Demonstrátor - Návrh kryptografického systému pro ochranu identity

Jan Hajný a Zdeněk Martinásek

Ústav telekomunikací
Fakulta elektrotechniky a komunikačních technologií
VUT v Brně
hajny@feec.vutbr.cz, martinasek@feec.vutbr.cz

Abstrakt

Výzkum se zabývá ochranou osobních údajů, konkrétně ochranou elektronické identity. Cílem je představit nové schéma pro autentizaci, jenž je založeno na poznatcích moderní kryptografie a které odpovídá současným požadavkům na ochranu osobních údajů. Schéma poskytuje tzv. anonymní autentizaci, tedy možnost ověření vlastností uživatele bez odhalení jeho skutečné identity. Výsledkem je systém, kde uživatelé mohou prokazovat svoje atributy (např. věk, národnost, registraci, platnou autorizaci) bez odhalení dalších údajů. Tyto vlastnosti jsou poskytnuty s prokazatelnou bezpečností, jenž je postavena na platnosti tzv. problému diskrétního logaritmu. Uživatelé elektronických systémů, především Internetu, tak získávají možnost řídit množství informací, které je o nich během využívání služeb uvolněno, a mohou tak zamezit např. krádežím identity, sledování či neoprávněnému shromažďování citlivých osobních údajů.

1. Požadavky

Pro ochranu klientů, ale i poskytovatelů, je nutné, aby systém splňoval následující požadavky:

- **Anonymita**: během ověření uživatele není uvolněna žádná informace o jeho skutečné identitě.
- **Nespojitelnost**: jednotlivé relace ověření uživatele jsou vzájemně nespojitelné, jsou zcela odlišné.
- **Nepodvrhnutelnost**: pouze oprávněný uživatel je schopen využívat služeb poskytovatele.
- **Odhalení identity útočníka**: uživatel, který poruší pravidla systému (např. poškodí poskytovatele), může být jednoznačně identifikován a vyřazen.
- **Jednoduchá správa**: výpočetní složitost algoritmů systému je nezávislá na počtu uživatelů a atributů, které prokazují. Uživatele lze snadno přidávat, odebírat.
- **Výpočetní nenáročnost**: systém je výpočetně nenáročný, je možné jej implementovat i na programovatelných smart-kartách (JavaCard, .NET).
- **Bezpečnost**: kryptografická konstrukce, na níž je systém postaven, je *prokazatelně* bezpečná, tedy redukovatelná na silný kryptografický problém.

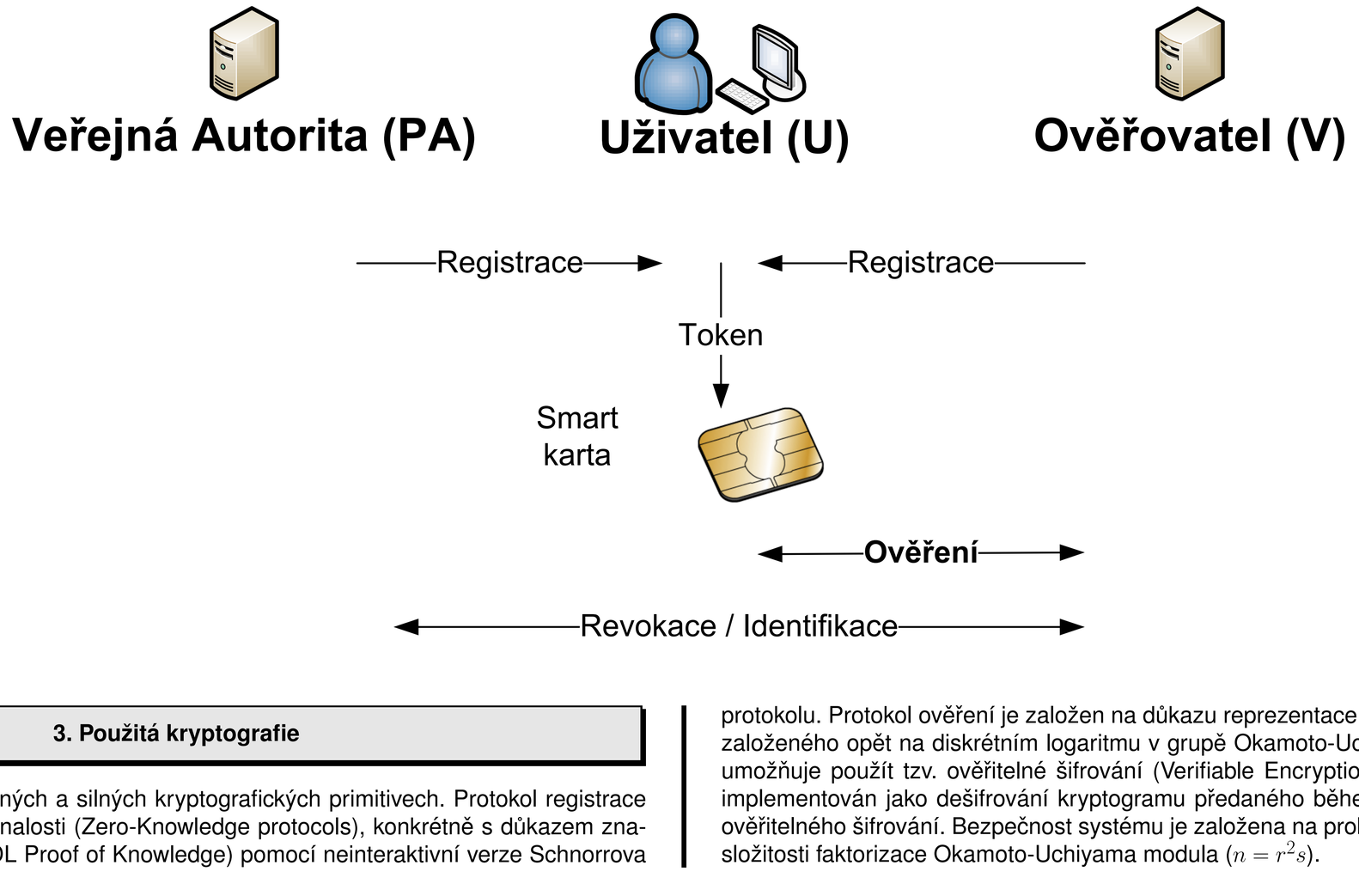
2. Schéma komunikace

Systém umožňuje uživateli (U - User), který je držitelem smart-karty nebo jiného komunikačního zařízení, bezpečné prokázání jeho atributů (věk, adresa, pohlaví, ...) u ověřovatele (V - Verifier). Prokázání atributu je bezpečné, zcela anonymní a nespojitelné v případě více relací prokázání. Pro ochranu ověřovatele je v systému přítomna Veřejná Autorita (PA - Public Authority), která dokáže odhalit ve spolupráci s V útočníky. V systému jsou tedy celkem 3 entity: uživatel U, ověřovatel V a veřejná autorita PA:

- **Uživatel U**: jeho cílem je anonymní využívání služeb, bez obav ze sledování a zneužívání soukromých dat.
- **Ověřovatel V**: jeho cílem je poskytování služeb pouze oprávněným klientům, identifikace útočníků a efektivní správa.
- **Veřejná autorita PA**: úkolem PA je dohlížet na identifikaci útočníků tak, aby V nemohl zneužívat funkce identifikace ke sledování uživatelů, kteří pravidla neporušují.

Schéma, které je zde představeno, je rozděleno do tří protokolů, které odpovídají fázím komunikace. Jedná se o *registraci uživatele*, *ověření uživatele* a volitelné *odhalení identity* uživatele.

- Účelem **registračního protokolu** je přihlášení uživatele k dané službě. Během této fáze se klient identifikuje poskytovateli služby, zaplatí poplatek za využívání systému (např. formou paušálu či předplacenky). Uživatel získá registrační fází autentizační token, který uloží na smartkartu a který anonymně používá pro budoucí ověření.
- Účelem **ověřovacího protokolu** je prokázat, že uživatel U vlastní platný token a že je oprávněn využívat služeb ověřovatele V (a/nebo že vlastní platné atributy). Protokol pracuje s vytvořeným tokenem, který je však pokaždé modifikován tak, aby nemohlo dojít k vzájemnému spojení relací. V této fázi je uživatel zcela anonymní.
- Účelem **protokolu pro odhalení identity** uživatele je odhalení skutečné identity potenciálních útočníků.



3. Použitá kryptografie

Systém je založen na ověřených a silných kryptografických primitivech. Protokol registrace pracuje s protokoly nulové znalosti (Zero-Knowledge protocols), konkrétně s důkazem znalosti diskrétního logaritmu (DL Proof of Knowledge) pomocí neinteraktivní verze Schnorrova protokolu. Protokol ověření je založen na důkazu reprezentace (DL Proof of Representation) založeného opět na diskrétním logaritmu v grupě Okamoto-Uchiyama kryptosystému, který umožňuje použít tzv. ověřitelné šifrování (Verifiable Encryption). Protokol revokace je pak implementován jako dešifrování kryptogramu předaného během protokolu ověření v rámci ověřitelného šifrování. Bezpečnost systému je založena na problému diskrétního logaritmu a složitosti faktorizace Okamoto-Uchiyama modula ($n = r^2 s$).

4. Acknowledgement

Tato Práce vznikla za podpory projektu MŠMT CZ.1.07/2.3.00/09.0067 TeamIT - Budování konkurenceschopných výzkumných týmu pro IT

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ