Ako začať využívať elektronickú podateľňu

- bezpečnostné, technické a legislatívne aspekty

27. október 2003
Hotel Forum, Bratislava

Rastislav Machel, CISSP
Consultant, META Group CESE

itapa 2003
Bratislava

Agenda

- Čo je elektronická podateľna
- Ako sa dozvieme, že úrad zriadil elektronickú podateľňu
- Elektronická podateľňa a okolie
- Ako na to?
- Elektronická podateľna využívajúca službu časových pečiatok ACA
- Elektronická podateľňa s vlastným bezpečným zariadením na vyhotovovanie časovej pečiatky
- Bezpečné zariadenie na vyhotovovanie časovej pečiatky
- Dôveryhodný zdroj času
- Príklady zariadení pre konštrukciu elektronickej podateľne

Čo je elektronická podateľňa

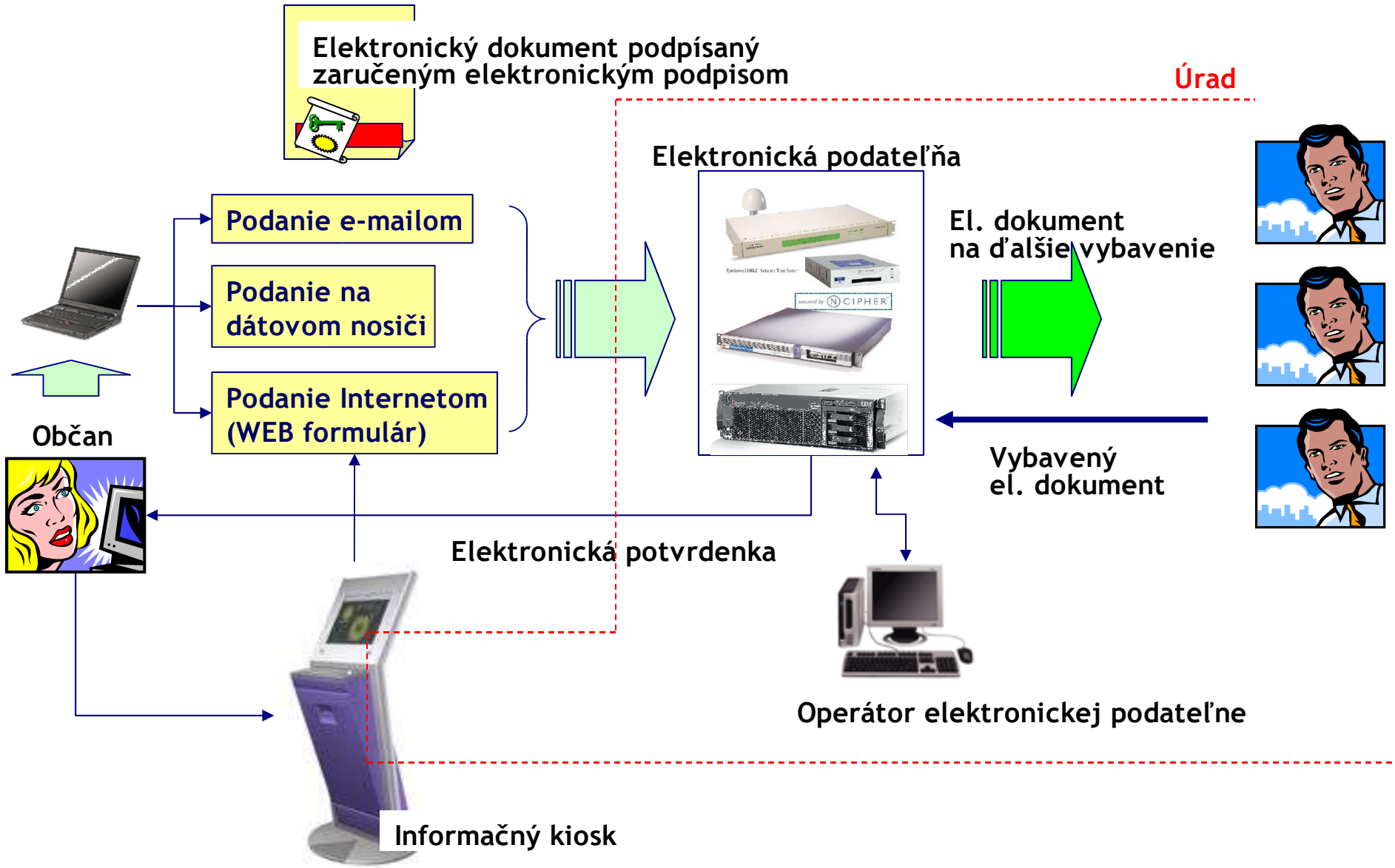
- **Elektronická podateľňa** umožňuje aby úrad, čiže orgán verejnej moci alebo orgán verejnej správy (napríklad daňový úrad, súd, krajský, mestský, obecný alebo iný úrad), mohol prijať elektronický dokument podpísaný zaručeným elektronickým podpisom

- Elektronická podateľňa (minimálne) **zabezpečuje**
  - **Prijímanie, odosielanie, overovanie, potvrdzovanie a spracovanie** elektronických dokumentov prostredníctvom
    1. siete na prenos údajov,
    2. elektronickej pošty,
    3. štandardných nosičov údajov,
  - **Kontrolu** prijímaných elektronických dokumentov – dodržanie ustanoveného formátu a obsahu, neprítomnosť škodlivých kódov (makrá, vírusy a pod.)
  - **Overenie platnosti kvalifikovaného certifikátu** viazaného na zaručený elektronický podpis elektronického dokumentu
  - **Potvrdenie o prijatí** alebo **odmietnutí** elektronického dokumentu vydaním vlastného elektronického dokumentu s použitím časovej pečiatky
  - Odoslanie elektronického dokumentu na ďalšie vybavenie (v úrade)
  - Prijatie elektronického dokumentu vybaveného alebo vytvoreného úradom na jeho odoslanie mimo úradu (napr. na iný úrad alebo fyzickej osobe žiadajúcej o vybavenie určitej veci)

Ako sa dozvieme, že úrad zriadil elektronickú podateľňu

- Úrad po zriadení el. podateľne je povinný zverejniť
  - Zoznam úplných elektronických adries umožňujúcich styk s elektronickou podateľňou
  - Adresu umiestnenia elektronickej podateľne a adresu, na ktorej možno s úradom komunikovať o otázkach využívania a činnosti elektronickej podateľne
  - Zoznam kvalifikovaných certifikátov alebo úplnú elektronickú adresu, na ktorej sa nachádza zoznam kvalifikovaných certifikátov všetkých zamestnancov úradu, ktorí zabezpečujú prevádzku elektronickej podateľne
  - Formáty elektronických dokumentov, ktoré elektronická podateľňa prijíma (z množiny prípustných formátov podľa prílohy č. 3 vyhlášky NBÚ č. 542/2002 Z.z.)
  - Typy a charakteristiky nosičov údajov, na ktorých elektronická podateľňa elektronické dokumenty prijíma
  - Pravidlá zasielania elektronických dokumentov a potvrdzovania ich prijatia vrátane možného časového obmedzenia styku s elektronickou podateľňou
  - Zoznam typov prijímaných elektronických dokumentov a spôsob získania elektronických predlôh podaní
- Tieto informácie úrad zverejní písomnou formou a elektronickou formou prostredníctvom siete na prenos údajov (prostredníctvom Internetu)

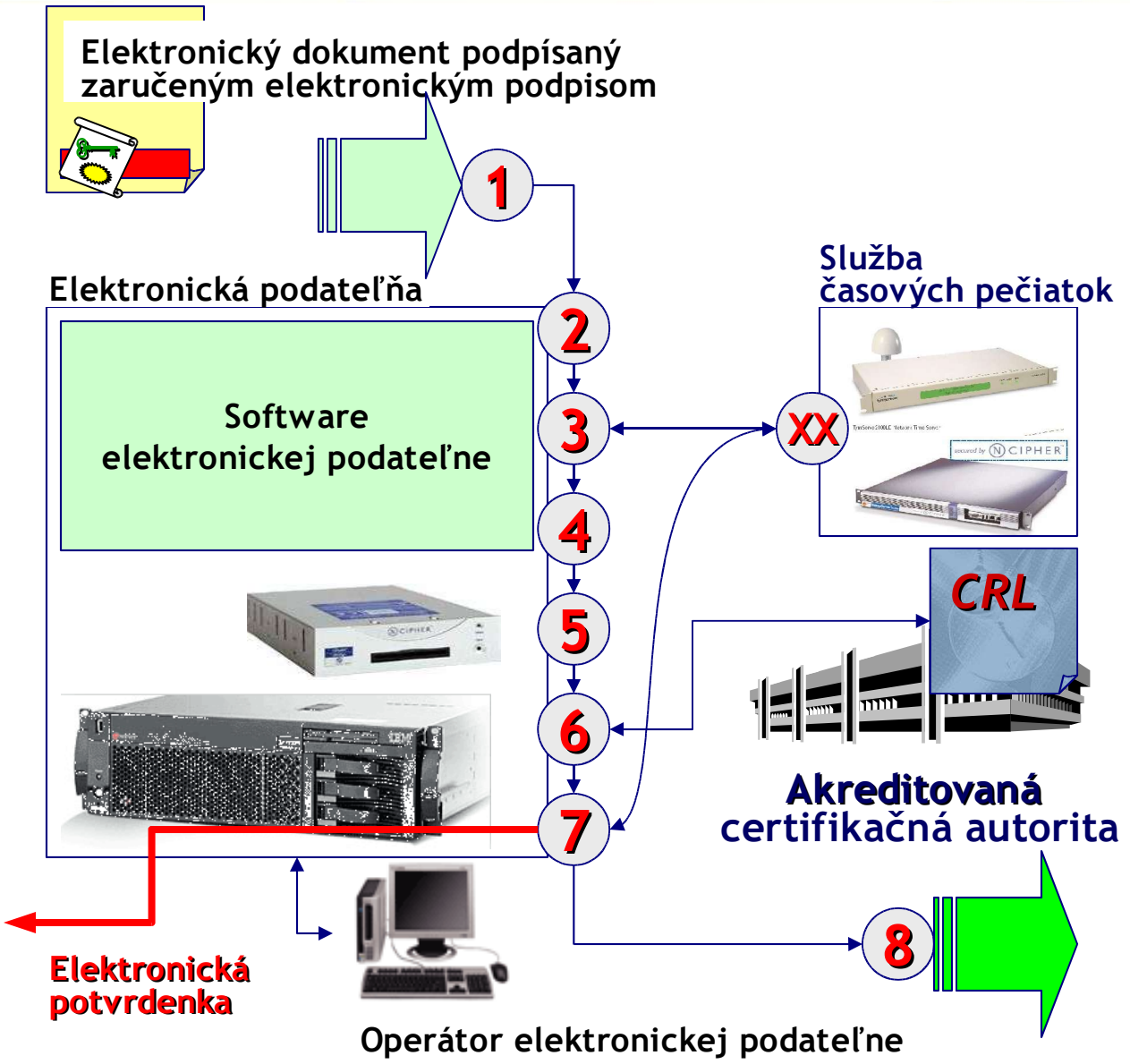
Elektronická podateľňa a okolie



- Ako na elektronickú podateľňu?
  - Elektronická podateľňa **využívajúca služby časových pečiatok** akreditovanej certifikačnej autority (alebo akreditovaného poskytovateľa služieb časových pečiatok)
  - Elektronická podateľňa **s vlastným bezpečným zariadením** na vyhotovovanie časovej pečiatky

- Na praktické využívanie elektronického podpisu je potrebné
  - Vytvorenie (a sprístupnenie občanom) technickej infraštruktúry pre elektronickú komunikáciu s využitím elektronického podpisu (najmä aplikácie podporujúce elektronický podpis)
  - Občania musia mať záujem komunikovať efektívne (a teda pri komunikácii vo zvýšenej miere využívať elektronický podpis)
  - Úrady musia uviesť do činnosti elektronické podateľne

El. podateľňa využívajúca službu časových pečiatok



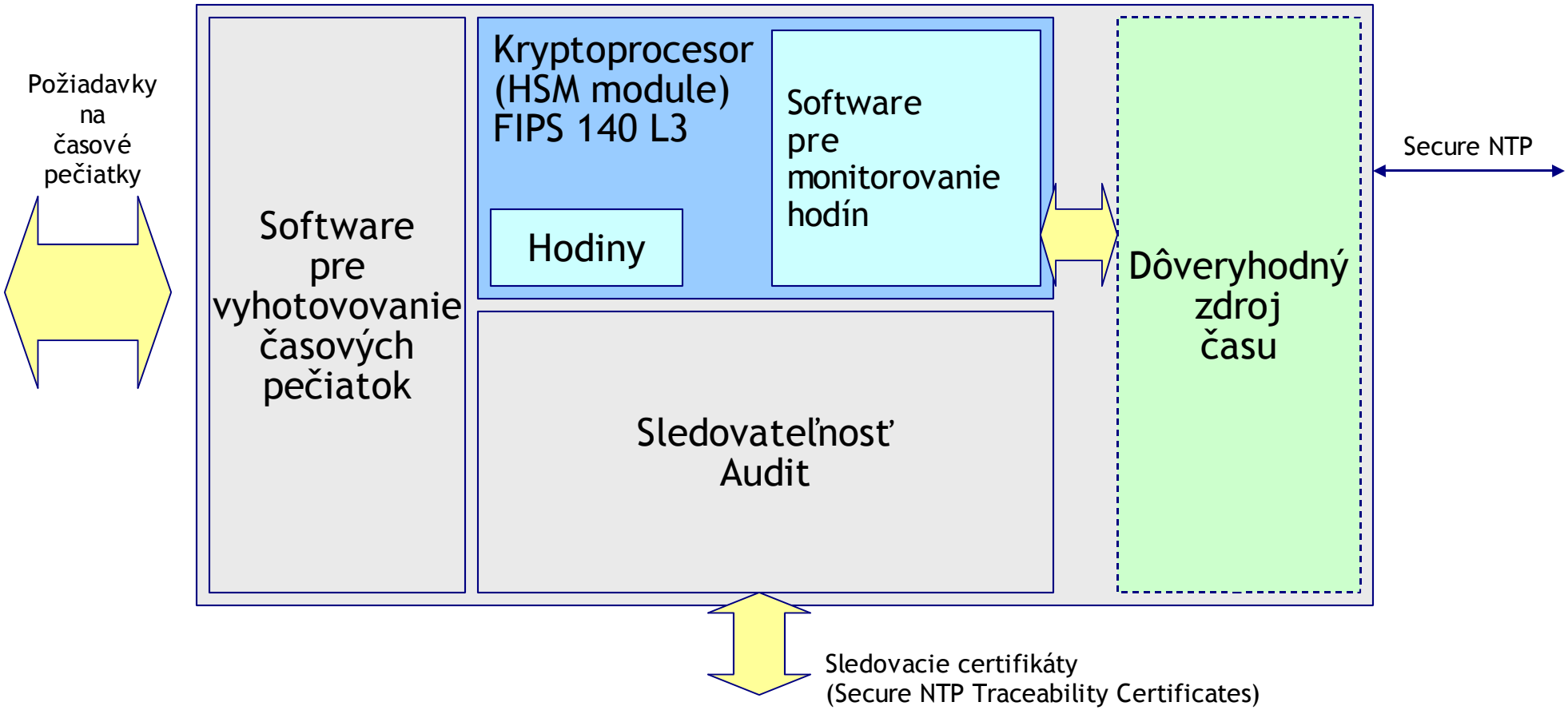
1. Prijatie elektronického dokumentu
2. Zaradenie do frontu prijatých dokumentov
3. Priradenie časového údaja prijatia dokumentu
4. Zápis do zoznamu prijatých dokumentov
5. Preskúmanie el. dokumentu a rozhodnutie o jeho prijatí alebo odmietnutí
6. Ak je dokument vyhovuje pravidlám, overenie platnosti kvalifikovaného certifikátu, zaručeného el. podpisu, integrity dokumentu
7. Ak je overenie podľa bodu 6 je OK, zaradenie do frontu overených prijatých dokumentov a vydanie el. potvrdenky, v opačnom prípade vyradenie z frontu prijatých dokumentov, záznam do zoznamu prijatých dokumentov a odmietnutie dokumentu
8. Vybratie z frontu overených prijatých dokumentov a postúpenie na ďalšie spracovanie

XX vyžiadanie časovej pečiatky

El. podateľňa s vlastným bezpečným zariadením na vyhotovovanie časovej pečiatky

1. Prijatie elektronického dokumentu
2. Zaradenie do frontu prijatých dokumentov
3. Priradenie časového údaja prijatia dokumentu
4. Zápis do zoznamu prijatých dokumentov
5. Preskúmanie el. dokumentu a rozhodnutie o jeho prijatí alebo odmietnutí
6. Ak je dokument vyhovuje pravidlám, overenie platnosti kvalifikovaného certifikátu, zaručeného el. podpisu, integrity dokumentu
7. Ak je overenie podľa bodu 6 je OK, zaradenie do frontu overených prijatých dokumentov a vydanie el. potvrdenky, v opačnom prípade vyradenie z frontu prijatých dokumentov, záznam do zoznamu prijatých dokumentov a odmietnutie dokumentu
8. Vybratie z frontu overených prijatých dokumentov a postúpenie na ďalšie spracovanie

Bezpečné zariadenie na vyhotovovanie časovej pečiatky



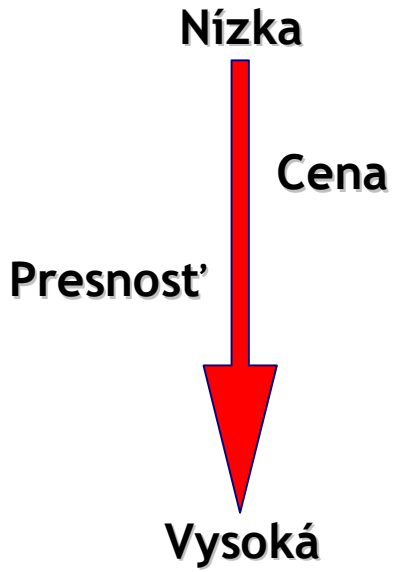
Čas ako globálny štandard

- ČAS je typický globálny štandard
- Reprezentácia času má veľa foriem
- Existuje viacero časových štandardov
  - TAI (International Atomic Time)
  - UT1 (Universal Astronomical Time)
  - **UTC (Universal Coordinated Time)**
- Jednotkou času je sekunda [s]

  (trvanie 9 192 631 770 períód žiarenia emitovaného pri prechode medzi dvoma veľmi jemnými úrovňami základného stavu atómu cézia 133)
- Reprezentácia času má veľa foriem
- TAI je definoval a udržiava BIPM (Bureau International des Poids et Mesures)
- TAI „nedrží krok" s nepravidelnou rotáciou zeme
- z praktických dôvodov bol definovaný UTC, ktorý je totožný s TAI, s výnimkou toho, že z času na čas je k TAI pridaná sekunda (tzv. „leap second")
- O dátumoch pridaní „leap second" rozhoduje IERS (International Earth Rotation Service)

Hodiny = stroj na meranie času

- Hodiny = oscilátor a počítadlo
- Oscilátory
  - Krištáľ (kremeňa)
    - Teplotne kompenzované (TCXO)
    - Mikroprocesorovo kompenzované (MCXO)
    - S reguláciou teploty (OCXO)
  - Atómové oscilátory
    - Rubídium
    - Cézium
    - Maser (vodík)
- Presnosť
  - Céziové hodiny NIST: 5×10^{-15} sekundy/deň
  - Rubídiové hodiny: 5×10^{-12} sekundy/deň
  - Hodiny s kremenným krištáľom: 10^{-6} sekundy /deň



Dôveryhodný zdroj času

- Potenciálne zdroje presného času
  - Krátkovlnné rádiové vysielače
    (napr. WWV, WWVB, WWVH, DCF-77, MSF 60 kHz, HBG 75 kHz,)
  - Mobilné telefónne siete (GSM, CDMA)
  - **GPS (Global Positioning System)**
  - Dôveryhodné, kalibrované NTP servery
    - poskytujú službu NTP, väčšinou tieto NTP servery využívajú viaceré nezávislé zdroje času (GPS, kalibrovaný zdroj NIST, CERN a pod).
- Pre systém elektronického podpisu:

nie je dôležité

vlastniť veľmi presné hodiny s atómovým oscilátorom,

ktoré sú nastavené na nesprávny čas (t.j. idú síce presne, ale nekorešpondujú s UTC),

ale **je nevyhnutný** dôveryhodný **zdroj** presného **času synchronizovaný s UTC**

- GPS ako zdroj presného času
  - Synchronizácia s UTC s odchýlkou menšou ako 200 ns (nano sekúnd)
  - Pre synchronizáciu postačuje priama viditeľnosť 1 satelitu GPS

Príklady zariadení pre konštrukciu el. podateľne

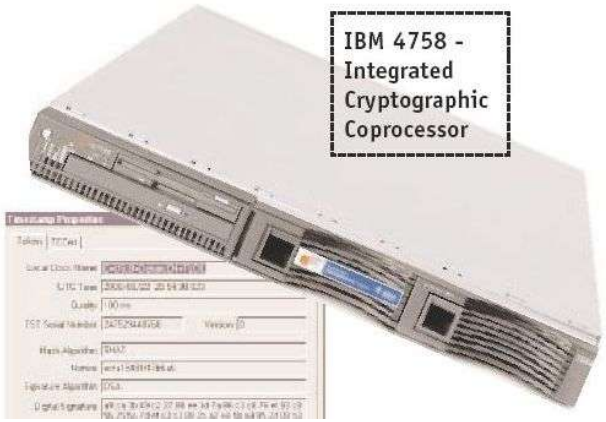
Zdroj presného času synchronizovaný s UTC (NTP server)

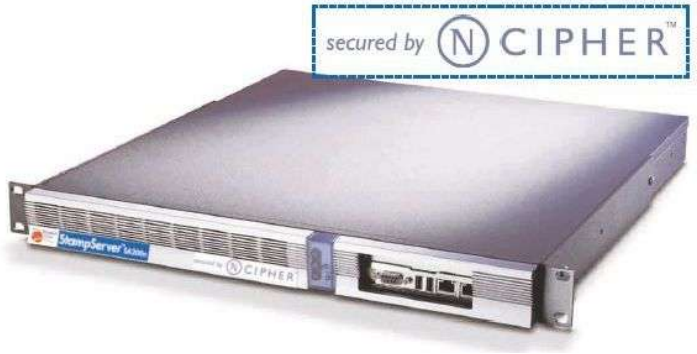
- Symmetricom TymServe 2100LD (http://www.ntp-systems.com)
  - Zdroj času: 8-kanálový GPS prijímač
  - Presnosť: max. odchýlka <10 mikrosekúnd (voči UTC)
  - Protokoly: TCP/IP, NTPv2 (RFC 1119), NTPv3 (RFC 1305)
    Daytime Protocol (RFC 867), Time Protocol (RFC 868)

TymServe 2100LD Network Time Server

Bezpečné zariadenie pre vyhotovovanie časových pečiatok

- Symmetricom Trusted Time StampServer SA100/SA200n (http://www.trusted-time.com)
  - Kalibrácia a audit zdroja času: služba Sovereign Time (http://www.wetstonetech.com/sovtime.html)
  - Implementovaný IETF PKIX Time Stamp Protocol (RFC 3161)
  - Výkon: SA 100: 50 časových pečiatok za sek. (1024 RSA sig.)
    SA 200n: 125 časových pečiatok za sek. (1024 RSA sig.)





Zhrnutie

- Na praktické využívanie elektronického podpisu je potrebné
  - Vytvorenie (a sprístupnenie občanom) technickej infraštruktúry pre elektronickú komunikáciu s využitím elektronického podpisu (najmä aplikácie podporujúce elektronický podpis)
  - Občania musia mať záujem komunikovať efektívne
    (a teda pri komunikácii vo zvýšenej miere využívať elektronický podpis)
  - Úrady musia uviesť do činnosti elektronické podateľne

- Praktické používanie je limitované
  - Existenciou vhodných komunikačných nástrojov
  - Schopnosťou preukázania, že tieto komunikačné nástroje sú spoľahlivé a bezpečné
  - Vôľou potenciálnych používateľov komunikovať s verejnou mocou elektronicky
  - Znalosťami potenciálnych používateľov komunikovať elektronicky
  - **Dôverou** potenciálnych používateľov

Otázky?

Viac informácií Vám poskytne:

Rastislav Machel, CISSP
Consultant META Group CESE
rastislav.machel@metagroup.com
+421-905-622435

Ďakujem za pozornosť!