Webovské rozhranie pre bezpečné zdieľanie dokumentov v cloude

Bakalárska práca

Autor: Peter Kovács

Školiteľ: RNDr. Michal Rjaško PhD.

Problém

Riešenie

Dostupnosť

Cloud

Bezpečnosť dát

Kryptografia

Zdiel'anie dát

Cloud + krypto

Motivácia

- Aktívne využívanie cloudu
- Jednoduché zdieľanie súborov
- Bezpečne ukladanie/zdielanie

Výsledky práce

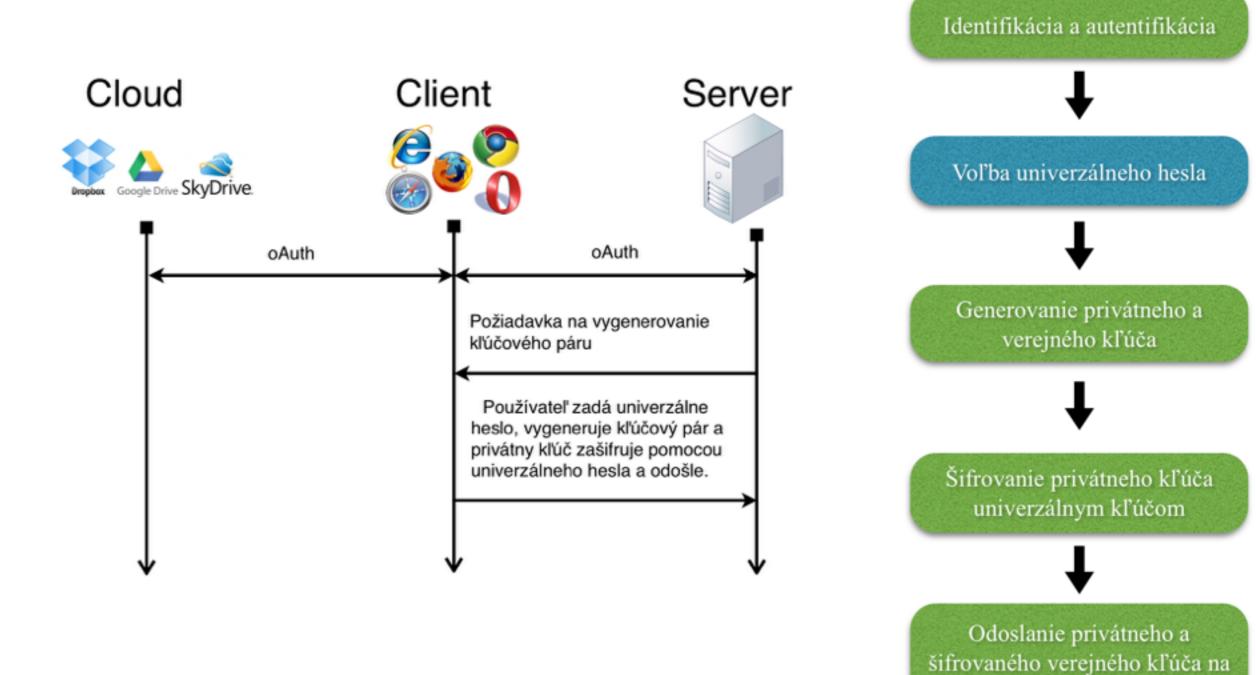
Web

· Ukladanie, sťahovanie, zdieľanie

Technické detaily

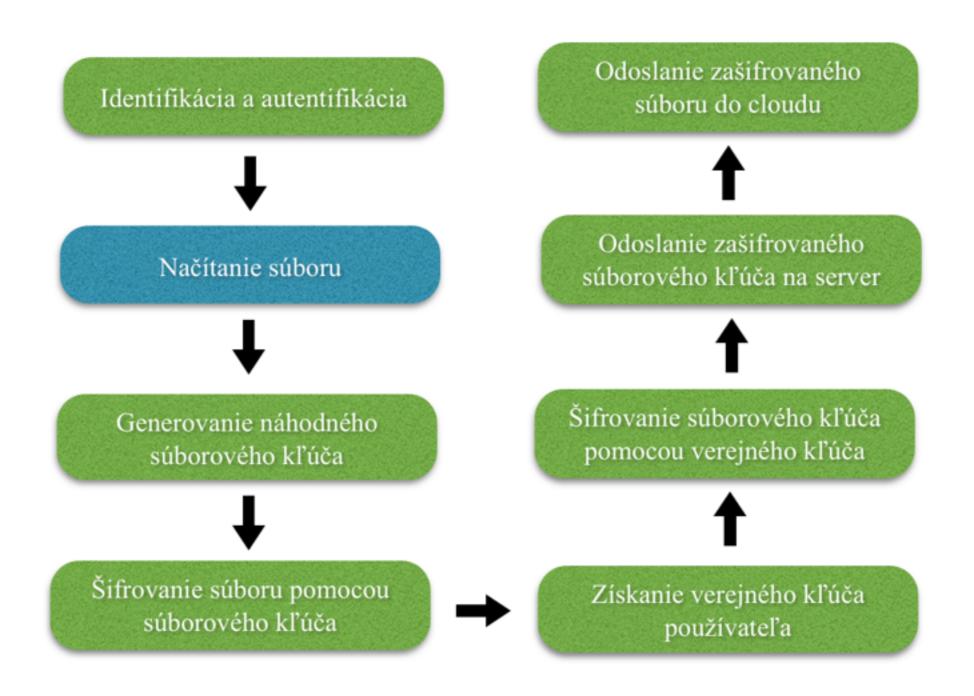
- Registrácia
- Nahrávanie
- Sťahovanie
- Zdiel'anie

Registrácia

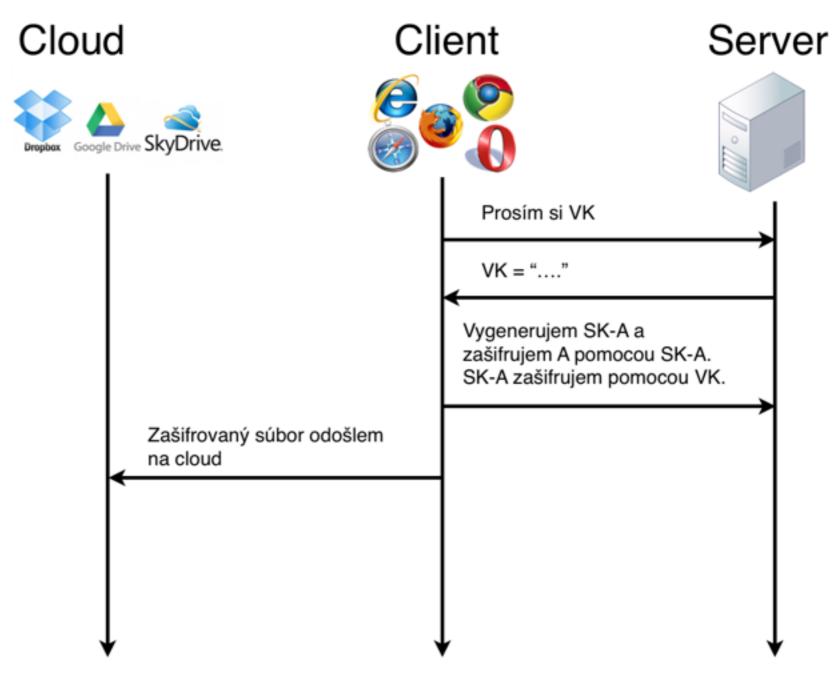


server

Nahrávanie



Nahrávanie komunikácia

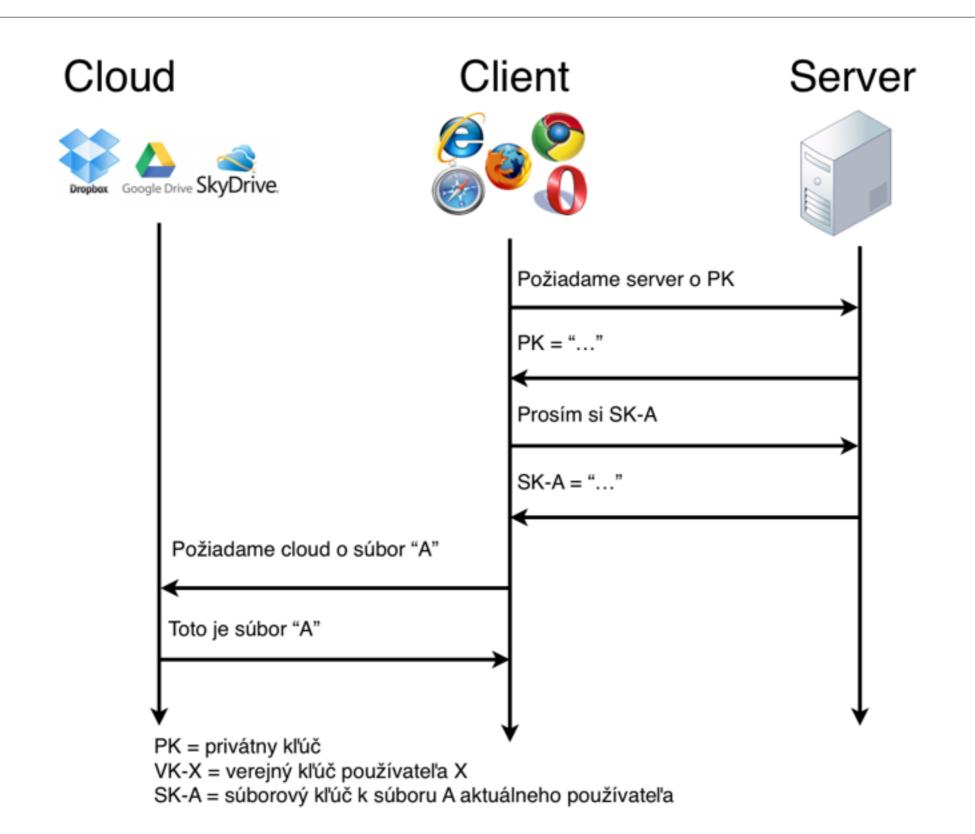


PK = privátny kľúč VK = verejný kľúč prihláseného používateľa SK-A = súborový kľúč k súboru A aktuálneho používateľa

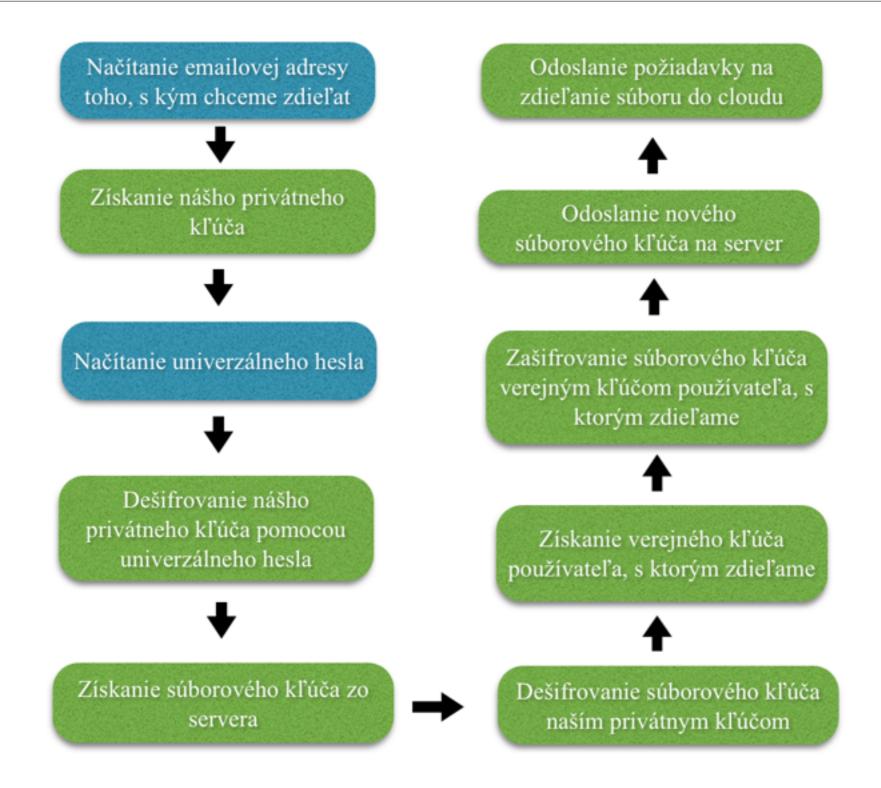
Sťahovanie

Získanie privátneho kľúča Dešifrovanie súboru Načítanie univerzálneho hesla súborovým kľúčom Dešifrovanie privátneho kľúča pomocou univerzálneho Stiahnutie súboru z cloudu hesla Získanie súborového kľúča zo Dešifrovanie súborového kľúča privátnym kľúčom servera

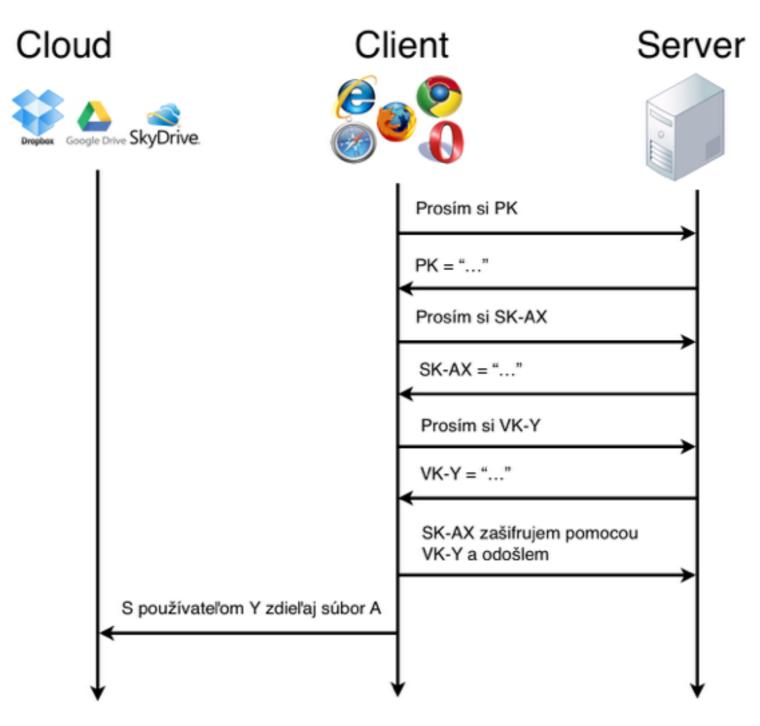
Sťahovanie komunikácia



Zdiel'anie



Zdieľanie komunikácia



PK = privátny kľúč VK-X = verejný kľúč používateľa X SK-AX = súborový kľúč k súboru A používateľa X

Možnosti zlepšenia

- Real-time bezpečná kolaborácia
- Možnosť zdieľaného tajomstva
- UX (progress bary, drag & drop, ...)
- Podpora dalších cloudov (dropbox, box, ...)

Ďakujem za pozornosť