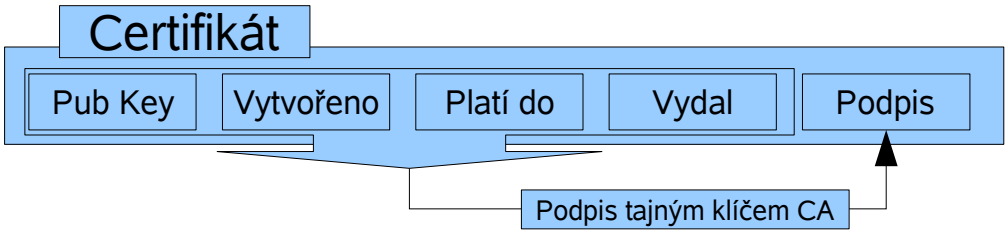
Otázka 2., Asymetrický key-management

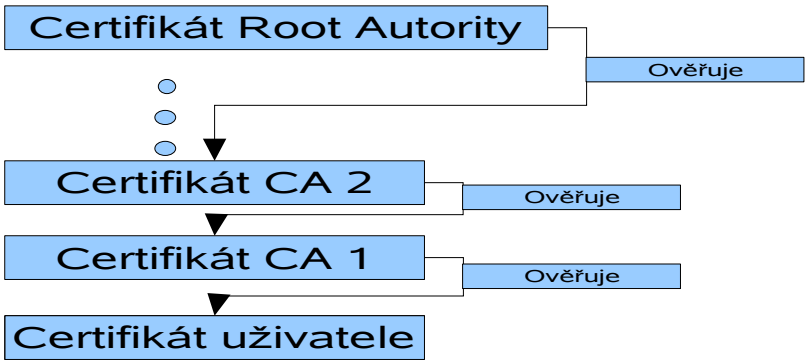
Pokud máme asymetrický klíč, tak rozlišujeme dvě skupiny a to klíče ruční (přenášené v kabele) a ověřované na základě certifikátu.

Co to je certifikát?



Jak se ověřuje klíč certifikacní autority?

Opět asymetrickým klíčem nadřazené CA (Certifikační autority).



Jak se ale dostat k certifikátu centrální autority?

- Pouze osobně, odnést si ho třeba na disketě, viz když si jdeme poprvé do banky pro certifikát.

Pokusy o normalizaci

- Norma x 500, pokus znormalizovat celý svět, celý svět byl seřazen do stromu, na vrcholu jeden certifikát, který měl být "všeobecně známý".

Jak zajistit, vzájemné důvěřování dvou autorit, třeba jednoho ze systému X 500 a nějaké jiné autority?

- Nadklíč, který by ověřoval i X 500 i jinou certifikační autoritu
- Tzv. CROSS-CERTIFIKÁT, kterémý stojí mezi těmito autoritami, a obě ho znají a důvěřují mu
- Prostředník (BRIDGE), entita, která je spojena jedním CROSS-CERTIFIKÁTEM s autoritou X-500 a jedním CROSS-CERTIFIKÁTEM s druhou autoritou.
- Osobní výměna klíčů fyzicky v kabele, nejjednodušší a nejpoužívanější.

Revokační listy (CLV)

Otázkou je, jak odstranit ze stromu klíčů některý, který již dále není klíčem, změna nadřazeného klíče by znamenala obměnit všechny ostatní certifikáty ve stejném patře, jako byl certifikát obměňovaný... Tento problém řeší REVOKAČNÍ LISTY.
CA jednou za nějaký čas vydá a podepíše, které certifikáty již nejsou platné. Pokud důvěřujeme certifikátu, měli bychom ověřit, že není na CVL. Problém je zpoždění (CA vystavuje a podepisuje list tak jednou deně). Od toho jsou OSCP, které odpovídají, co by bylo na CLV, ale není to podepsané.