

## Federativní přístup k autentizaci

Milan Sova\*

sova@cesnet.cz

**Abstrakt:** Příspěvek předkládá stručný úvod do problematiky autentizace a autorizace a seznamuje s koncepcí autentizačních federací. Je určen informačním odborníkům pracujícím se systémy obsluhujícími uživatele různých institucí.

**Klíčová slova:** informační systémy, autentizace, autorizace, federativní autentizační a autorizační infrastruktura

### 1 Úvod

Moderní informační služby poskytované v prostředí rozvinutých datových sítí obvykle vyžadují autentizaci a autorizaci uživatelů. Ať už proto, aby zajistily přístup pouze oprávněným uživatelům, nebo aby mohly poskytnout každému uživateli personalizované prostředí. „Klasický“ režim správy uživatelských dat, kdy každá služba registruje své uživatele a jejich autentizační informace, naráží v situaci, kdy běžný uživatel využívá mnoho informačních služeb spravovaných různými poskytovateli, na některé problémy.

- Při registraci ke každé službě je uživatel nucen poskytnout údaje, z nichž některé mohou být považovány za soukromé až citlivé, aniž by vždy měl jistotu, že je poskytovatel služby opravdu potřebuje, a že s nimi bude nakládat podle uživatelových představ.
- Pro přístup k jednotlivým službám si musí uživatel zvolit (nebo jsou mu přiděleny) autentizační údaje (obvykle uživatelské jméno a heslo), které si pak musí zapamatovat. Běžnou reakcí uživatele je volba stejného hesla pro všechny služby, jehož případné prozrazení pak ohrožuje bezpečnost všech služeb, kde je použil.
- Na straně poskytovatelů služeb vznikají velké náklady na samotnou správu autentizačních dat – registrace uživatelů, modifikace uživatelských záznamů při změně, řešení problémů se „zapomenutými hesly“ apod.

Ukazuje se, že cestou k řešení všech těchto problémů může být federativní přístup k autentizaci. Principy tohoto řešení ozřejmíme v tomto článku. Pro snadnější pochopení najdete na konci článku terminologický slovníček.

### 2 Architektury autentizačních systémů

V průběhu vývoje informačních systémů postupně vzniklo několik typů architektur organizujících autentizační a autorizační služby. Nejstarší je zřejmě lokální autentizační a autorizační systém.

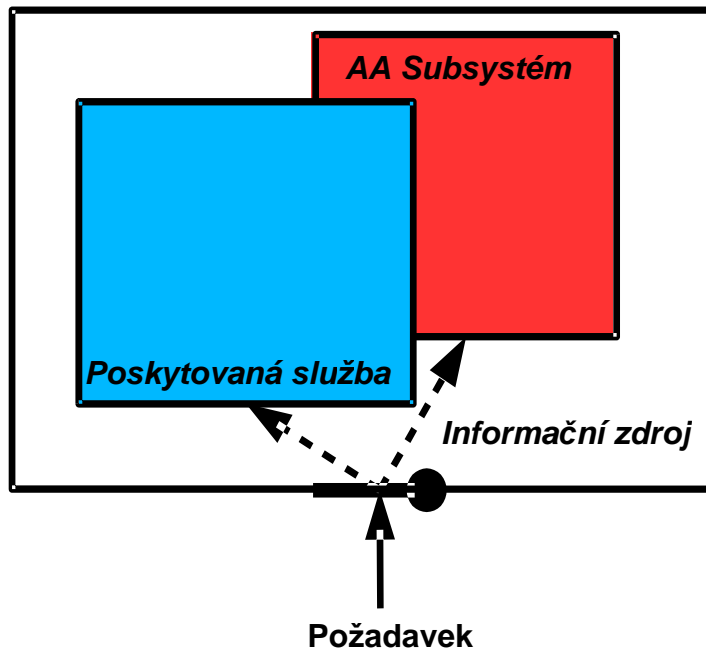
#### 2.1 Lokální autentizační a autorizační systém

V „klasické“ lokální autentizační architektuře (Obr. 1 Lokální AA systém) je autentizační a autorizační subsystém přímo integrován do systému či aplikace poskytující službu. Všechna data o uživateli, jejich autentizační údaje, kategorizace atd. jsou uložena přímo v informačním systému. Ten také poskytuje všechny potřebné funkce a uživatelské rozhraní pro jejich vytváření, modifikaci a správu. Takový systém je plně samostatný, ovšem za cenu

---

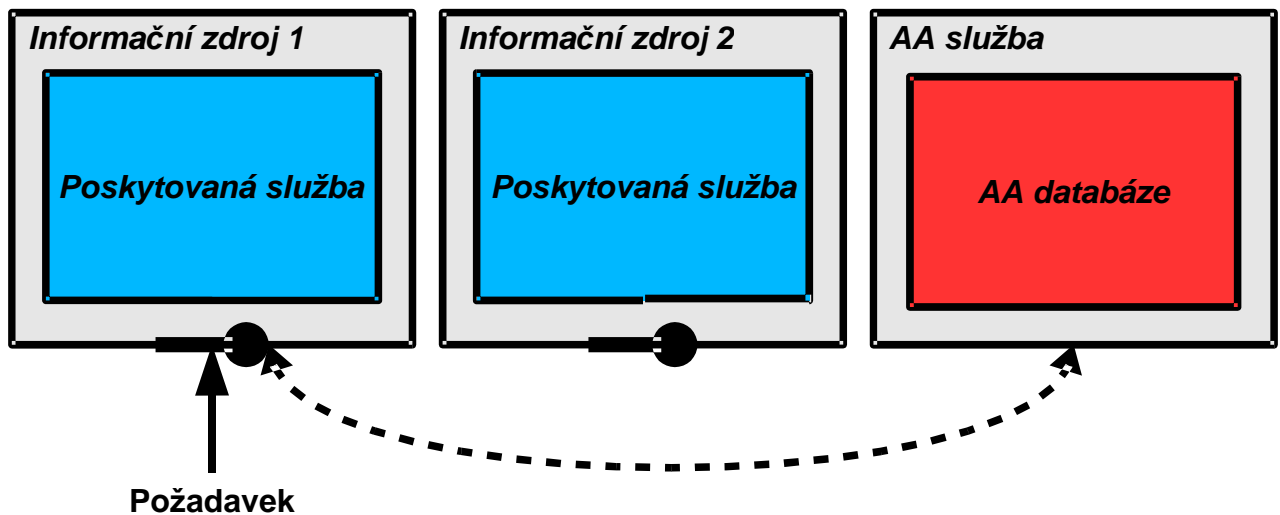
\*CESNET, z.s.p.o., Žitná 4, 160 00 Praha 6-Dejvice

zvýšené vlastní složitosti (musí obsahovat kompletní implementaci autentizačního a autorizačního subsystému). Je obvykle velmi obtížné plně jej integrovat s jinými systémy.



Obr. 1. Lokální AA systém

## 2.2 Centralizovaný autentizační a autorizační systém



Obr. 2. Centralizovaný AA systém

V organizacích, které poskytují rozmanité informační služby poměrně stálému, uzavřenému okruhu uživatelů, je dnes obvyklá centralizovaná architektura autentizačních a autorizačních služeb (Obr. 2 Centralizovaný AA systém). Údaje o uživatelích jsou spravovány centrálně jako nezávislý systém informační infrastruktury a jednotlivé služby a aplikace se při autentizaci odkazují na služby centra. Výhody jsou nesporné: centralizovaná správa a oddělení autentizačního a autorizačního systému umožňují zajistit jeho vyšší zabezpečení, zjednodušit jeho údržbu. Uživatelům pak tato architektura přináší transparentnější a přívětivější pracovní prostředí při vyšší bezpečnosti systému. Je-li pro všechny aplikace používáno např. jedno heslo, může správce systému klást vyšší nároky na jeho vlastnosti (délka, výskyt znaků z různých tříd apod.). Organizace provozující centralizovaný autentizační a autorizační systém obvykle vyžadují, aby i nové aplikace a služby byly do tohoto systému integrovatelné.

### 2.3 Federativní autentizační a autorizační infrastruktura

V poslední době roste význam spolupráce mezi organizacemi. Je stále obvyklejší, že různé organizace navzájem sdílejí své informační zdroje, jejich uživatelé úzce spolupracují na společných projektech nebo několik organizací společně využívá zdroje poskytované třetí stranou (typické pro vysokoškolské knihovny a přístup jejich uživatelů ke konsorcionálně pořízeným on-line informačním zdrojům). Aby nebylo nutné zavádět každého uživatele do autentizačních databází všech zúčastněných organizací, vznikají autentizační federace.

Základní princip je jednoduchý: zúčastněné organizace se dohodnou, že budou navzájem uznávat své autentizační postupy a respektovat jejich výsledky. Kdykoli má být uživatel autentizován pro přístup k prostředkům některé cizí organizace, je přeměrován na autentizační službu své domovské instituce. Ta provede vlastní autentizaci a vydá uživateli „potvrzení“, že jeho identita byla ověřena, obsahující identifikátor uživatele a identifikátor domovské instituce. Identifikátor uživatele může být pouze dočasný, bez zjevného vztahu ke skutečné identitě uživatele, takže služba může být poskytována anonymně. S vydaným potvrzením je uživatel přeměrován zpět k původně požadovanému informačnímu zdroji. Tam je „potvrzení“ ověřeno (obvykle se jedná o zprávu opatřenou elektronickým podpisem domovské instituce) a v případě úspěchu je uživatel autentizován.

Jsou-li pro autorizaci potřebné další údaje z domovské instituce (např. kategorie uživatele), může si je vzdálený systém vyžádat od domovské instituce. K tomuto účelu slouží v každé domovské instituci Atributová služba – síťová služba poskytující federovaným institucím informace o uživatelích ve formě tzv. atributů. Atributy popisují charakteristiky jednotlivých uživatelů: jejich příslušnost k různým skupinám (student, vědecký pracovník, host, ale také např. aktivní řešitel projektu X, absolvent základního kurzu algebry apod.), právo vystupovat v některých rolích (správce síťové služby, správce licence produktu Y, ...) až po osobní údaje (věk, jméno, ...). Ne všechny atributy jsou dostupné všem poskytovatelům služeb. Uživatel může konfigurací Atributové služby ve své domovské instituci ovlivnit to, které ze svých osobních údajů budou poskytnuty pro autorizaci k jednotlivým službám. Atributová služba může navíc pracovat ve dvou režimech:

- a) Může přímo vydávat hodnoty požadovaných atributů, nebo
- b) pouze odpovídat na dotazy typu „má atribut A uživatele  $U$  hodnotu  $H$ ?“, např. „Je uživatel  $U$  studentem?“, „Je plnoletý?“ apod.

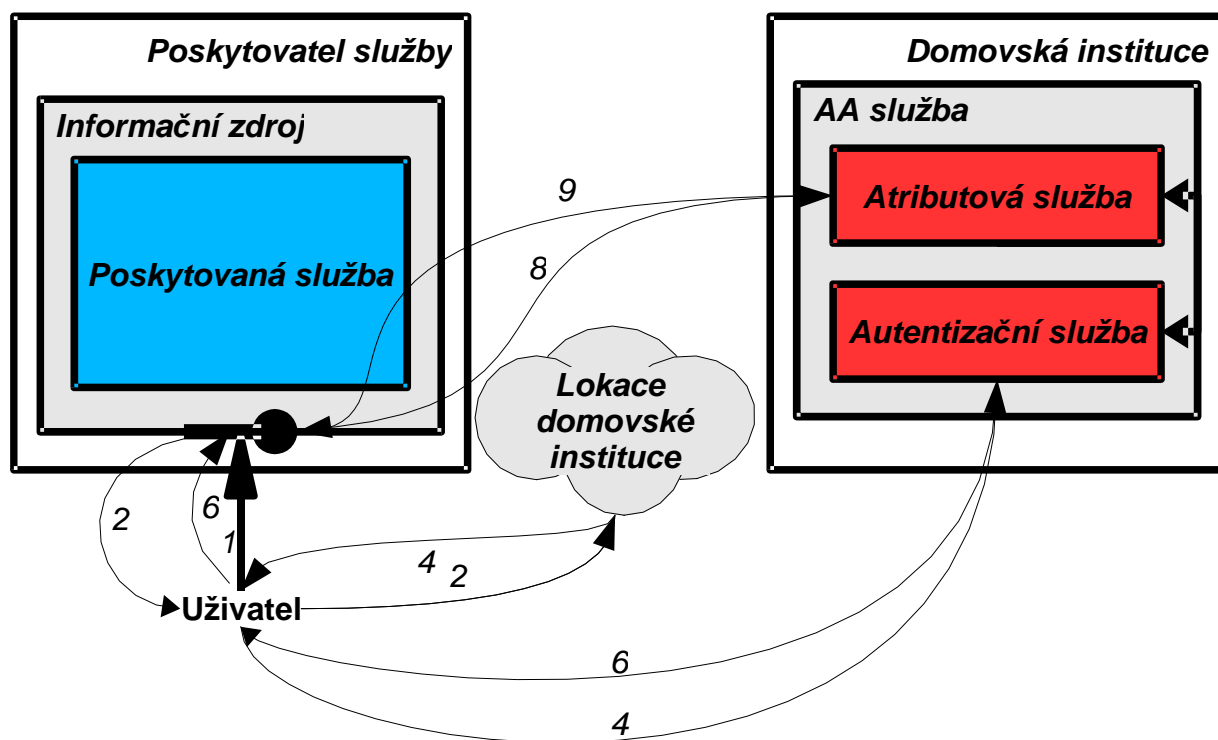
Federativní architektura vyžaduje ovšem existenci další služby: lokátoru domovské instituce. Běžný uživatel samozřejmě neví, kde (na které síťové adrese) provozuje jeho domovská organizace provozuje Autentizační a Atributovou službu. Z toho důvodu provozuje federace službu Lokátor domovské instituce. Ta na základě údajů dodaných uživatelem

(obvykle jméno domovské instituce, nebo jméno její DNS domény) poskytne síťovou adresu (URL) příslušné autentizační služby.

### Scénář autentizace ve federativní architektuře

Podívejme se podrobněji na to, jak autentizace a autorizace ve federativním prostředí probíhá (Obr. 3 Federativní AA). Pro zjednodušení a větší konkrétnost předpokládejme službu poskytovanou prostřednictvím HTTP, tedy dostupnou běžným WWW klientem.

1. Uživatel přistupuje na WWW stránku poskytující službu
2. Poskytovaná služba zjistí, že uživatel není autentizován a přesměruje jej na stránky služby Lokace domovské instituce. Součástí dat předávaných při přesměrování je identifikátor poskytované služby, např. ve formě URL.
3. Uživatel vybere ze seznamu federovaných institucí svoji domovskou instituci.



Obr. 3. Federativní AA

4. Lokátor domovské instituce vyhledá URL domovské autentizační služby a přesměruje uživatele na ni (identifikátor původně požadované služby je opět součástí předávaných dat).
5. Uživatel poskytne domovské autentizační službě své autentizační údaje (např. uživatelské jméno a heslo).
6. Autentizační služba ověří data poskytnutá uživatelem a v případě úspěchu vystaví „potvrzení o autentizaci“. To obsahuje identifikátor uživatele, identifikátor domovské instituce a dobu platnosti potvrzení, případně další údaje jako např. použitý autentizační mechanismus (jméno/heslo, digitální certifikát...). Potvrzení je podepsáno soukromým klíčem autentizační služby. S tímto potvrzením je uživatel přesměrován zpět na původně požadovanou službu.

7. Aplikace poskytující službu ověří platnost potvrzení a použije dvojici v něm uvedených identifikátorů jako výsledný identifikátor uživatele (tím se zabrání případné kolizi uživatelských identifikátorů z různých institucí).
8. Potřebuje-li služba pro autorizační rozhodnutí další informace o uživateli, obrátí se na Atributovou službu uživatelovy domovské instituce. Její lokaci zjistí s pomocí služby Lokace domovské služby. Žádost o atributy jsou podepsané soukromým klíčem služby a jsou předávány zašifrované.
9. Atributová služba přijme žádost o hodnoty atributů uživatele, ověří její elektronický podpis, z něj zjistí, kdo (která služba) údaje požaduje. Na základě filtrovacích pravidel zadaných uživatelem a správcem služby vybere ty atributy, které smí dané službě poskytnout, zařadí jejich hodnoty do odpovědi, tu podepíše svým soukromým klíčem a předá žadateli.
10. Služba ověří platnost elektronického podpisu na odpovědi a použije obsažené hodnoty atributů pro autorizační rozhodnutí.
11. Jsou-li splněny všechny požadované podmínky, je uživateli umožněn přístup ke službě.

Jak je vidět, při konstrukci federativní architektury je velká pozornost věnována zajištění ochrany osobních a autentizačních údajů. Osobní údaje jsou poskytovány pouze na základě povolení jejich nositele, autentizační údaje poskytuje uživatel pouze na jediném místě v celé federaci – tím je Autentizační služba jeho domovské instituce. Mezi členy federace jsou předávána pouze autentizační potvrzení a povolené uživatelské atributy.

### Organizační a technická podpora federace

Jak vyplývá z předchozího, existence autentizační federace předpokládá zřízení a provoz některých nových služeb a funkcí. Můžeme je rozdělit podle jejich provozovatele:

**Domovská instituce:** spravuje údaje o uživateli, provozuje Autentizační a Atributovou službu. Jejich zřízení obvykle spočívá ve zprovoznění bran, které zprostředkují některé funkce existujícího centrálního AA systému instituce prostředkům federace. Zřejmě nejnáročnějším úkolem je vytvoření Atributové služby, zejména zavedení a následná správa atributů požadovaných federací.

**Poskytovatel služby:** musí opatřit službu autentizačním a autorizačním rozhraním využívajícím služeb federace. Z organizačního hlediska bývá nejnáročnější rozhodnutí o tom, které atributy bude služba potřebovat pro autorizační rozhodnutí.

**Federace:** zajišťuje společné služby a funkce, především provoz a správu služby Lokace domovské instituce, definice protokolů a formátů zpráv, definice a správa syntaxe a sémantiky atributů a koordinaci infrastruktury veřejných klíčů, tj. výběr/schvalování důvěryhodných certifikačních autorit (v některých případech sama potřebné certifikační služby provozuje).

Některé instituce (typicky vysoké školy, velké vědecké knihovny...) samozřejmě mohou vystupovat jak v roli domovské instituce, tak v úloze poskytovatele služeb.

### 3 Závěr

Autentizační federace přináší nejen úspory jednotlivým federovaným institucím a vyšší komfort jejich uživatelům, ale i novou kvalitu do poskytování informačních služeb v globálním síťovém prostředí a přístupu k nim.

Není divu, že k největším hybatelům v rozvoji autentizačních federací patřily od počátku po celém světě knihovny (zejména vysokoškolské). Poskytují nebo zprostředkují přístup

k informačním službám pro rozsáhlé komunity uživatelů, kteří již obvykle jsou registrováni v některé instituci. Mezi takto motivované projekty patří PAPI a Athens. Momentálně nejslibnějším projektem v této oblasti je Shibboleth vyvíjený konsorciem Internet2. Technologiím podporujícím autentizační federace je věnována i činnost aktivity JRA5 projektu EU Géant2.

## Použité termíny

**AA.** Autentizace a autorizace.

**Autentizace.** Ověření identity. Odpovídá na otázku „Kdo jsi?“. Jako důkaz se obvykle používá znalost nějakého tajemství (hesla nebo soukromého klíče), které má znát pouze konkrétní uživatel. Někdy je do autentizace zapojena třetí strana, např. certifikační autorita, která vydává certifikát veřejného klíče, tj. elektronicky podepsané potvrzení, že držitelem soukromého klíče, který odpovídá danému veřejnému klíči je příslušný uživatel.

**Autorizace.** Ověření přístupových práv. Odpovídá na otázku „Smí daný uživatel provést danou operaci s daným zdrojem?“. Jako podklad pro autorizační rozhodnutí mohou sloužit různé informace: identita uživatele získaná při autentizaci, příslušnost uživatele k nějaké kategorii, identifikátory požadované operace a příslušného informačního zdroje, aktuální časové údaje apod.

**Certifikát veřejného klíče.** Elektronicky podepsaná zpráva obsahující veřejný klíč a identifikátor (jméno) držitele odpovídajícího soukromého klíče. Certifikáty vydává důvěryhodný úřad – certifikační autorita – jako potvrzení o tom, že ověřil identitu držitele soukromého klíče odpovídajícího veřejnému klíči uvedenému v certifikátu.

**Klíčový pár.** Dvojice klíčů (čísel), z nichž jeden lze použít k zašifrování nebo podepsání zprávy a druhý k jejímu dešifrování resp. ověření podpisu. Jeden z klíčů (ověřovací, šifrovací) je veřejný a je publikován obvykle ve formě certifikátu veřejného klíče, druhý (podpisový, dešifrovací) je soukromý.

**Veřejný klíč.** Veřejná část klíčového páru. Používá se k ověření elektronického podpisu provedeného odpovídajícím soukromým klíčem nebo k zašifrování zprávy pro držitele soukromého klíče. Zprávu zašifrovanou veřejným klíčem je možné dešifrovat pouze s pomocí odpovídajícího soukromého klíče.

**Soukromý klíč.** Soukromá část klíčového páru. Používá se k podepisování zpráv nebo k jejich dešifrování.

## Odkazy

1. PAPI <<http://papi.rediris.es/>>
2. Athens <<http://www.athens.ac.uk/>>
3. Shibboleth <<http://shibboleth.internet2.edu/>>
4. GÉANT2 – Joint Research Activity 5 <<http://www.geant2.net/server/show/nav.00d00a005>>