Zaručená archivace elektronických dokumentů …

… hezké, ale co s tím?

Moderní metody nejsou nedostupné!

RNDr. Miroslav Šedivý
Telefónica CZ

Důvěryhodné ukládání dokumentů

Úvod

Něco málo definicí:

- Atributy důvěryhodnosti
  - Integrita dokumentu
  - Původ dokumentu
  - Časové umístění dokumentu

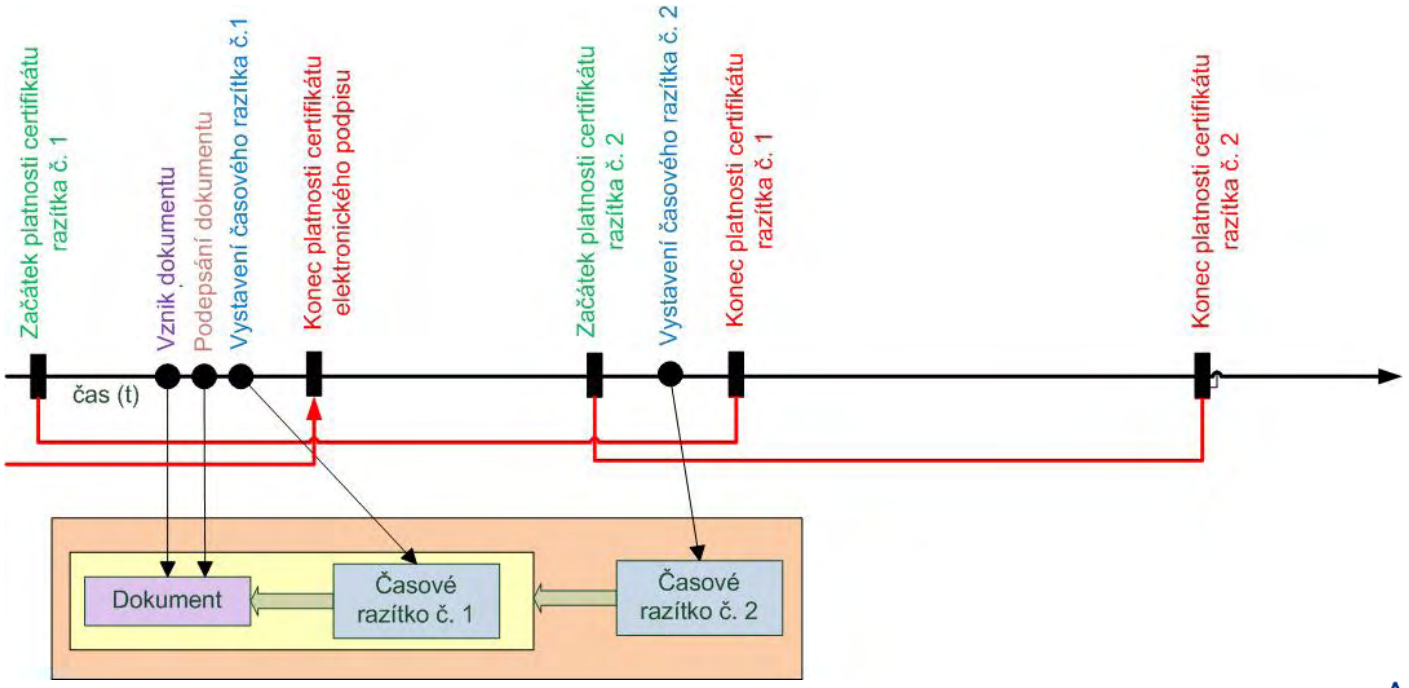
- Důvěryhodný dokument – dokument se zajištěnými a prokazatelnými atributy důvěrnosti

- Důvěryhodné (dlouhodobé) ukládání – správa dokumentů zajišťující důvěryhodnost dokumentů v dlouhodobém horizontu

Důvěryhodné ukládání dokumentů

Prostředky pro zajištění důvěryhodnosti – kryptografické metody

- Elektronický podpis + kvalifikovaný certifikát
  - Zajištění integrity
  - Zajištění původu dokumentu (nebo odpovědnosti aktérů)
- Časové razítko
  - Časové umístění dokumentu

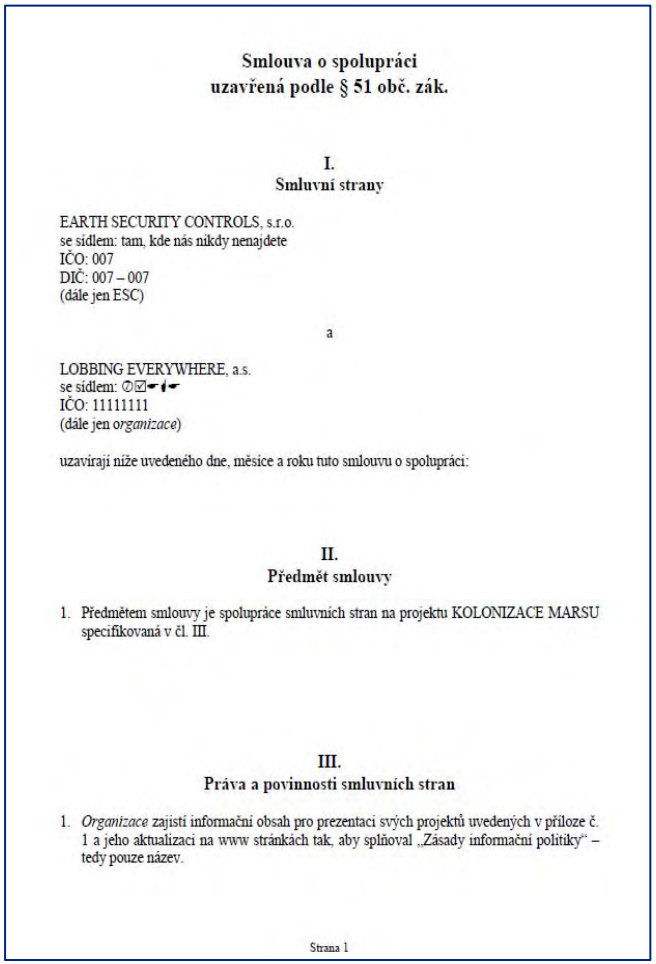


4 Důvěryhodné ukládání dokumentů

Nová opatření přinášejí nová rizika

Hrozby

- zneplatnění nebo expirace certifikátu
- oslabení algoritmů
- nefunkčnost CA
- ukončení činnosti CA



Smlouva o spolupráci
uzavřená podle § 51 obč. zák.

I.
Smluvní strany

EARTH SECURITY CONTROLS, s.r.o.
se sídlem: tam, kde nás nikdy nenajdete
IČO: 007
DIČ: 007 – 007
(dále jen ESC)

a

LOBBING EVERYWHERE, a.s.
se sídlem: ✆☑☛☛
IČO: 11111111
(dále jen *organizace*)

uzavírají níže uvedeného dne, měsíce a roku tuto smlouvu o spolupráci:

II.
Předmět smlouvy

1. Předmětem smlouvy je spolupráce smluvních stran na projektu KOLONIZACE MARSU specifikovaná v čl. III.

III.
Práva a povinnosti smluvních stran

1. *Organizace* zajistí informační obsah pro prezentaci svých projektů uvedených v příloze č. 1 a jeho aktualizaci na www stránkách tak, aby splňoval „Zásady informační politiky" – tedy pouze název.

Strana 1

RIZIKA

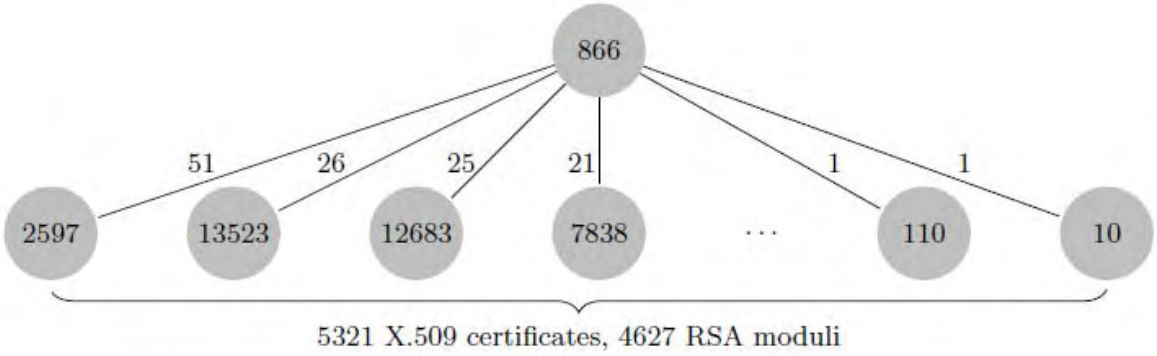
- narušení integrity
- neprokazatelnost časového umístění
- neplatnost elektronických podpisů
- neprokazatelnost elektronických podpisů

Důvěryhodné ukládání dokumentů

Nikdo není dokonalý

Něco málo faktů:

- Pouhých 10 let trvalo, než byl prolomen algoritmus MD5, navržený jedním z nejlepších kryptologů
- Zpráva skupiny matematiků a kryptologů o stavu používání kryptografie v roce 2011
  - Testováno 11,4 miliónů RSA certifikátů
  - 26965 nebezpečných (lze získat privátní klíče)
  - Použití „kombinovaných“ modulů
- **Závěr – archivace elektronických dokumentů vyžaduje odborný přístup**



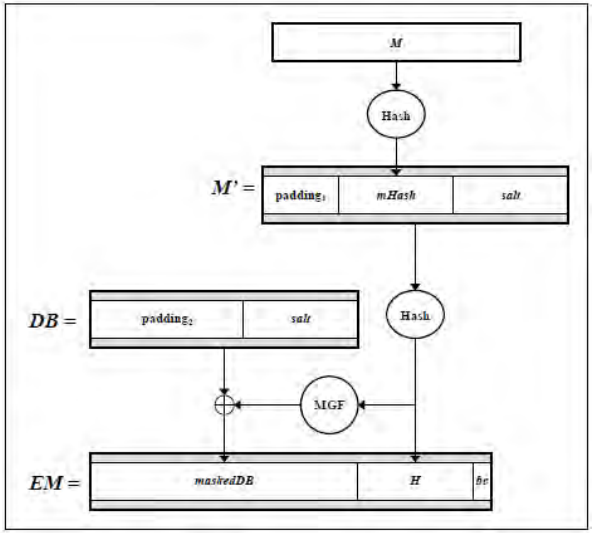
Zdroj: Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter: „Ron was wrong, Whit is right“, IACR 2012, *eprint.iacr.org/2012/064.pdf*

Služby v oblasti správy důvěryhodných dokumentů

Historie

O_2 Smart Trusted Archive (O2STA):

- Dlouholetý vývoj
  - 2007 – 2008 : analýzy, příprava pro vývoj
  - 2009 – dosud : vývoj, vylepšování
  - Od 2011 dostupný i jako služba
  - Od tohoto roku dostupný prostřednictvím O_2Cloud

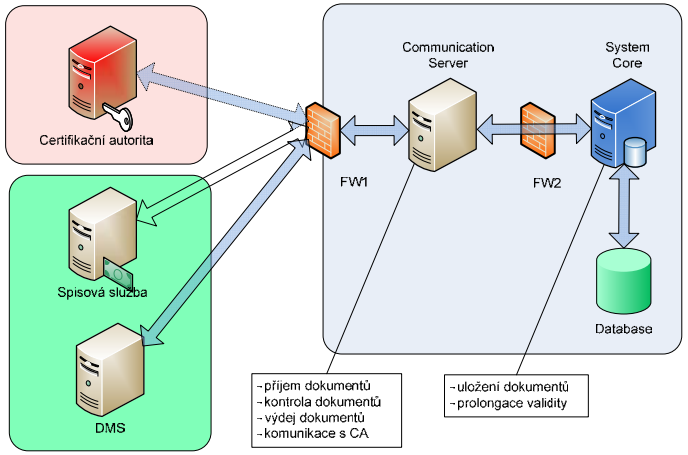


Služby v oblasti správy důvěryhodných dokumentů

Vlastnosti O2STA

Základní vlastnosti:

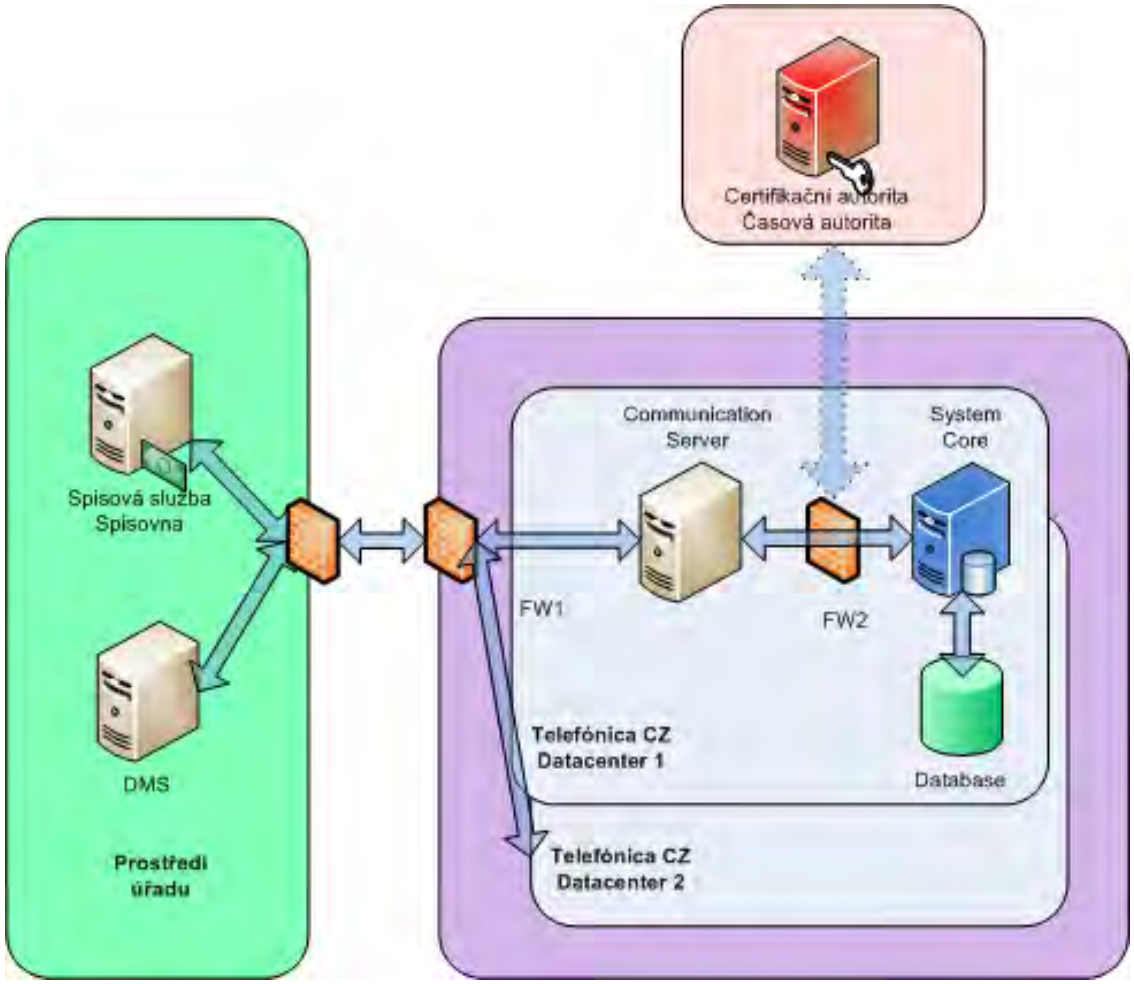
- Snadná integrace se stávajícími systémy
  - Rozhraní web services
  - Alternativně rozhraní „shared disk“
- Autonomní archivace (archivuje se vše potřebné, v budoucnosti již není potřeba nic dohledávat)
- Striktní řízení přístupu
- V oblasti zabezpečení dokumentů jde nad požadavky standardů (CAdES, XAdES, PAdES)
- Zcela stabilní i v případě prolomení dříve používaných algoritmů
- Odolný proti pádu certifikačních a časových autorit



Služby v oblasti správy důvěryhodných dokumentů

O2STA jako služba

- V nabídce od poloviny roku 2011
- Data zcela pod vlastní správou
- Snadné napojení

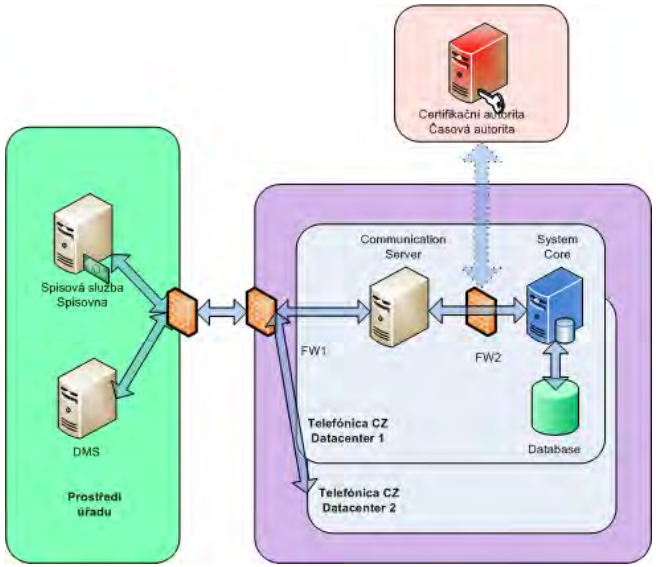


Služby v oblasti správy důvěryhodných dokumentů

O2STA jako služba

Výhody:

- Spojuje výhody outsourcingu a vlastní správy
- Není nutné investovat do infrastruktury
- Řešení roste s potřebami úřadu
- K dispozici zkušený tým řešící specifické potřeby úřadu
- Možnost využít další služby bezpečnosti (Web Security Gateway apod.)



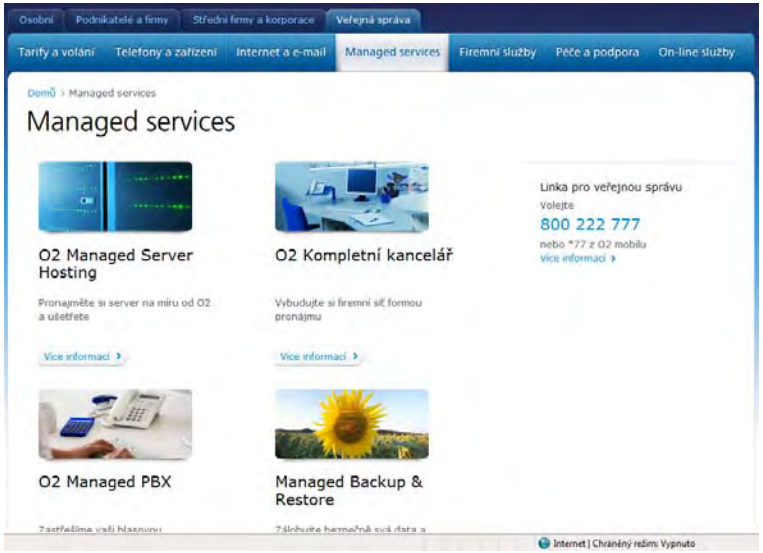
- **A především odborná péče zajištěna zkušenými specialisty společnosti Telefónica CZ**

Služby v oblasti správy důvěryhodných dokumentů

O2STA jako služba

Varianty:

- Samostatné řešení na bázi standardních MHS (managed hosting services)
- Totéž v prostředí O2Cloud
- Řešení na bázi nové služby MHS – Managed Archive (spouští se od ½ roku 2012)

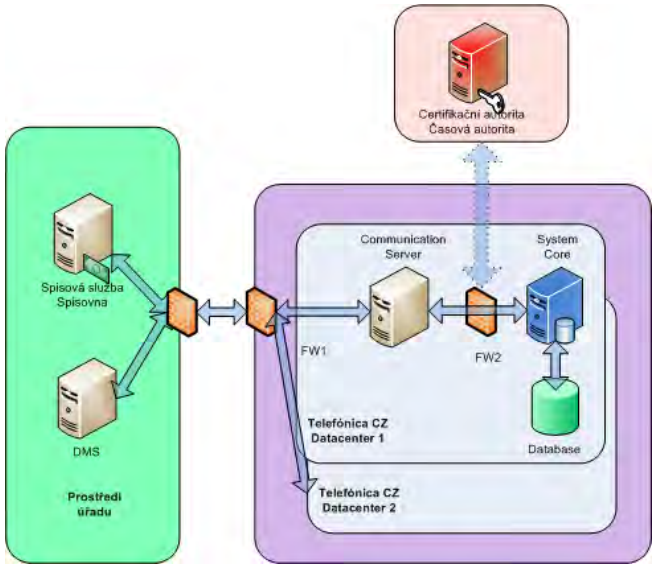


Služby v oblasti správy důvěryhodných dokumentů

Standardní MHS

Výhody:

- Oddělené řešení (individuální O2STA)
- Možnost parametrizace na požádání (výkon, datový prostor)
- Přehledná struktura poplatků
- Možnost využití prostředí DMS (varianta O2STA-I)
- K dispozici testovací aplikace, umožňující rychlý vývoj interface na bázi WS pro vlastní aplikace
- Před vlastním rozhodnutím možnost vyzkoušet (prostředí **Try&Buy**) včetně vyzkoušení napojení vlastních aplikací

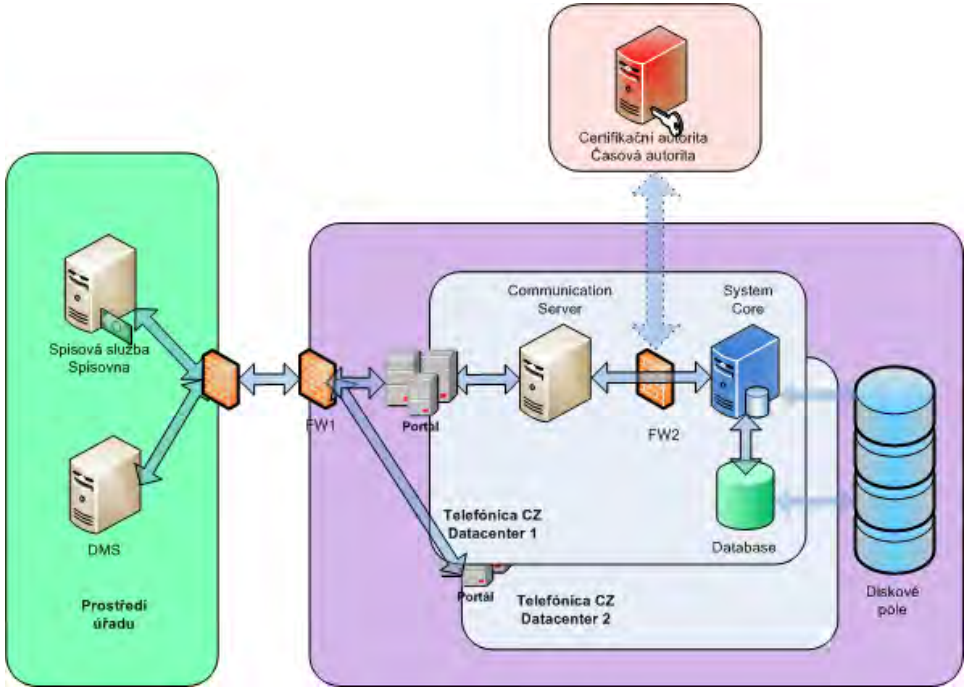


Služby v oblasti správy důvěryhodných dokumentů

Nová služba MHS – Managed Archive

Výhody:

- Logicky oddělené prostory
- Možnost parametrizace na požádání (datový prostor)
- Přehledná struktura poplatků
- K dispozici je portál pro přístup k O2STA



Služby v oblasti správy důvěryhodných dokumentů

Certifikováno na shodu se zákonem o archivnictví

ELEKTROTECHNICKÝ ZKUŠEBNÍ ÚSTAV

ELECTROTECHNICAL TESTING INSTITUTE - CZECH REPUBLIC
ELEKTROTECHNISCHE PRÜFANSTALT - 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

razítko

004879-01


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