační autority

- Rozhodnutí Komise 2009/767/ES, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst" podle směrnice EP a Rady 2006/123/ES o službách na vnitřním trhu
  - 28.12.2009

EU certifikační autority

- TSL - Trusted Services Lists
  - seznam poskytovatelů certifikačních služeb, kteří vydávají kvalifikované certifikáty, a kteří jsou pod kontrolou
  - vydává každá vláda
  - digitálně podepsáno I.CA
- Centrální seznam
  - https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf
  - https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml
- CZ webová aplikace
  - https://tsl.gov.cz/certiq/

Enterprise PKI

NÁVRH DMS S ELEKTRONICKÝM PODPISEM A ČASOVÝMI RAZÍTKY

Návrh DMS s podpisy

- podepisovat musím kvalifikovaným certifikátem (osobním)
  - kvalifikovaným systémovým certifikátem mohu provádět transport, přihlašování apod.
    - i tak ale musím značkující osobu informovat, že právě značkuje
  - podepisující osoba musí být informována o tom, že podepisuje
- kvalifikovaným certifikátem (osobním) se nesmím přihlašovat
  - pokud k tomu nepoužiji data, se kterými může člověk souhlasit a která mu předem zobrazím
  - ideálně by měl potvrdit, že je vidí, aby byl "seznámen"
- musím lidem zobrazit data, která budou podepisovat
  - pouze lidská data, se kterými může člověk souhlasit (non-repudiation)
  - "bezestylový" dokument?
  - nesmím data před podpisem nijak změnit, co jsem lidem zobrazil, podepíšu
- podpis a data mohou ležet odděleně
  - PKCS#7
- hash algoritmus k podpisu by měla být stejná SHAxxx jako je SHA značka podepisujícího certifikátu
  - abychom nedegradovali bezpečnost kryptosystému

Long term validation

- Uchovávat certifikát podpisový
  - není potřeba uchovávat privátní klíč
- Uchovávat certifikáty všech autorit, které podpisový certifikát vydaly
- Stahovat všechna CRL všech certifikátů včetně všech autorit od okamžiku podpisu do okamžiku konce platnosti certifikátu vydávající CA
  - možná by mohla stačit jen dvě po sobě jdoucí
  - stejná CRL i certifikáty se poznají podle jejich thumbprintu