Autentizace

Kamil Malinka

malinka@fit.vutbr.cz

Fakulta informačních technologií

Slides of Matyas, Riha, FI MU were used for parts of this presentation.

Tři základní notace

- autentizace
  - proces ověření identity (s požadovanou zárukou)
- autorizace
  - přidělení privilegií, specifikace povolené aktivity
- identifikace
  - rozpoznání entity v předem dané množině uživatelů

Autentizace/identifikace uživatele

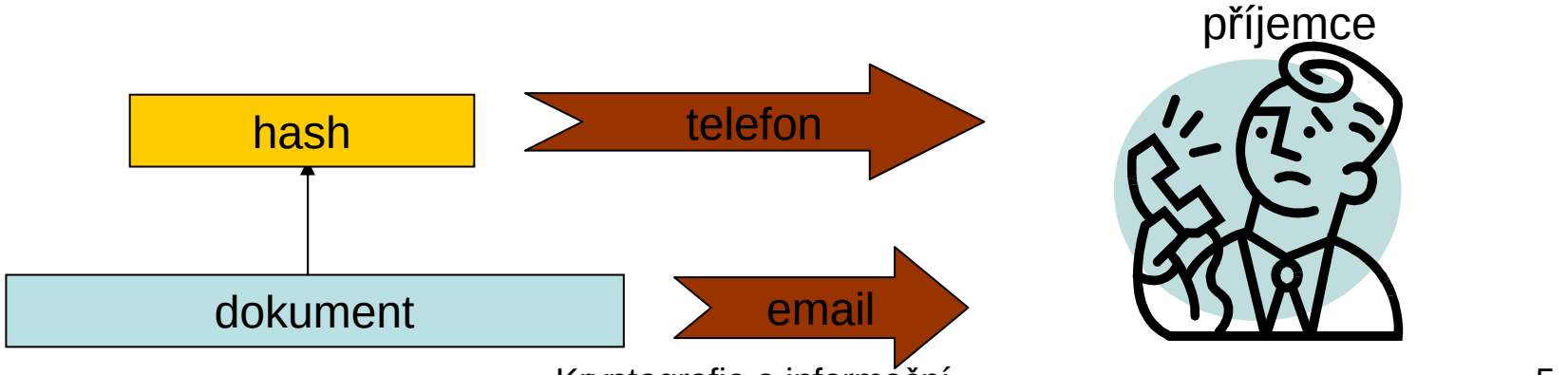
- Autentizace (verifikace)
  - subjekt vydá prohlášení o své identitě – 1:1
- Identifikace (prohledávání)
  - subjekt nijak neproklamuje svou identitu
  - systém prochází všechny záznamy v databázi, aby našel shodu
  - 1:n
  - podstatně náročnější proces

Autentizace dat/zpráv

- souvisí s ověřováním integrity
- bez použití kryptografie
  - CRC apod.
  - odhalují pouze náhodné chyby
- s použitím kryptografie
    - umožňuje detekci úmyslných chyb
  - sdílený tajný symetrický klíč
  - přenesení hashe bezpečným kanálem
  - klíčovaný has/MAC
  - digitální podpis

Hashování a autentizace dat

- komunikace kanálem s malou kapacitou:
  - data poslána kanálem s vysokou průchodností (např. email)
  - je spočítán hash těchto dat, výsledek je poslán jiným kanálem (telefon, vizitka. …)
  - příjemce znovu spočítá hash přijatých dat a výsledek porovná s přijatým hashem



Algoritmy digitálního podpisu

- nejstarší, hojně využívaný - RSA
- USA 1994 – soutěž o standard pro digitální podpis – vítěz DSA - modifikovaný algoritmus El-Gamal, založený na problému výpočtu diskrétního algoritmu nad tělesem Z_p.
- K těmto dvěma nejpoužívanějším algoritmům existují varianty pracující nad tělesy eliptických křivek EC-RSA, EC-DSA

Digitální podpis – délky klíčů

- RSA
  - 1977 – publikován příklad, který byl považován za bezpečný (využíval 64 a 65 bitové prvočísla)
  - tento kryptosystém byl prolomen r. 1994
  - 1999 – prolomení 512b kryptosystému (bylo použito několik stovek počítačů po dobu 4 měsíců)
  - V současné době jsou používány délky klíčů RSA a DSA na tělesem zbytkových tříd (klasická varianta) o délce 2048 bitů.

Digitální podpis – časová složitost

Operace	Modulo	Exponent	Čas
RSA podpis	1024 bitů	1024 bitů	25.2 ms
RSA podpis	2048 bitů	2048 bitů	0,17 s
RSA verifikace	1024 bitů	32 bitů	2,8 ms
RSA verifikace	2048 bitů	F_4	38 ms
RSA generování klíče	1024 bitů		1,56 s
RSA generování klíče	2048 bitů		14,4 s
EC DSA (GF(p)) podpis	160 bitů		24 ms
EC DSA (GF(p)) verifikace	160 bitů	160 bitů	50 ms

Autentizace dat - příklad

- autentizace EXE souborů v MS Windows
  - proč autentizovat?
  - chceme a potřebujeme zajistit integritu dat
  - chceme znát autora programu
  - chceme věřit MS a chceme si být jistí tím, že kód nebyl změněn během distribuce

Microsoft Autenticode

- Jak funguje?
  - EXE soubor je digitálně podepsán
  - digitální podpis je verifikován
  - úspěšná verifikace => program je spuštěn
  - neúspěšná verifikace => uživatel je požádán o rozhodnutí

Microsoft Autenticode

Microsoft Autenticode

Microsoft Autenticode

- stále není 100%
- 2001 – neznámý útočník získal 2 certifikáty veřejného klíče pro Microsoft podepsaná f. Verisign (obě společnosti jsou klíčovými hráči a mají adekvátní bezpečnostní procedury)
  - útočník se vydával za zaměstnance Microsoftu, byly mu vydány certifikáty podepsané Verisignem
  - každý kód podepsaný klíčem, který náleží k těmto certifikátům může být spuštěn na OS Win bez jakéhokoliv varování
- 2005 – rootkity – OS Win může být změněn tak, že se neptá uživatele na povolení k instalaci

Kryptografické protokoly

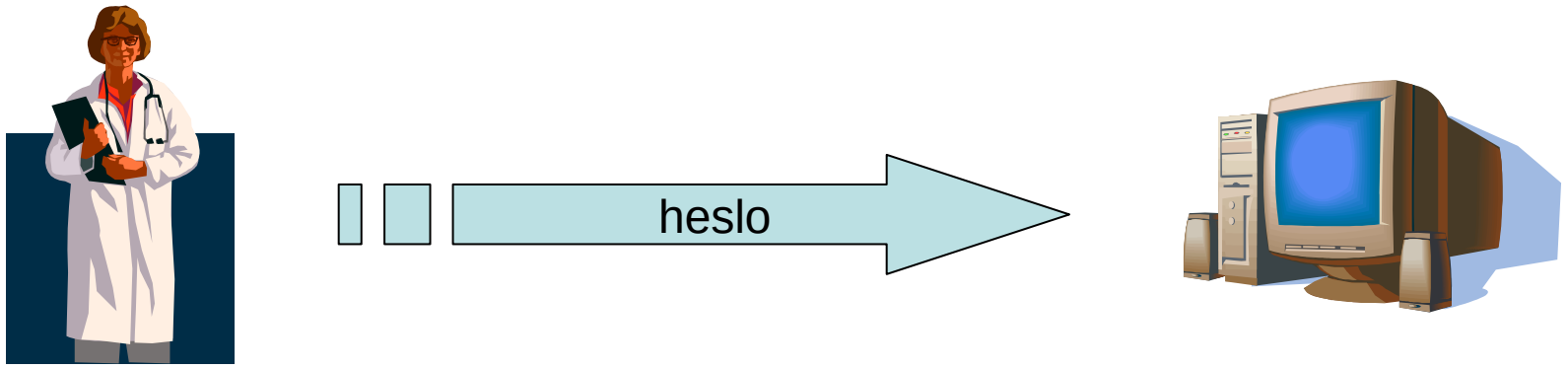
- Autentizační protokoly
  - používají existující sdílená tajemství
  - cílem je ujistit jednu stranu o identitě druhé strany, se kterou chce komunikovat
- Protokoly pro ustanovení klíče
  - cílem je vytvořit a distribuovat tajemství
- Autentizované protokoly pro ustanovení klíče
  - vytváří sdílené tajemství mezi stranami, jejichž identita byla ověřena

Autentizační protokoly

- autentizace je:
  - jednosměrná
  - obousměrná
  - průběžná
- kdo autentizuje koho
  - klient sám započne protokol
  - protokol je iniciovaný výzvou

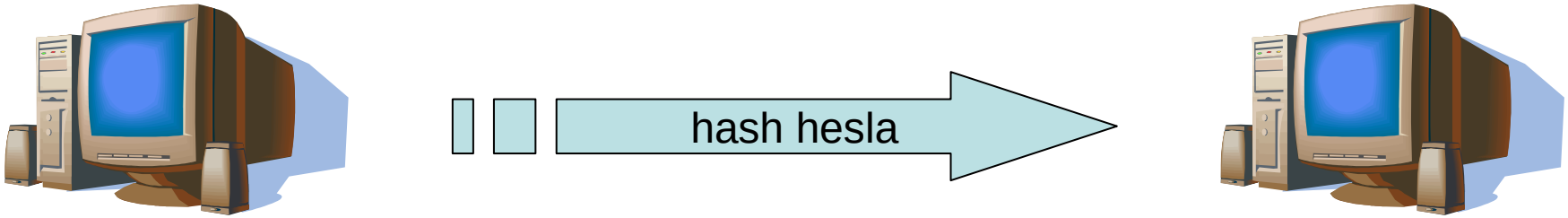
Heslo

- Alice se autentizuje Bobovi zasláním hesla
- heslo může být odposlechnuto
- Bob (na konci protokolu) zná Alicino heslo a může se následně vydávat za Alici



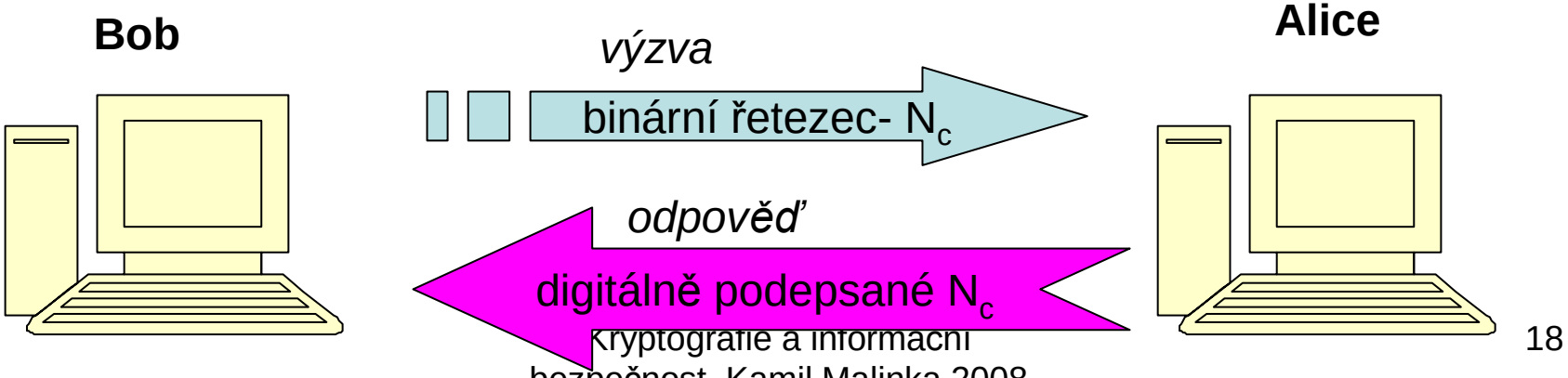
Hashované heslo

- v průběhu autentizace – heslo není posíláno v otevřeném textu, je posílán hash
- odposlouchávání hashe automaticky neodhalí heslo
- hash může být stále využit pro maškarádu



Protokoly výzva-odpověď

- protokol se sestává minimálně ze dvou zpráv
  - odposlech výzvy/odpovědi neumožňuje útočníkovi opakovat autentizaci
  - Bob je schopen verifikovat Alicinu identitu bez znalosti jejího tajemství
  - výzva musí být čerstvá
  - odpověď je vypočtena na základě výzvy tak, aby nebylo možné ze známých odpovědí odvodit odpovědi na nové výzvy



Časově závislé proměnné - N_c

- náhodná čísla – značí se **r**
  - čísla jsou nepředvídatelná (pseudonáhodná, náhodná). Zaručují unikátnost a čerstvost. Není jednoduché je generovat (vyžaduje specializovaný HW), běžně generovány SW z nějakého semínka
- sekvenční čísla – značí se **n**
  - monotónní sekvence čísel, obě strany musí uchovávat naposledy použité číslo, jednoznačně identifikují zprávu, umožňují detekci útoků přehráním
- časová známka – značí se **t**
  - obě strany musí udržovat časovou synchronizaci
  - zaručuje unikátnost a přesné určení času vytvoření zprávy

Symetrické algoritmy

- protokoly založené na symetrických algoritmech (Alice a Bob sdílejí symetrický klíč **K**)
- Standard ISO/IEC 9798-2
- Jednocestná autentizace s časovou známkou
  - $A \rightarrow B: E_K(t_A,\text{“B“})$
- Jednocestná autentizace s náhodným číslem
  - $A \leftarrow B: r_B$
  - $A \rightarrow B: E_K(r_B,\text{“B“})$
- Obousměrná (vzájemná) autentizace s náhodnými čísly
  - $A \leftarrow B: r_B$
  - $A \rightarrow B: E_K(r_A,r_B,\text{“B“})$
  - $A \leftarrow B: E_K(r_B,r_A)$

Symetrické algoritmy

- protokoly založené na jednosměrné klíčované funkci(Alice a Bob sdílejí symetrický klíč **K**)
- Standard ISO/IEC 9798-4, protokoly SKID
- Obousměrná (vzájemná) autentizace
  - $A \leftarrow B: r_B$
  - $A \rightarrow B: r_A, h_K(r_A,r_B,\text{”B”})$
  - $A \leftarrow B: h_K(r_B,r_A,A)$
  - h_K je algoritmus MAC

Asymetrické algoritmy

- Založeny na šifrování se soukromými klíčy
- Jednocestná autentizace
  - A ← B: h(r), „B“, P_A(r,”B”)
  - A → B: r
- *h* – hashovací funkce
- *h(r)* slouží jako důkaz znalosti ***r*** bez jeho odhalení

Asymetrické algoritmy

- založeny na digitáním podpisu
- Standard ISO/IEC 9798-3
- Jednocestná autentizace s časovou známkou
  - $A \rightarrow B$: $cert_A$, t_A, ”B“, $S_A(t_A$, “B“)
- Jednocestná autentizace s náhodným číslem
  - $A \leftarrow B$: r_B
  - $A \rightarrow B$: $cert_A$, r_A, “B“, $S_A(r_A,r_B$,“B“)
  - r_A zabraňuje chosen plain-text útokům
- Obousměrná (vzájemná) autentizace s náhodnými čísly
  - $A \leftarrow B$: r_B
  - $A \rightarrow B$: $cert_A$, r_A, “B“, $S_A(r_A,r_B$,“B“)
  - $A \leftarrow B$: $cert_B$, “A“, $S_B(r_B,r_A$,“A“)

Správa klíčů

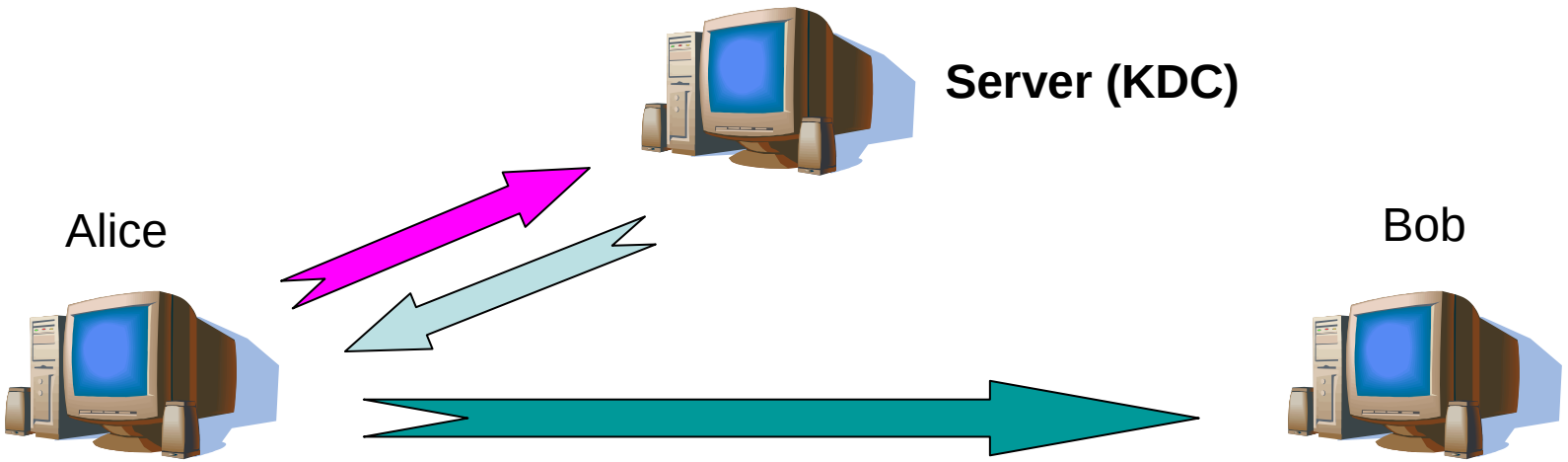
- Cíle
  - přenos klíče
  - dohoda na klíči
  - aktualizace klíče (strany sdílejí dlouhodobý klíč **K**)
- Počty zúčastněných stran
  - dvoustranné protokoly
  - protokoly s důvěryhodnou třetí stranou

Kerberos

- vytvořen jako část projektu Athena (MIT)
- předpokladem je bezpečná symetrickýá šifrovací funkce E
- 2 strany (A,R) a důvěryhodný autentizační server (T)
- Cíle:
  - autentizace Alice ke zdroji R
  - ustanovení klíče K (vybírá-generuje T)
  - případná distribuce sdíleného tajemství mezi A a R
- Každá strana sdílí symetrický klíč se serverem T
  - (K_{AT}, K_{RT})

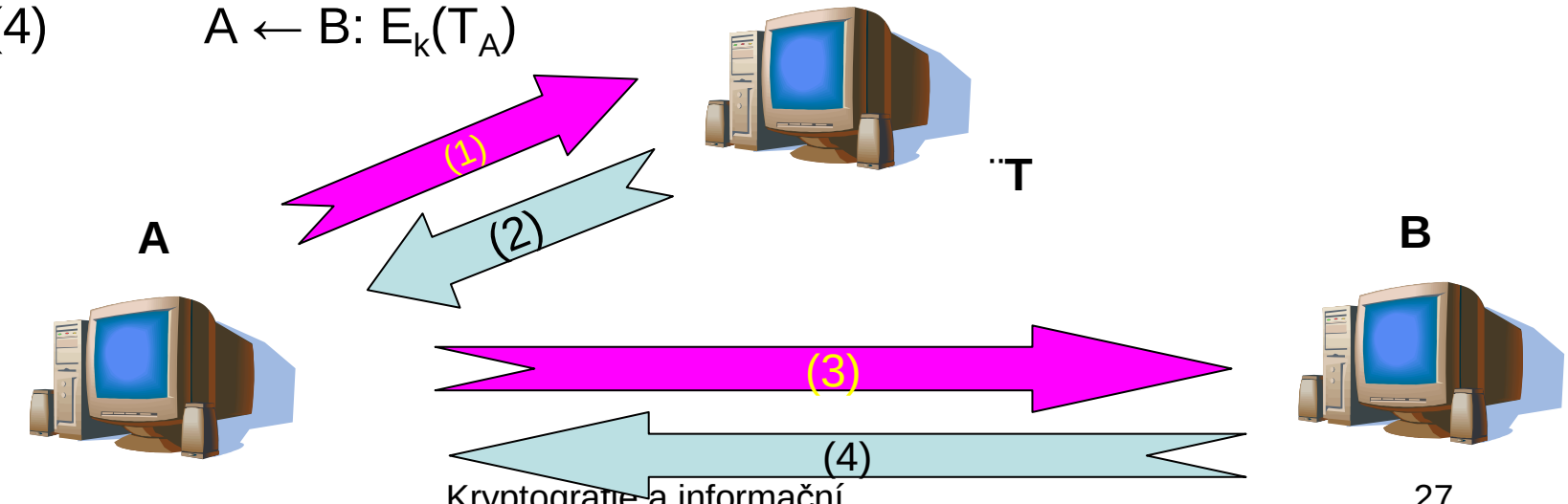
Kerberos

- **KDC** (key distribution centre) – centrum sdílí klíče se všemi klienty, generuje a distribuuje klíče
  KTC (key translation centre) – centrum negeneruje klíče – pouze je přeposílá



Kerberos

- zjednodušený protokol
  - L – časová platnost lístku
  - Def.: $ticket_B = E_{K_{BT}}(k, \text{“A”}, L)$, $auth = E_k(\text{“A”}, T_A)$
  - (1) $A \rightarrow T$: ”A”, ”B”, n_A
  - (2) $A \leftarrow T$: $ticket_B$, $E_{K_{AT}}(k, n_A, L, \text{“B“})$
  - (3) $A \rightarrow B$: $ticket_B$, $auth$
  - (4) $A \leftarrow B$: $E_k(T_A)$



Diffie Hellman

- Diffie-Hellman key agreement protocol
  - common prime p, generator α form Z_p
  - Alice chooses secret *x*, Bob chooses secret *y*
  - A $\rightarrow$ B: $\alpha^x \bmod p$
  - A $\leftarrow$ B: $\alpha^y \bmod p$

  - Alice and Bob share $K=\alpha^{xy} \bmod p$

Správa identit (IDM)

(tutorial Hanáček, Staudek, DATAKON'05)

- Pokrytí oblasti
  - definice identity pro entity a objekty
  - bezpečné úložiště pro identifikační informace entit
  - zajištění standardizovaného rozhraní pro přístup k identifikačním informacím
  - zajištění robustní infrastruktury pro IDM, správu dat,…
  - zajišťuje: autentizaci, autorizaci, řízení přístupu, audit

Federované IDM

- problém – existence mnoha systémů pro uložení ID informace
- potřeba kombinace dat, zajišťování konzistence (integrity), rychlého přístupu…
- potřeba škálovatelnosti
- po integraci musí být data editovatelná z libovolného systému
  - analogie k pasům a rozpoznávání identity v rámci EU

Federování IDM

- autentizace
  - password management, SSO (single-sign on)
    - LDAP, DSML, Win, Linux, DBMS, …
  - access control (Web)
    - WS (web services), WS-S (WS security), SOAP (simple object access protocol), SAML (security assertion markup language), WSDL (web services description lang.), UDDI (univ. description, discovery, and integration), XACML, SPML, BPEL, …

Vývoj IDM

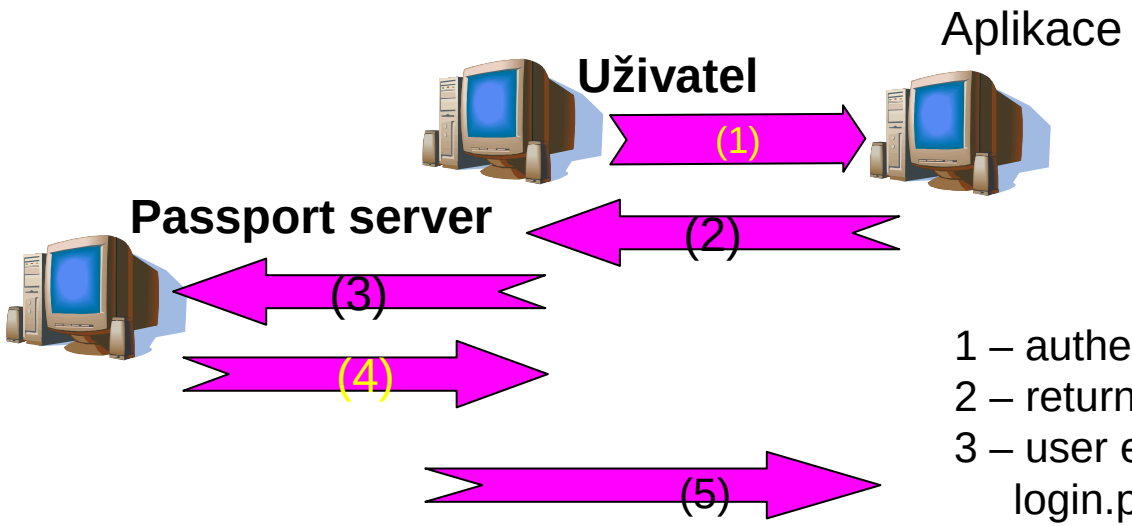
- X.500 – v 80.letech => X.400 email, X.509, …
- LDAP – lightweight DAP (directory access protocol), podporuje TCP/IP
- současnost: protokoly založené na XML
- konkrétní systémy:
  - MS Passport (200 mil účtů) – mrtvá koncepce
  - Liberty Alliance – založen na SAML (180 mil účtů) – žijící a vyvíjející se…
  - Shibboleth
  - …

Single Sign-on

- velké organizace mohou mít desítky systémů s vlastním autentizačním mechanismem
- řešení?
  - webová aplikace synchronizující změny
  - centrální úložiště (adresář), synchronizace pomocí meta-adresářů
  - obě varianty
- efekty SSO
  - snížení počtu autentizací
  - zvýšená bezpečnost zjednodušenou administrací
  - nižší cena autentizačního mechanismu
  - centralizované řešení znamená vyšší přínos útoku

MS Passport

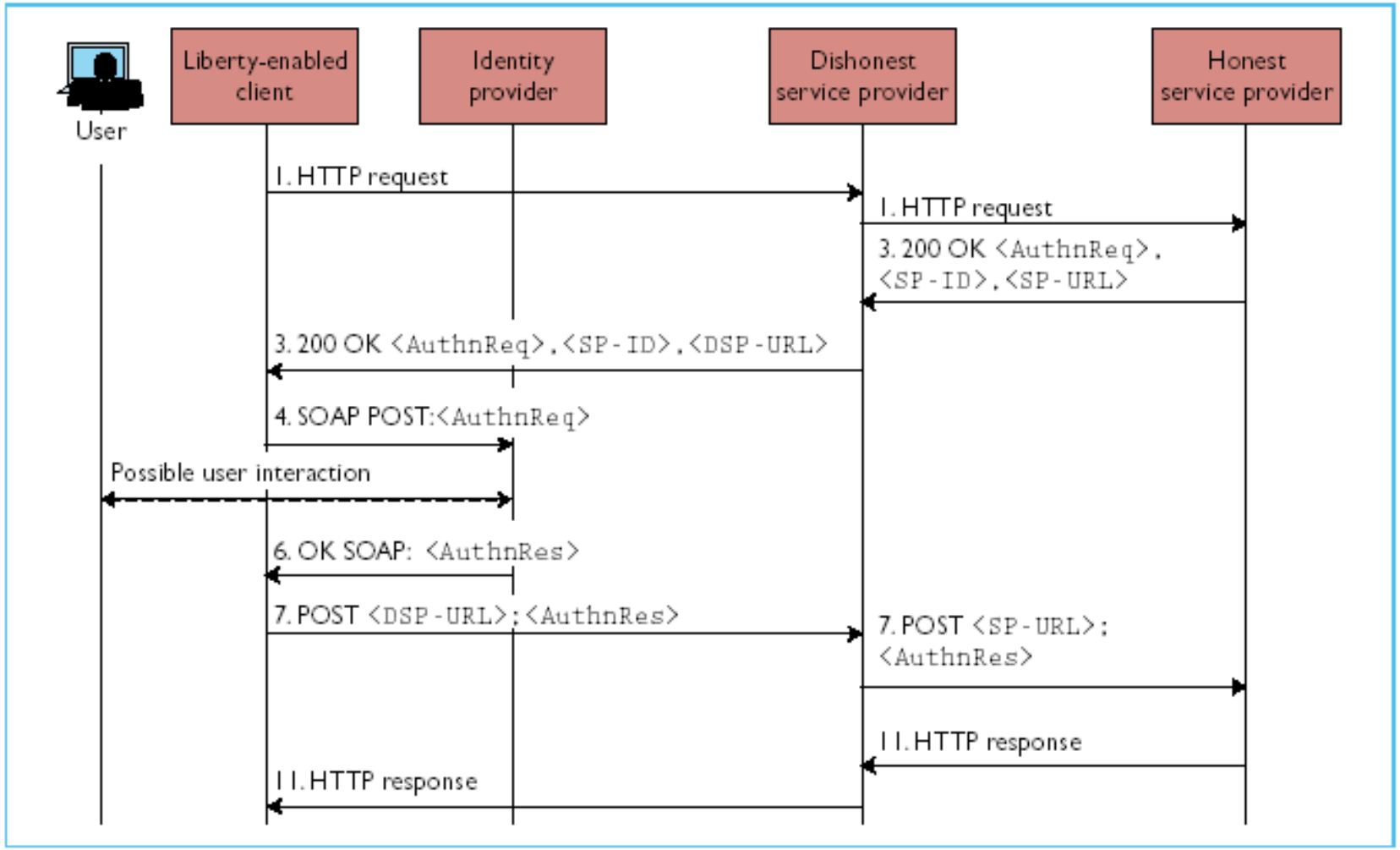
- www variace Kerberovských principů
  - TGS – passport server
  - aplikace musí být passportizovaná



1 – authentication request
2 – return url (302 – redirect)
3 – user enters login/password
login.passport.com/?=www.aplikace.com

4 – ticket and cookie sent, redirect
www.aplikace.com/menu?MSPAuth=ticket&MSPProf=coo
5 – verification of ticket and cookie

Autentizační protokol Liberty Alliance



Security measures in LA v.1

- Service-provider-specific tokens. <SP-ID>
- Secure channels - <SP-URL> is an https addr
- Token authentication – user ID and <SP-ID>
- Countermeasures
  - Client derives service provider's address – must know secure infrastructure
  - Service provider authenticates for client – SP-URL, SP-ID
  - *Identity provider derives service provider's addr*
  - Service provider authenticates for id. provider