# Počítačové siete - Elektronický podpis, odtlačok (Hash), certifikačná autorita

## Nástroj, ktorého úlohou je autentizácia odosielateľa elektronického dokumentu.


Požiadavky na prenos údajov možno stanoviť nasledovne:

- **Utajenie údajov** predstavuje ochranu údajov pred nepovolanými objektmi či subjektmi (najmä v prípade použitia verejných kanálov na prenos citlivých informácií).
- **Integrita informácií** požaduje, aby doručené informácie boli úplné a pôvodné (nezmenené počas prenosu). Ak by aj niekto odhalil kľúč a správu dešifroval, aby nemohol zmiasť a dezinformovať adresáta zmenou obsahu.
- **Autentizácia** spočíva v potvrdení totožnosti odosielateľa správy.

Utajenie je zabezpečené kryptovaním prenosu, integrita informácií a autentizácia odosielateľa **elektronickým podpisom**, ktorého úlohou je potvrdiť, že podpisujúci je skutočne ten, za ktorého sa vydáva a že súhlasí s obsahom podpísaného dokumentu. Postupne stále viac právnych predpisov (zákon o elektronickom podpise bol schválený v roku 2002) umožňuje používanie elektronického podpisu v oblasti orgánov verejnej správy, a to ako pri komunikácii medzi úradmi navzájom, tak i pri komunikácii občanov s nimi.

Každý elektronický podpis ma dva kľúče - súkromný a verejný. Platia pre ne rovnaké pravidlá, ako pre kľúče používané pri asymetrickom šifrovaní. Elektronicky môžeme podpísať akýkoľvek súbor - e-mail, video, obrázok atď.

Z údajov dokumentu sa v prvom kroku vytvorí tzv. **odtlačok** (*hash*) - číselná hodnota získaná aplikáciou špeciálneho algoritmu. V druhom kroku sa hash zašifruje prostredníctvom autorovho súkromného kľúča - výsledok šifrovania sa označuje ako elektronický podpis. Tento je pre rovnaký dokument vždy rovnaký a pre rôzne dokumenty zvyčajne iný.

Adresát dostane podpísaný dokument a podpis. Overenie spočíva vo výpočte hashu z dokumentu a v jeho porovnaní s hashom získaným dešifrovaním elektronického podpisu prostredníctvom verejného kľúča. Pokiaľ sú oba odtlačky totožné, je dokument považovaný za dôveryhodný.

Autor nemôže poprieť svoje autorstvo, pretože jeho súkromný kľúč je tajný a nikto iný nemôže zašifrovať hash tak, aby bol pri použití verejného kľúča totožný so správnou hodnotou.

Pokiaľ dokument počas prenosu zmení niekto iný, zmení sa i jeho hash a výsledok dešifrovania podpisu nebude totožný s hashom nového dokumentu.

Certifikát umožňujúci využívanie elektronického podpisu poskytuje **certifikačná autorita**, reprezentovaná dôveryhodnou osobou alebo inštitúciou, ktorá vystavuje bezpečnostné certifikáty určené na identifikáciu majiteľa elektronického podpisu (napr. na základe databázy elektronických podpisov potvrdí, že osoba, ktorá elektronický dokument podpísala, je naozaj tou , za ktorú sa vydáva). Pri elektronickej komunikácii tak plní úlohu prostredníka medzi komunikujúcimi subjektmi a potvrdzuje pravosť elektronického podpisu.

Certifikačná autorita vystupuje v úloha akéhosi notára, ktorý overuje elektronický podpis a garantuje osobu, ktorej patrí a dokedy platí. Právo na poskytovanie služieb certifikačnej autority prideľuje koreňová certifikačná autorita (u nás Prvá certifikačná autorita spravovaná Národným bezpečnostným úradom).

Bezpečnostný certifikát ↑