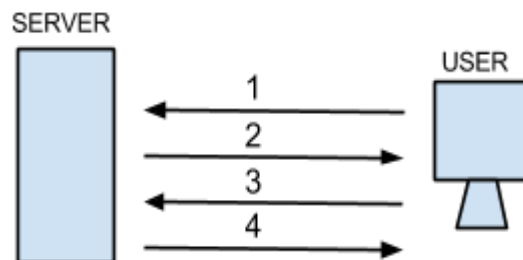


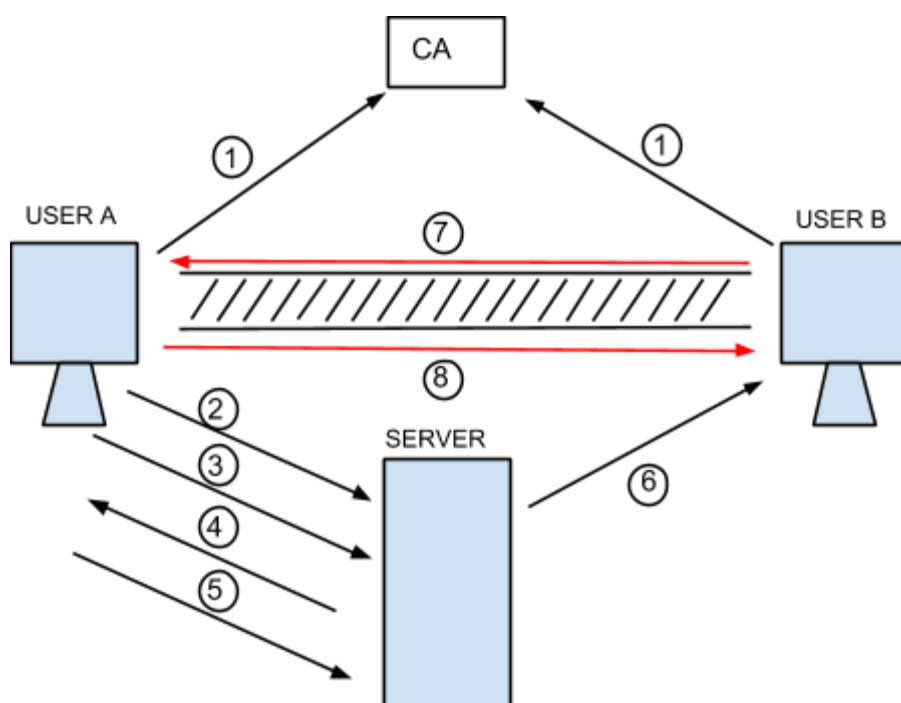
Video-konferenční server

Registrace

1. Uživatel pošle požadavek o registraci serveru.
2. Server pošle certifikát uživateli a uživatel si ověří certifikát v seznamu důvěryhodných certifikátů.
3. Uživatel pošle certifikát (získaný od CA) serveru a server to ověří.
4. Server si vygeneruje náhodné heslo a zašifruje veřejným klíčem uživatele a odešle ho zpět.



Průběh před navázáním spojení



1. Uživatelé požádají CA o vydání certifikátu.
2. Pokud uživatel není registrovaný, požádá server o registraci - jednotlivé kroky viz Registrace. Pokud je registrovaný, tento krok se vynechá a přejde se na krok č.3
3. Uživatel zašifruje login a heslo veřejným klíčem serveru a odešle. Server ověří a přihlásí ho.
4. Server pošle seznam dostupných uživatelů.
5. Uživatel si vybere ze seznamu.
6. Server pošle IP adresu a certifikát uživatele A. Uživatel B ověří certifikát.
7. Uživatel B naváže spojení s uživatelem A a pošle mu certifikát a veřejný klíč.
8. Uživatel A vygeneruje pár symetrických klíčů a jeden zašifruje veřejným klíčem uživatele B a pošle ho uživateli B. Uživatel B dešifruje pomocí privátního klíče. Pak mohou posílat data pomocí symetrických klíčů a hash zprávy.

Použité nástroje:

- Symetrická kryptografie - AES-128
- Asymetrická kryptografie - RSA 1024 bitů
- Certifikáty - norma X.509
- Hashování - SHA-2

Přehled vlastností a funkcí:

- Certifikační autorita
 - veřejný a soukromý klíč
 - seznam certifikátů
 - sign (CA cert, personal info, public key of client) - vytvoří certifikát a zašifruje veřejným klíčem uživatele
 - sendCert (IP receiver , CA cert) - posílá vyhotovený certifikát uživateli
 - addToList (CA cert) - přidá nový certifikát do seznamu certifikátů
- Server
 - seznam registrovaných uživatelů
 - seznam online uživatelů - class (nebo struct)
 - certifikát
 - veřejný a soukromý klíč
 - bool checkCert (cert, VK CA) – ověření certifikátu ověří podpis na daném certifikátu pomocí veřejného klíče CA, v seznamech se hledá jako opatření navíc, kdyby byl certifikát náhodou zneplatněný.
 - registration (login, password, cert) - provede registraci uživatele
 - generPassword () - vygeneruje náhodný klíč
 - encrypt (key, data) - zašifruje pomocí klíče data
 - hash (data) - vytvoření hash
 - sendData (data, IP receiver) - odešle data adresátovi podle IP
 - login (login) - přihlásí uživatele
 - logout (login) - odhlásí uživatele
- Client
 - login
 - veřejný a soukromý klíč
 - IP adresa, certifikát
 - symetrický klíč aktuální komunikace
 - IP adresa druhého uživatele, s kým právě komunikuje
 - encryptSym (key, data) - šifrování pomocí symetrického klíče
 - hash (data) - vytvoření hashu
 - encryptAsym (key, data) - šifrování pomocí asymetrického klíče uvedeného v hlavičce funkce
 - decryptSym (key, data) - dešifruje pomocí symetrického klíče
 - decryptAsym (key, data) - dešifruje pomocí asymetrického klíče uvedeného v hlavičce funkce
 - sendData (data, IP) - odešle data adresátovi podle IP
 - generKey () - vygeneruje symetrický klíč