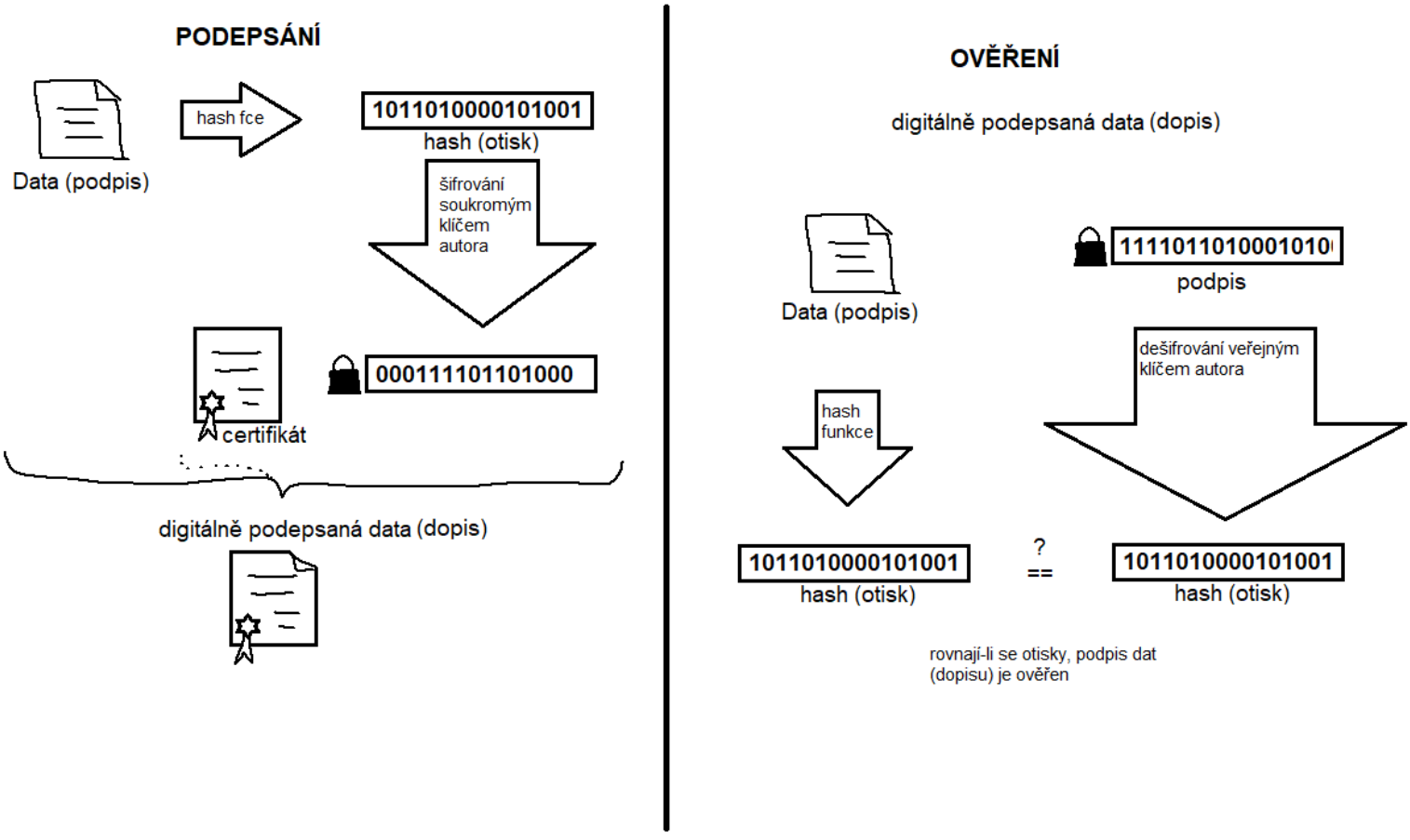
27.

Elektronický podpis (popis, použité funkce, získání, použití, omezení), certifikáty, zabezpečení dat před zneužitím a před ztrátou. Definujte a uveďte příklad využití redundance dat.

Význam jako reálný podpis jen elektronicky



POPIS

- el. podpis = označení specifických dat, které v počítači nahrazují klasický vlastnoruční podpis, respektive ověřený podpis
- připojen k datové zprávě nebo je s ní logicky spojen
- umožňuje ověření totožnosti podepsané osoby ve vztahu k datové zprávě
- vytvořen pro konkrétní data -> možnost ověření, zda je platný a zda jsou data v té podobě, ve které byla podepsána

POUŽITÉ FUNKCE

Hash funkce

- Asymetrická a jednosměrná funkce
- Jakékoliv množství vstupních dat poskytuje stejně dlouhý výstup (otisk)
- Malou změnou vstupních dat dosáhneme velkou změnou na výstupu (tj. výsledný otisk se od původního zásadně liší)
- Z Hashe je prakticky nemožné rekonstruovat původní texty zpráv
- V praxi je vysoce nepravděpodobné, že dvěma různým zprávám odpovídá stejný Hash, jinými slovy pomocí Hashe lze v praxi identifikovat právě jednu zprávu (ověřit její správnost)

ZÍSKÁNÍ

Postup získání elektronického podpisu:

1. Vygenerování žádosti na PC a žádost odešleme
2. Uložení na médium (flash disk)
3. Czechpoint či jiná certifikovaná autorita
4. Ověření totožnosti (občanský průkaz)
5. Přehrání ověřeného klíče do PC
6. Pravidelné obnovování (každý rok)

OVĚŘUJE

- Autenticitu – identitu subjektu
- Integritu – nedošlo ke změně od vytvoření
- nepopiratelnost původu – ví se, kdo dokument vytvořil
- časové ukotvení – datum a čas podepsání

CERTIFIKAČNÍ AUTORITA

- vydává kvalifikované certifikáty, uznání pro komunikaci se státní správou (úroveň jako OP)
- zneplatnění: čas, změna údajů, odcizení, ztráta
- kvalifikovaný certifikát elektronického podpisu (např. pro komunikaci se státní správou) lze získat na pobočce české pošty
- elektronickým podpisem je i podpis v emailu

POUŽITÍ

- Kvalifikované certifikáty využijete především v komunikaci s úřady, například s finančním úřadem, soudy, Českou správou sociálního zabezpečení, Celní správou, na elektronických tržištích, v aplikaci Czechinvest nebo třeba v komunikaci s některými zdravotními pojišťovnami.
- Kvalifikovaný osobní certifikát je naprosto nezbytný při odesílání zpráv z datové schránky u společností s více jednateli nebo ze schránek orgánů

veřejné moci. Společně s časovým razítkem se vám bude hodit při elektronické archivaci vašich dokumentů.
- při podání přehledu o příjmech a výdajích OSVČ
- u přihlášky a odhlášky k nemocenskému pojištění
- u přiznání k DPH
- při elektronické komunikaci se státní správou
- při elektronické komunikaci s krajskými a městskými úřady
- při elektronické komunikaci se zdravotními pojišťovnami
- při žádosti o sociální dávky
- při podávání žádostí o dotace EU
- při použití datové schránky
- při podepisování faktur
- jako elektronický podpis PDF dokumentů

OMEZENÍ
- časové
- doba vzniku el. podpisu (nevíme kdy podpis vznikl)

DATOVÁ SCHRÁNKA
- elektronické úložiště zřízené státem od roku 2009 (mojedatovaschranka.cz)
- zabezpečení komunikačním šifrovacím protokolem SSC
- na vrstvě transportní a aplikační ISO OSI modelu
- **možnosti přihlášení:** jméno a heslo, SMS
- **vyhledání schránky:** název, IČO, identifikátor

OCHRANA DAT
PŘED ZNEUŽITÍM
- zničení (spalovna, skartace)
- autorizovaný přístup
- hesla
- biometrie

PŘED ZTRÁTOU
- zálohování
- distribuovaná báze dat (řeknu to info více lidem, oni si to budou pamatovat)
- centralizovaná báze dat (hodně lidí dává info na jedno místo)

REDUNDANCE DAT
- data která jsou zbytečná a dají se odvodit od ostatních dat
- např. pevné disky v RAIDu, nebo informace v databázi že máme 4 rohlíky pokud tam už bylo že jsme jich koupili 10 a 6 snědli

Kódování – Převod mezi jednotlivými abecedami (např. Binární -> Dekadická)

Šifrování – Kódování v rámci jedné abecedy (např. hash)

Privátní klíč
Kryptografie – šifrování

- Nauka o utajování zpráv

Symetrická kryptografie
Zpráva se šifruje a dešifruje tím samým klíčem
Příjemce a odesílatel zprávy se dohodnou na klíči, pomocí kterého budou dále šifrovat

Příklady možnosti sym. Šifry

Substituční šifra

- Písmena se posunou o dohodnuté číslo v abecedě
- NEBO se dohodne, že jednotlivá písmena budou představovat jiná písmena a udělá se tabulka

Permutační šifra

- Podle tabulky se mění pořadí písmen

Moderní symetrická šifra – Advanced Encryption Standard (AES)

- Substituční a permutační šifra
- Délky 128/192/256 bitů

Nevýhoda symetrického šifrování

- Dostat utajeně od odesílatele příjemci
- Čili přes tajný kanál, k čemu nemá nikdo jiný přístup... v realitě neexistuje

Řešení asymetrické šifrování

- Dva klíče
- Privátní a veřejný

Jednoduchý princip – jeden si vytvoří dva klíče – jeden podle které se bude zpráva šifrovat (veřejný) a jeden dešifrovací (privátní)

Takto zašifrovanou zprávu přetečte pouze ten s privátním klíčem
Já jako tvořitel obou klíčů si nechám privátní klíč u sebe

Pro obousměrné komunikace si oba účastníci vytvoří takovéto klíče, skrze které bude probíhat komunikace

Zásadní výhodou je, že pro navázání zabezpečené komunikace není třeba předání tajné informace nezašifrovanou zprávou.
− Malice má přístup k veřejnému klíči. Může tak šifrovat svoje zprávy, a pak se je snažit podvrhnout jako zprávy od Alice/Boba.
+ (Některé) asymetrické algoritmy se dají využit k robustnímu systému digitálních podpisů, což efektivně řeší předchozí problém.

− Oproti symetrickým šifrám jsou ty asymetrické komplikovanější. Co je podstatnější, jsou také výrazně náročnější na výpočetní výkon.
+ Asymetrické šifrování se dá výborně kombinovat se symetrickým. Pomocí kanálu navázaného asymetrickou šifrou je možno si bezpečně předat klíč k jiné symetrické šifře, použité pro následnou rychlejší zabezpečenou komunikaci.