Garantovaná a bezpečná archivace dokumentů

Miroslav Šedivý, Telefónica CZ

A Telefónica company

2 Garantovaná a bezpečná archivace dokumentů

Dokumenty vs. legislativa

- Co nového v oblasti legislativy?

- Nic …
- Pokud nepočítáme některé výklady a vyjádření, mající především tu vlastnost, že situaci neřeší

- Otázka: Máme ale vůbec nějaký problém? Vždyť vše funguje, jak má …
- Odpověď: Teď ano, ale co za deset let ? A co za dvacet let ?

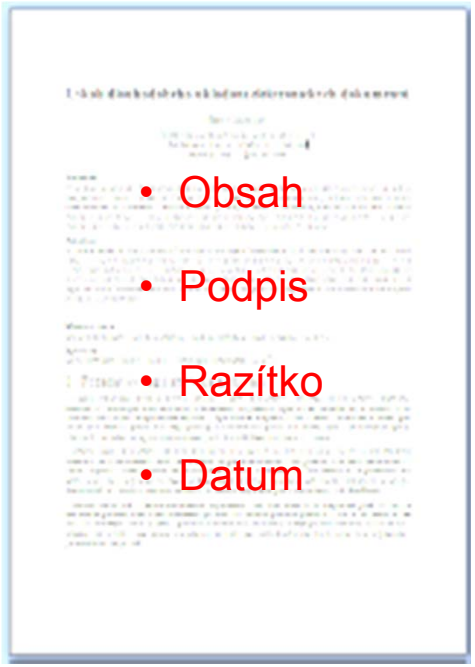
3 Garantovaná a bezpečná archivace dokumentů

Jaký problém vlastně musíme (chceme) řešit?

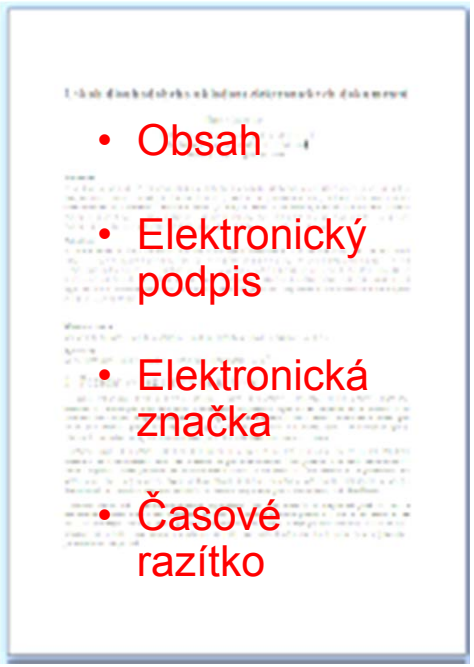
-> Zachování právní síly elektronického dokumentu

Analogie s listinným dokumentem:

Listinný dokument



Elektronický dokument



4 Garantovaná a bezpečná archivace dokumentů

Uchovávání dokumentu

Listinný dokument

Žádný problém !

Elektronický dokument

Žádný problém ???

A Telefónica company

5 Garantovaná a bezpečná archivace dokumentů

Pravost dokumentu

- Základní postulát – tzv. vyvratitelná domněnka pravosti

> (8) Neprokáže-li se opak, dokument v digitální podobě se považuje za pravý, byl-li podepsán platným uznávaným elektronickým podpisem nebo označen platnou elektronickou značkou osoby, která k tomu byla v okamžiku podepsání nebo označení oprávněna, osoby odpovědné za převedení z dokumentu v analogové podobě nebo změnu formátu dokumentu v digitální podobě nebo osoby odpovědné za provedení autorizované konverze dokumentů a opatřen kvalifikovaným časovým razítkem. Ustanovení věty první se vztahuje i na dokumenty vzniklé z činnosti původců, kteří nejsou určenými původci.

- Zdánlivě není co řešit, ale …

6 Garantovaná a bezpečná archivace dokumentů

Možné problémy s archivací elektronických dokumentů

Předpoklad: Dokumenty jsou elektronicky podepsány (označeny) a opatřeny jedním časovým razítkem

- Integrita dokumentu
  - Existence dvou obsahově různých dokumentů se stejným e-podpisem a časovým razítkem (tzv. kolizní dokumenty)
  - Který z nich označíme za pravý?
- Elektronický podpis po době platnosti podpisového certifikátu a certifikátu časového razítka
  - Kdy byl podpis vytvořen – v době platnosti certifikátu nebo po platnosti?
  - Co když byl privátní klíč certifikátu zcizen a zneužit?
  - Co když po několika letech byl algoritmus podpisu prolomen?
- Časové razítko – totéž jako elektronický podpis

- Opravdu stačí elektronický podpis a jedno časové razítko ???

7 Garantovaná a bezpečná archivace dokumentů

Kolizní dokumenty (blízká budoucnost, jedno časové razítko)

Listinný dokument

Smlouva o prodeji nemovitosti

Pan: **Jan Novotný**.....

narozen: 1.1.1980.....

bytem: Praha 1, Václavské nám. 1.....

(dále jen „prodávající")

a

Pan: **Jaroslav Vikář**.....

narozen: 29.12.1985.....

bytem: Kladno, Vrchlického 15.....

(dále jen „kupující")

uzavírají dle ust. § 588 a násl. občanského zákoníku tuto"

smlouvu o prodeji nemovitosti:

I. Předmět smlouvy

Prodávající je výlučným vlastníkem pozemku parc. č. 1245/15, trvalý travní porost, o výměře 2547 m2, zapsaného na Katastrálním úřadě pro Středočeský kraj se sídlem v Praze, katastrální pracoviště Praha západ, na LV č. 1478574 pro obec Kladno a katastrální území Kladno-střed (dále jen „Nemovitost") a prohlašuje, že jeho vlastnické právo k uvedené nemovitosti je nesporné, je oprávněn s ní volně nakládat a jeho smluvní volnost není ničím omezena.

II. Kupní cena

Prodávající prodává kupujícím nemovitost uvedenou v čl. I. této smlouvy za dohodnutou kupní cenu ve výši 2 050 000,- Kč (slovy: dvamilionypadesáttisíc korun českých) a Kupující tuto nemovitost za takto dohodnutou kupní cenu kupují do svého výlučného vlastnictví.

III. Platba

Kupní cena uvedená v čl. II. bude uhrazena následujícím způsobem:

1. Část kupní ceny ve výši 1 625 000,-Kč (slovy: jedenmilionšestsetdvacetpěttisíc korun českých) uhradili Kupující Prodávajícímu v hotovosti při podpisu této smlouvy.

2. Zbylou část kupní ceny ve výši 425 000-Kč (slovy: čtyřistadvacetpěttisíc korun českých) předal Kupující při podpisu této smlouvy v hotovosti do úschovy zprostředkovateli ing.Petrovi Jasnému, IČ 125456789222. Tato částka bude zprostředkovatelem převedena na účet Prodávajícího č. 00045789654/0900, vedený u Evropské národní banky, a.s. v Brně, do 15 dnů po převodu vlastnického práva k předmětné Nemovitosti na jména Kupujících a po předložení výpisu z katastru nemovitostí, kde jako vlastník Nemovitosti budou uvedeni výlučně Kupující, části „C" a „D" budou bez zápisu a rovněž na předloženém listu vlastnictví nebude žádná plomba.

Elektronický dokument

Smlouva o prodeji nemovitosti

Pan: **Jan Novotný**.....

narozen: 1.1.1980.....

bytem: Praha 1, Václavské nám. 1.....

(dále jen „prodávající")

a

Pan: **Jaroslav Vikář**.....

narozen: 29.12.1985.....

bytem: Kladno, Vrchlického 15.....

(dále jen „kupující")

uzavírají dle ust. § 588 a násl. občanského zákoníku tuto"

smlouvu o prodeji nemovitosti:

I. Předmět smlouvy

Prodávající je výlučným vlastníkem pozemku parc. č. 1245/15, trvalý travní porost, o výměře 2547 m2, zapsaného na Katastrálním úřadě pro Středočeský kraj se sídlem v Praze, katastrální pracoviště Praha západ, na LV č. 1478574 pro obec Kladno a katastrální území Kladno-střed (dále jen „Nemovitost") a prohlašuje, že jeho vlastnické právo k uvedené nemovitosti je nesporné, je oprávněn s ní volně nakládat a jeho smluvní volnost není ničím omezena.

II. Kupní cena

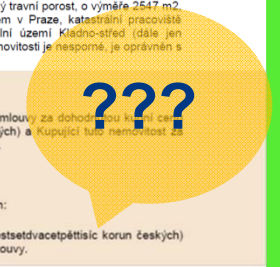
Prodávající prodává kupujícím nemovitost uvedenou v čl. I. této smlouvy za dohodnutou kupní cenu ve výši 2 050 000,- Kč (slovy: dvamilionypadesáttisíc korun českých) a Kupující tuto nemovitost za takto dohodnutou kupní cenu kupují do svého výlučného vlastnictví.

III. Platba

Kupní cena uvedená v čl. II. bude uhrazena následujícím způsobem:

1. Část kupní ceny ve výši 1 625 000,-Kč (slovy: jedenmilionšestsetdvacetpěttisíc korun českých) uhradili Kupující Prodávajícímu v hotovosti při podpisu této smlouvy.

2. Zbylou část kupní ceny ve výši 425 000-Kč (slovy: čtyřistadvacetpěttisíc korun českých) předal Kupující při podpisu této smlouvy v hotovosti do úschovy zprostředkovateli ing.Petrovi Jasnému, IČ 125456789222. Tato částka bude zprostředkovatelem převedena na účet Prodávajícího č. 00045789654/0900, vedený u Evropské národní banky, a.s. v Brně, do 15 dnů po převodu vlastnického práva k předmětné Nemovitosti na jména Kupujících a po předložení výpisu z katastru nemovitostí, kde jako vlastník Nemovitosti budou uvedeni výlučně Kupující, části „C" a „D" budou bez zápisu a rovněž na předloženém listu vlastnictví nebude žádná plomba.



8 Garantovaná a bezpečná archivace dokumentů

Kolizní dokumenty (vzdálená budoucnost, jedno časové razítko)

Listinný dokument

Smlouva o prodeji nemovitosti

Pan: **Jan Novotný**.....

narozen: 1.1.1980.....

bytem: Praha 1, Václavské nám. 1.....

(dále jen „prodávající")

a

Pan: **Jaroslav Vikář**.....

narozen: 29.12.1985.....

bytem: Kladno, Vrchlického 15.....

(dále jen „kupující")

uzavírají dle ust. § 588 a násl. občanského zákoníku tuto"

smlouvu o prodeji nemovitosti:

I. Předmět smlouvy

Prodávající je výlučným vlastníkem pozemku parc. č. 1245/15, trvalý travní porost, o výměře 2547 m2, zapsaného na Katastrálním úřadě pro Středočeský kraj se sídlem v Praze, katastrální pracoviště Praha západ, na LV č. 1478574 pro obec Kladno a katastrální území Kladno-střed (dále jen „Nemovitost") a prohlašuje, že jeho vlastnické právo k uvedené nemovitosti je nesporné, je oprávněn s ní volně nakládat a jeho smluvní volnost není ničím omezena.

II. Kupní cena

Prodávající prodává kupujícím nemovitost uvedenou v čl. I. této smlouvy za dohodnutou kupní cenu ve výši 1 050 000,- Kč (slovy: jedenmilionpadesáttisíc korun českých) a Kupující tuto nemovitost za takto dohodnutou kupní cenu kupují do svého výlučného vlastnictví.

III. Platba

Kupní cena uvedená v čl. II. bude uhrazena následujícím způsobem:

1. Část kupní ceny ve výši 625 000,-Kč (slovy: šestsetdvacetpěttisíc korun českých) uhradili Kupující Prodávajícímu v hotovosti při podpisu této smlouvy.
2. Zbylou část kupní ceny ve výši 425 000-Kč (slovy: čtyřistadvacetpěttisíc korun českých) předal Kupující při podpisu této smlouvy v hotovosti do úschovy zprostředkovateli ing.Petrovi Jasnému, IČ 125456789222. Tato částka bude zprostředkovatelem převedena na účet Prodávajícího č. 00045789654/0900, vedený u Evropské národní banky, a.s. v Brně, do 15 dnů po převodu vlastnického práva k předmětné Nemovitosti na jména Kupujících a po předložení výpisu z katastru nemovitostí, kde jako vlastník Nemovitosti budou uvedeni výlučně Kupující, části „C" a „D" budou bez zápisu a rovněž na předloženém listu vlastnictví nebude žádná plomba.

Elektronický dokument

Smlouva o prodeji nemovitosti

Pan: **Jan Novotný**.....

narozen: 1.1.1980.....

bytem: Praha 1, Václavské nám. 1.....

(dále jen „prodávající")

a

Pan: **Jaroslav Vikář**.....

narozen: 29.12.1985.....

bytem: Kladno, Vrchlického 15.....

(dále jen „kupující")

uzavírají dle ust. § 588 a násl. občanského zákoníku tuto"

smlouvu o prodeji nemovitosti:

I. Předmět smlouvy

Prodávající je výlučným vlastníkem pozemku parc. č. 1245/15, trvalý travní porost, o výměře 2547 m2, zapsaného na Katastrálním úřadě pro Středočeský kraj se sídlem v Praze, katastrální pracoviště Praha západ, na LV č. 1478574 pro obec Kladno a katastrální území Kladno-střed (dále jen „Nemovitost") a prohlašuje, že jeho vlastnické právo k uvedené nemovitosti je nesporné, je oprávněn s ní volně nakládat a jeho smluvní volnost není ničím omezena.

II. Kupní cena

Prodávající prodává kupujícím nemovitost uvedenou v čl. I. této smlouvy za dohodnutou kupní cenu ve výši 2 050 000,- Kč (slovy: dvamilionypadesáttisíc korun českých) a Kupující tuto nemovitost za takto dohodnutou kupní cenu kupují do svého výlučného vlastnictví.

???

III. Platba

Kupní cena uvedená v čl. II. bude uhrazena následujícím způsobem:

1. Část kupní ceny ve výši 1 625 000,-Kč (slovy: jedenmilionšestsetdvacetpěttisíc korun českých) uhradili Kupující Prodávajícímu v hotovosti při podpisu této smlouvy.
2. Zbylou část kupní ceny ve výši 425 000-Kč (slovy: čtyřistadvacetpěttisíc korun českých) předal Kupující při podpisu této smlouvy v hotovosti do úschovy zprostředkovateli ing.Petrovi Jasnému, IČ 125456789222. Tato částka bude zprostředkovatelem převedena na účet Prodávajícího č. 00045789654/0900, vedený u Evropské národní banky, a.s. v Brně, do 15 dnů po převodu vlastnického práva k předmětné Nemovitosti na jména Kupujících a po předložení výpisu z katastru nemovitostí, kde jako vlastník Nemovitosti budou uvedeni výlučně Kupující, části „C" a „D" budou bez zápisu a rovněž na předloženém listu vlastnictví nebude žádná plomba.

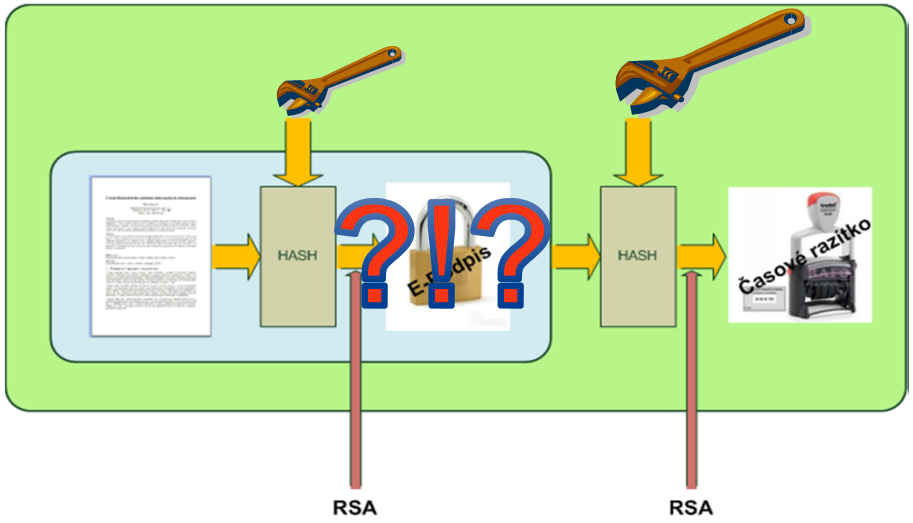
Malá lekce z historie – Algoritmus MD5

- Používal se jako součást elektronického podpisu
- Vytvořil jej jeden z největších světových kryptologů Ron Rivest (podílel se např. na RSA)
- 1995 – Hans Dobertin našel kolize v tzv. kompresní funkci – MD5 jako celek však ohrožen ještě nebyl
- 2004 – čínští kryptologové našli kolize pro úplný algoritmus MD5 – algoritmus byl vyřazen jako nevyhovující po stránce bezpečnosti – nalezení kolizí = 1 hodina
- 2005 – demonstrace vytvoření dvou různých certifikátů s různými veřejnými klíči a stejnou hodnotou MD5 hash
- 2006 – Klíma nalezl vylepšení, umožňující nalezení kolizí během 1 minuty na standardním notebooku
- 2010 – dramatické vylepšení původního útoku na MD5, zatím utajováno

Stále si ještě myslíte, že v budoucnosti budou dnešní opatření stačit?

Blízká budoucnost

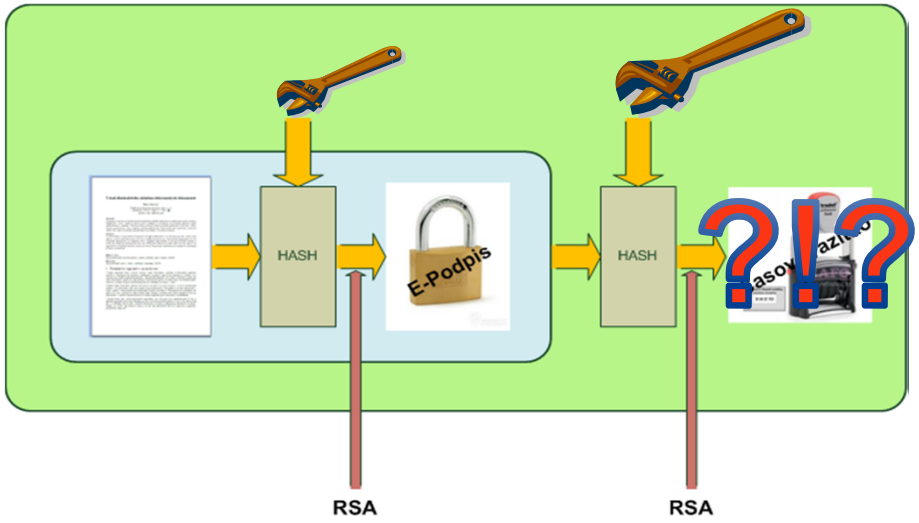
- Algoritmus RSA je stále ještě odolný,
- Odolnost SHA1 pomalu končí (cca 1 rok?)
- SHA 2 se zatím drží, ale …



- Rozdíl mezi e-podpisem a časovým razítkem je pouze ve velikosti klíče
- Podpis už „bezpečný“ není, časové razítko ano

Vzdálená budoucnost

- Algoritmus RSA je prolomen,
- SHA1 je minulostí
- SHA 2 je prolomen



- Lze lehce vyrobit časové razítko z doby před x lety, o podpisech z této doby ani nemluvě
- Dokonce můžeme postupovat takovým způsobem, že e-podpis vlastního dokumentu „napasujeme“ na e-podpis skutečného dokumentu

Garantovaná a bezpečná archivace dokumentů

Co může hrozit

Několik příkladů

- Neautorizované změny dokumentů
- Podvrhy dokumentů
- Podvrhy podpisů pod dokumenty
- Vyvracení podpisů pod dokumenty
- Posuny dokumentů v čase podle potřeby
- Atd…

Stále si ještě myslíte, že v budoucnosti budou dnešní opatření stačit?

Garantovaná a bezpečná archivace dokumentů

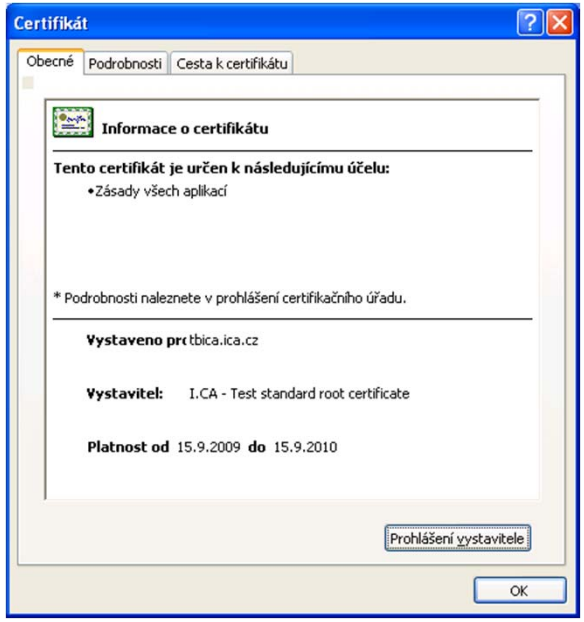
Co s tím ?

Co se musí zajistit

- Aplikace řetězce časových razítek

To ale nestačí – je třeba dělat více

- Uchovávat certifikáty časových autorit
- Uchovávat certifikáty systému certifikačních autorit
- Uchovávat všechny ostatní relevantní certifikáty
- To vše zabezpečeným způsobem



Dokument „Politika vydávání kvalifikovaných časových razítek PostSignum TSA“ (*kap. 7.3.4.1 Platnost kvalifikovaného časového razítka*)

- *Pokud je kvalifikovaný systémový certifikát TSU **neplatný** vzhledem k uvedené době platnosti v certifikátu (skončila mu platnost), **není standardními kontrolami možné ověřit platnost časového razítka**. V daném případě je podle potřeb spoléhající se strany nezbytné použít dodatečná opatření. Mezi tato opatření může patřit například:*
  - ***„přeorazítkování“** v době platnosti kvalifikovaného systémového certifikátu TSU,*
  - *kontrola, že certifikát TSU nebyl zneplatněn a že nedošlo k oslabení použitých kryptografických algoritmů,*
  - *protokolární uložení dat na nepřepisovatelné médium,*
  - *protokolární převod dat do papírové formy,*
  - *použití nadstandardních kontrol uvedených v [TS 102023], příloze D.*
  - *TSU – Time Stamp Unit – zařízení „produkující“ časová razítka*

Stačí jedna časová autorita?

Dokument „Politika vydávání kvalifikovaných časových razítek PostSignum TSA“ (*kap. 7.3.4.1 Platnost kvalifikovaného časového razítka*):

Pokud byl kvalifikovaný systémový certifikát TSU zneplatněn s následujícími důvody zneplatnění:

- keyCompromise (1),
- caCompromise (2),
- nebo bez uvedeného důvodu pro zneplatnění,

je časové razítko, pro jehož ověření je uvedený certifikát používán**, neplatné (a to i zpětně)**.

Jedna časová autorita může být málo – dvě jsou lepší !

Garantovaná a bezpečná archivace dokumentů

O2 Smart Trusted Archive

Co je O2 Smart Trusted Archive (O2STA):

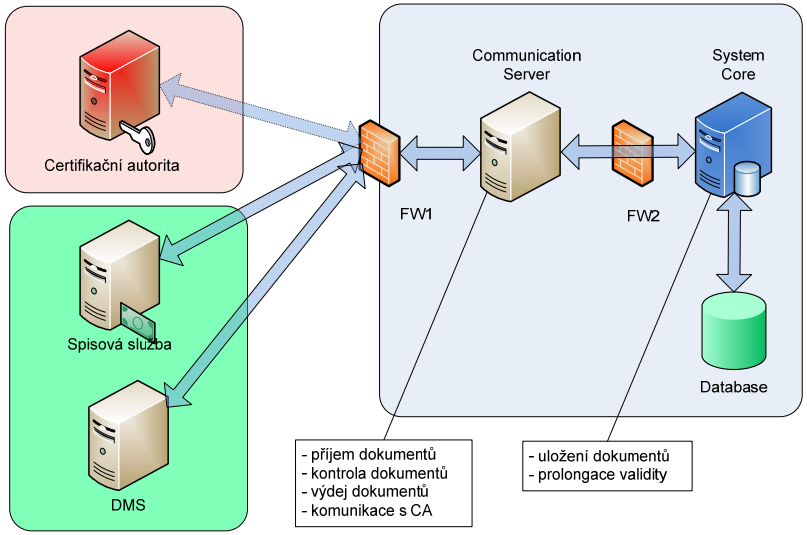
- Modul realizující důvěryhodné úložiště schopné dlouhodobě uchovávat dokumenty bez narušení vlastností
  - integrity
  - časového určení
  - neodvolatelnosti odpovědnosti

- Zajišťuje
  - kontrolu atributů ukládaného dokumentu
  - přidání dalších nezbytných doplnění dokumentu
  - pravidelnou kontrolu jejich validitu
  - tvorbu důkazního materiálu

- **To vše bez závislosti na vnějším okolí (včetně CA)!**

Garantovaná a bezpečná archivace dokumentů

Funkčnosti O2STA

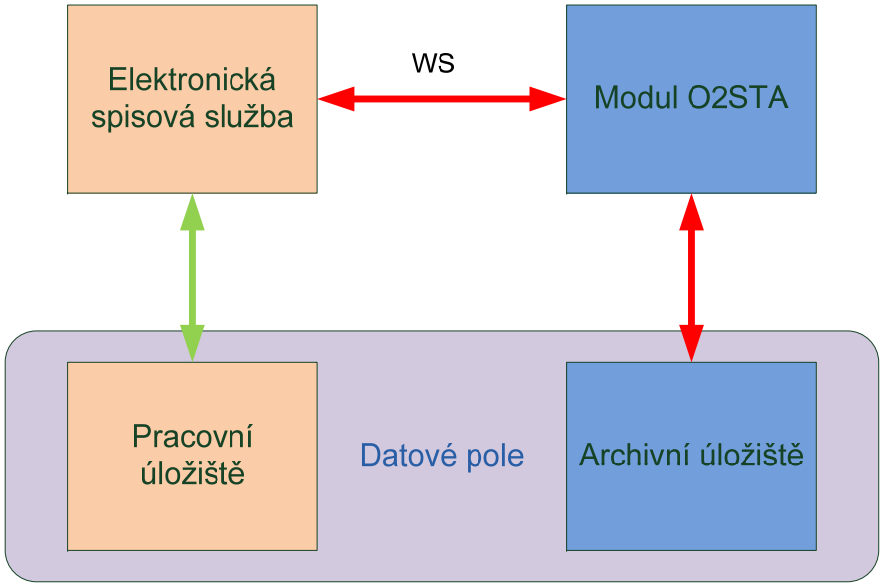


Důvěryhodné úložiště zajišťuje

- příjem dokumentů ze zdrojových systémů
- přidání archivní elektronické značky
- vystavení nového časového razítka
- kontrolu atributů dokumentu a kontrolu elektronických podpisů a časových razítek s dokumentem spojených - **karanténa**
- uložení do úložiště
- pravidelnou kontrolu validity a opatřování následnými časovými razítky
- poskytování informací o dokumentech
- poskytování důkazů o validitě dokumentů

Garantovaná a bezpečná archivace dokumentů

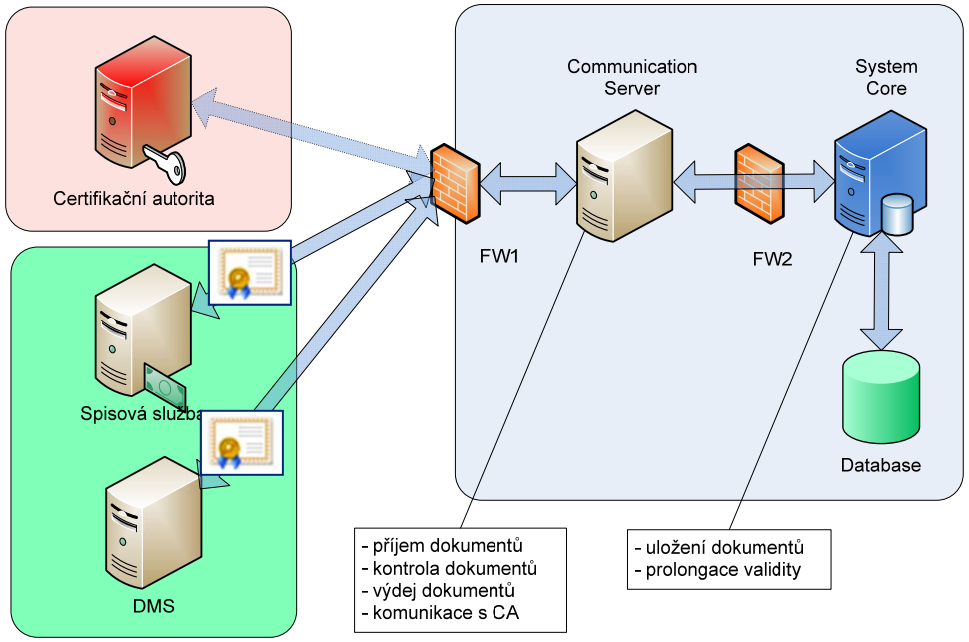
O2STA - využití



- O2STA může sloužit jako přídavný modul k jiné aplikaci (např. spisové službě)
- Důvěryhodné úložiště není pracovním úložištěm
  - Do DA přicházejí dokumenty, u nichž je nezbytné zachovat obsah včetně atributů
  - Pokud se má dokument dále měnit, do archívu lze ukládat jednotlivé verze
- Propojení pomocí WS
- Možnost napojení přes sdílený diskový prostor

Garantovaná a bezpečná archivace dokumentů

Co s tím ?



- Modul důvěryhodného úložiště nemá souborový přístup:
  - jakákoliv manipulace na základě elektronicky podepsané žádosti
  - k podpisu žádosti se používá kvalifikovaný certifikát,
  - žádosti se archivují stejně jako dokumenty
- Důležité z pohledu pozdějšího prokazování aktivit
- Základní typy žádostí
  - Uložení dokumentu
  - Vyzvednutí dokumentu
  - Vyzvednutí důkazu
  - Skartace dokumentu

Garantovaná a bezpečná archivace dokumentů

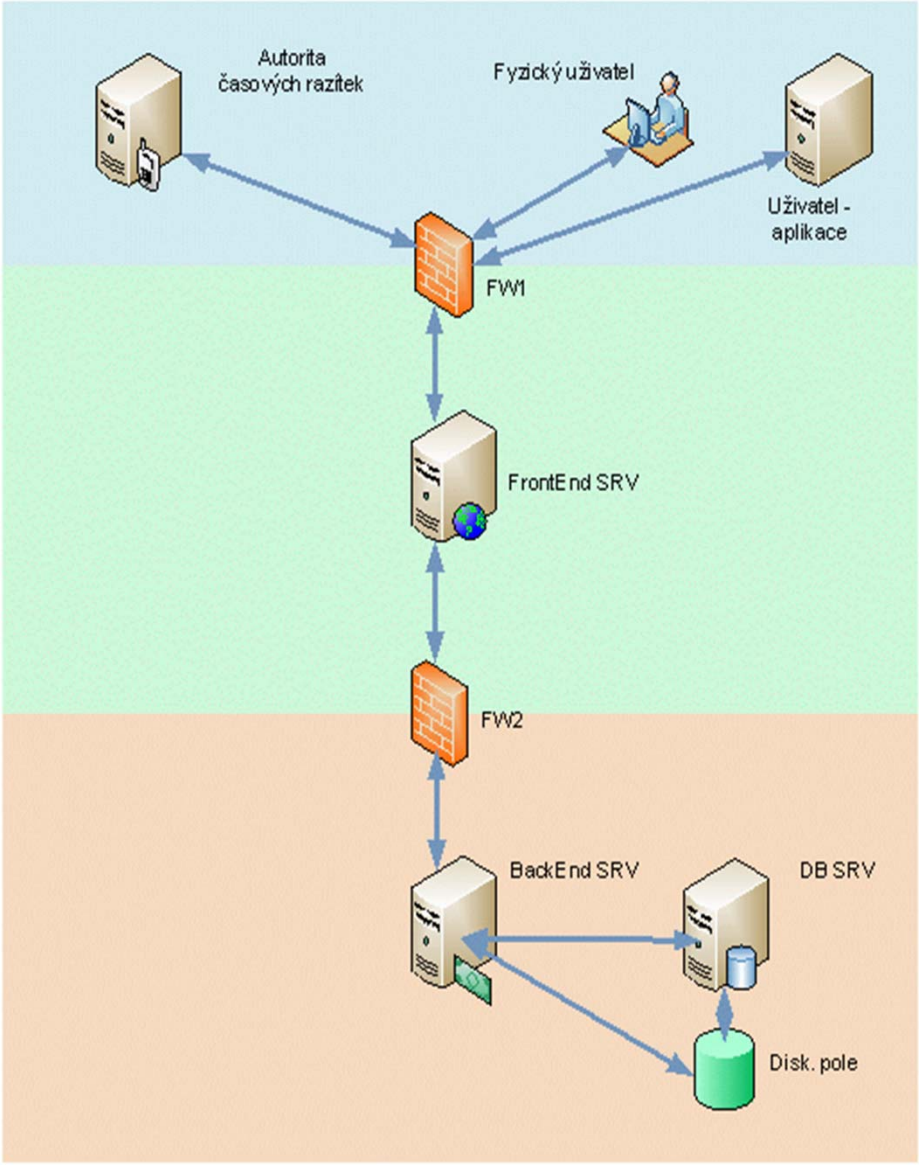
O2STA

Formy realizace:

Typ	HW	Aplikace
Na klíč u zákazníka	•Dodávka •Instalace OS •Konfigurace OS	•Instalace •Konfigurace •Nastavení politik
Na HW zákazníka	•Konfigurace OS	•Instalace •Konfigurace •Nastavení politik
Hosting Telefonica	•Zprovoznění v HC	•Instalace •Konfigurace •Nastavení politik
Služba v DC Telefonica (formou měsíční platby)	•Zprovoznění v HC	•Instalace •Konfigurace •Nastavení politik

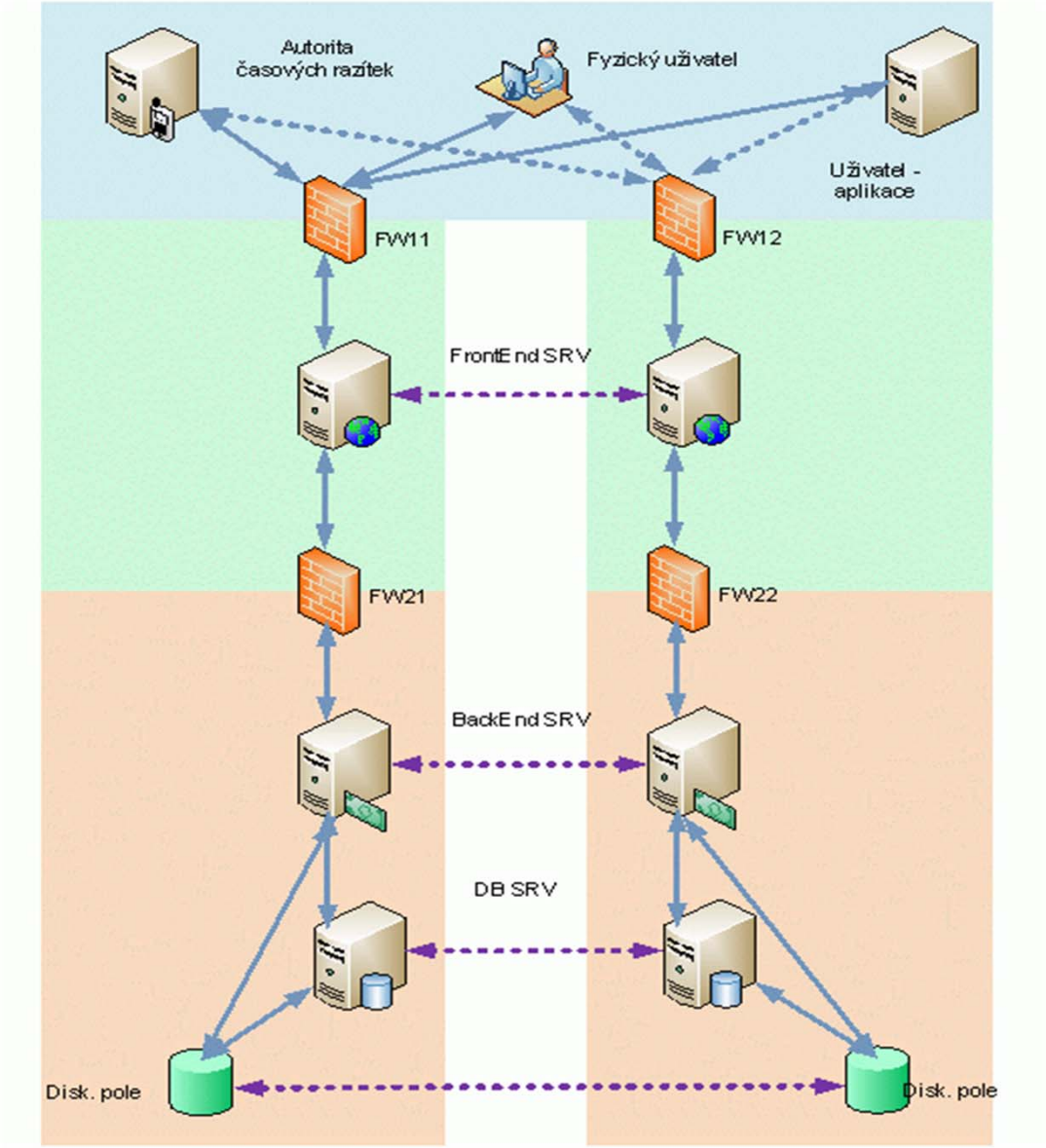
Garantovaná a bezpečná archivace dokumentů

Jednoduchá architektura



Garantovaná a bezpečná archivace dokumentů

HA architektura



Garantovaná a bezpečná archivace dokumentů

Certifikováno

ELEKTROTECHNICKÝ ZKUŠEBNÍ ÚSTAV

ELECTROTECHNICAL TESTING INSTITUTE - CZECH REPUBLIC
ELEKTROTECHNISCHE PRUFANSTALT - TSCHECHISCHE REPUBLIK
INSTITUT ELECTROTECHNIQUE D'ESSAIS - RÉPUBLIQUE TCHÈQUE
ЭЛЕКТРОТЕХНИЧЕСКИЙ ИСПЫТАТЕЛЬНЫЙ ИНСТИТУТ - ЧЕШСКАЯ РЕСПУБЛИКА

Pod Lisem 129, 171 02 Praha 8 - Troja

CERTIFIKÁT

č.: 1100949

Výrobek: SW modul informačního systému

Typ: O2STA - Důvěryhodné úložiště

Objednavatel: Telefónica O2 Czech republic, a. s.
Za Brumlovkou 266/2, 140 22 Praha 4-Michle, Česká republika

Výrobce: Telefónica O2 Business Solutions, spol. s r.o.
Kodaňská 1392, 100 00 Praha 10 - Vršovice, Česká republika

Obchodní značka: O2STA - Důvěryhodné úložiště

Výsledky zkoušek jsou uvedeny v protokolu č.: 004879-01 ze dne: 17.12.2010

Vzorek zkoušeného výrobku je ve shodě s požadavky:
Čl. 5.5 ČSN ISO/IEC 15288, § 68, 69a zákona č. 499/2004 Sb., § 16 vyhlášky č. 191/2009 Sb. a čl. 3.1.2, 3.1.3 a 4.3 Národního standardu pro vedení elektronického systému spisové služby

Platnost certifikátu je omezena do: 31.12.2013

30.12.2010
V Praze dne

Mgr. Miroslav Sedláček
Vedoucí certifikačního orgánu

Elektrotechnický zkušební ústav, s.p. Pod Lisem 129, 171 02 Praha 8 - Troja
razítko

004879-01

A Telefónica company


Děkuji Vám za pozornost
Miroslav Šedivý, Telefónica CZ
Miroslav.Sedivy@o2bs.com
A Telefónica company