IOT KERETRENDSZEREK ÉS IPARI ALKALMAZÁSAIK

SmartComLab

IoT keretrendszerek felépítése II. : adatbázisok, biztonságtechnikai megoldások

Adatbázis típusok az IoT-ben

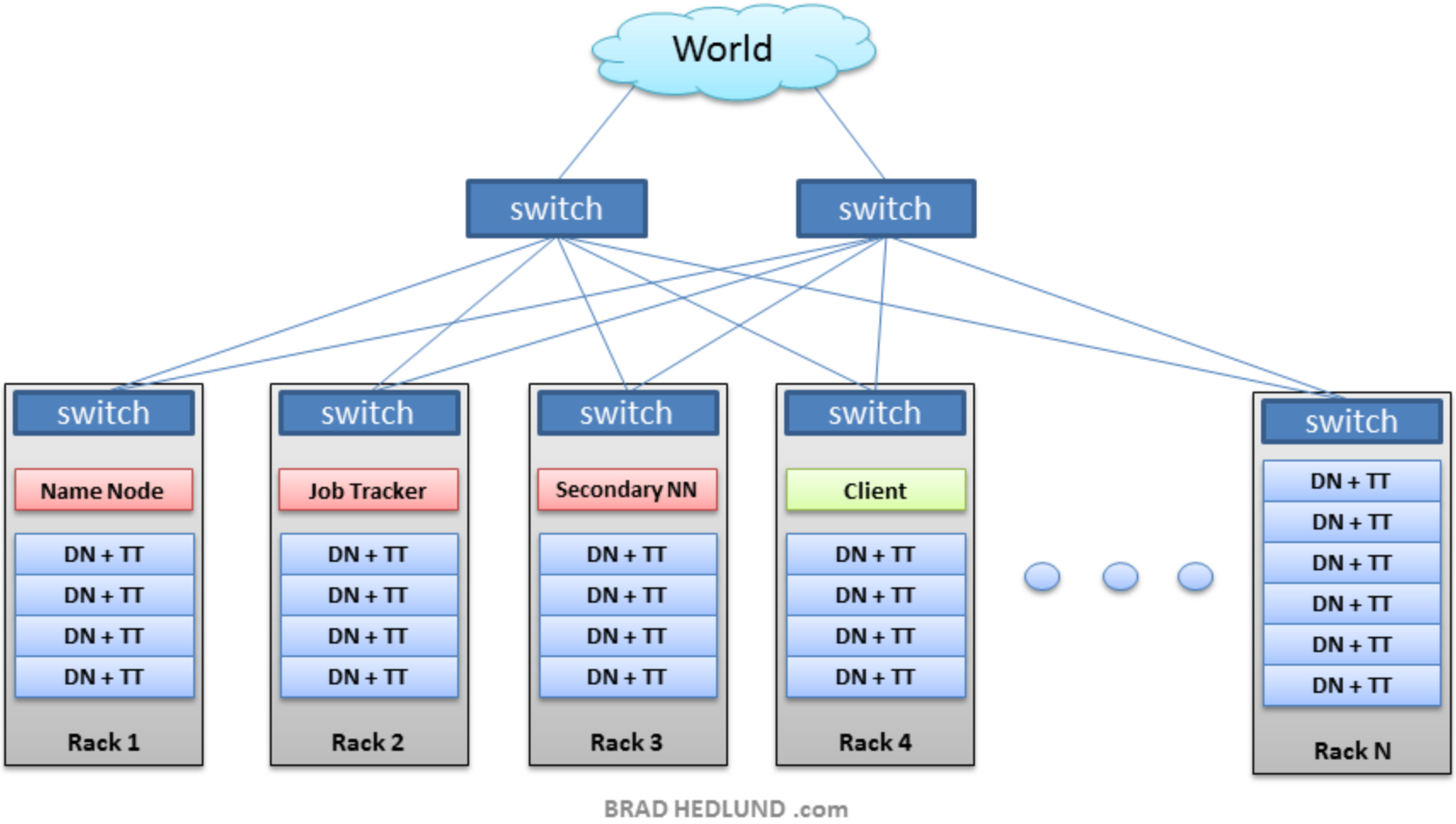
Alapvetések

- Régen szerettük az SQL-t, ma már mindenre más van (10 year challenge).
- Az IoT-ben heterogén adatforrások vannak. Ezt nehéz kezelni relációs adatbázisokkal.
- Adatbázis típusok:
  - Traditional SQL databases: Microsoft SQL, MySQL, …
  - Big Data File Systems: Google File System, Hadoop File System, Disco File System
  - NoSQL: Key-Value, Column-Oriented, Documents, Graph

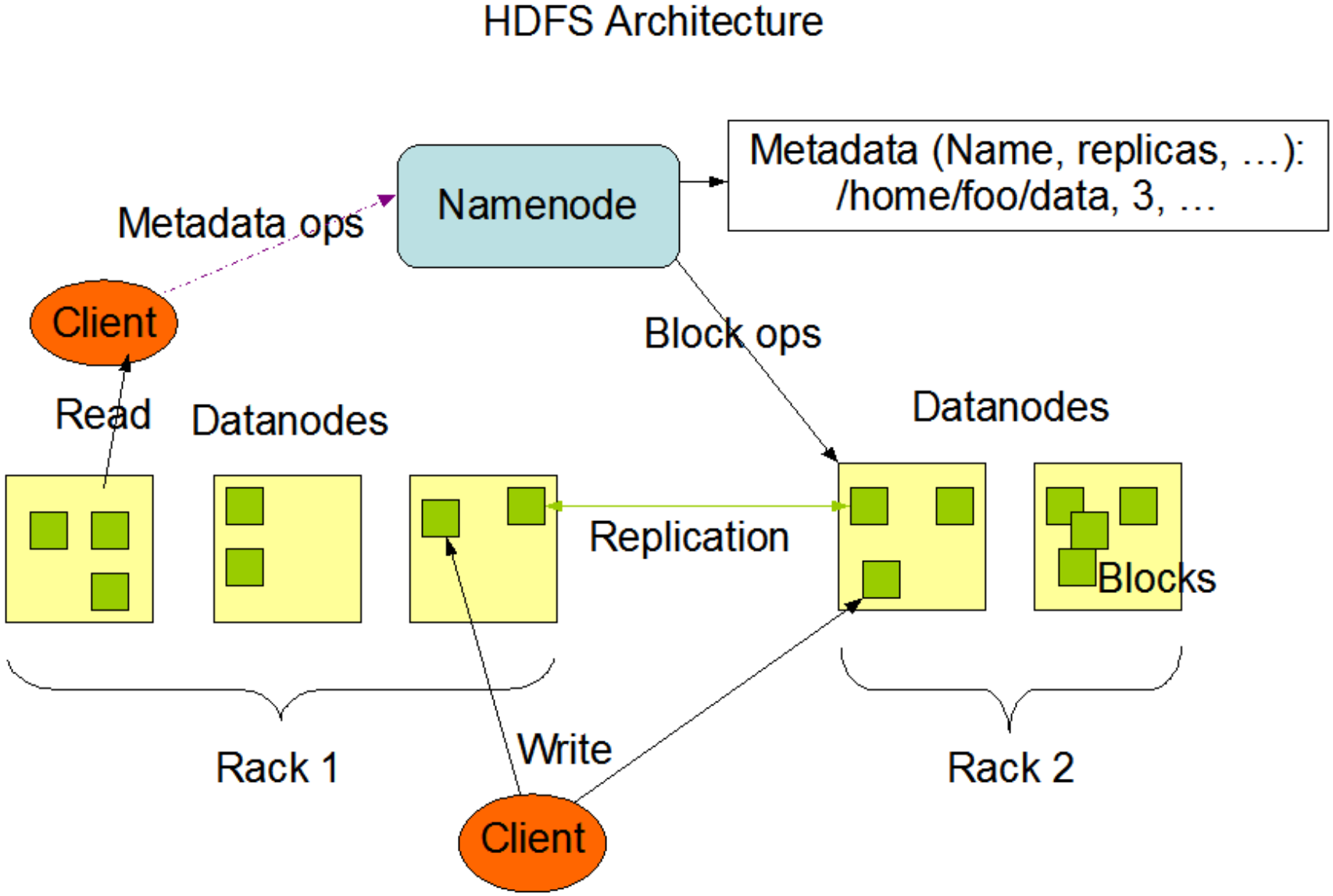
Big Data File Systems

- Példák
  - Hadoop FS
  - Google File System
  - Disco Distributed FS
- Fájlok tárolása hibatűrő és skálázható módon a hálózaton
  - Replikálva (~RAID), cluster balance-olás (terheléselosztás)
- URL-hez hasonló fájlrendszer elérhető a kliensekben
- Enyhén relaxált POSIX parancsok: stream és egyidejű fájlhozzáférés lehetővé tevése

Hadoop Cluster



Hadoop hálózati felépítés

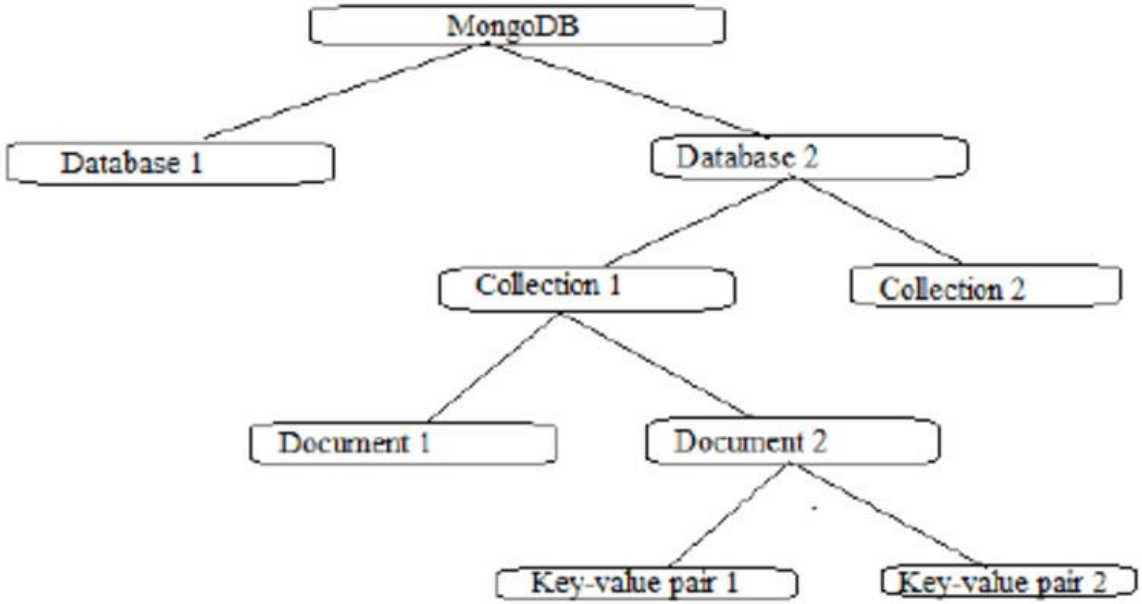


NoSQL

- key-value: kulcs-érték párok
  - Range query, nincs fix séma, magas skálázódás
  - pl. Cassandra, Voldemolt
- column-oriented
  - Pl. hBase vagy HyperTable
- document-oriented
  - MongoDB: plaintext documents, query of entries
- graph-oriented: gráfot tárol hatékonyan, gráfkeresések végrehajthatók
  - Neo4J
- time-series adatbázisok is léteznek

MongoDB

- JSON vagy plaintext alapú dokumentumok tárolása, lekérése



MongoDB vs SQL terminológia

Relationship of MySQL terminology with MongoDB

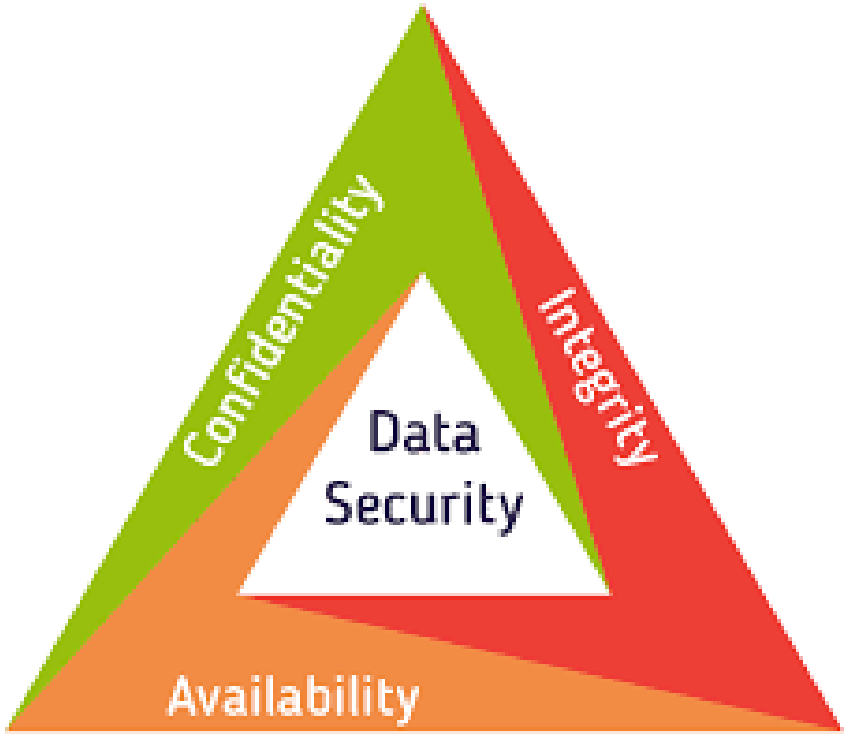
MySQL	MongoDB
Database	Database
Table	Collection
Row	Document
Column	Field
Table Join	Embedded Documents
Database Server and Client	
mysqld/mysql	Mongod/mongo

Data lake def

- A data lake is a system or repository of data stored in its natural format, usually object ***blobs*** or files.
- A data lake is usually a single store used for tasks such as reporting, visualization, analytics and machine learning.
  - structured data from relational databases (rows and columns)
  - semi-structured data (CSV, logs, XML, JSON)
  - unstructured data (emails, documents, PDFs)
  - binary data (images, audio, video)

Biztonságtechnikai megfontolások

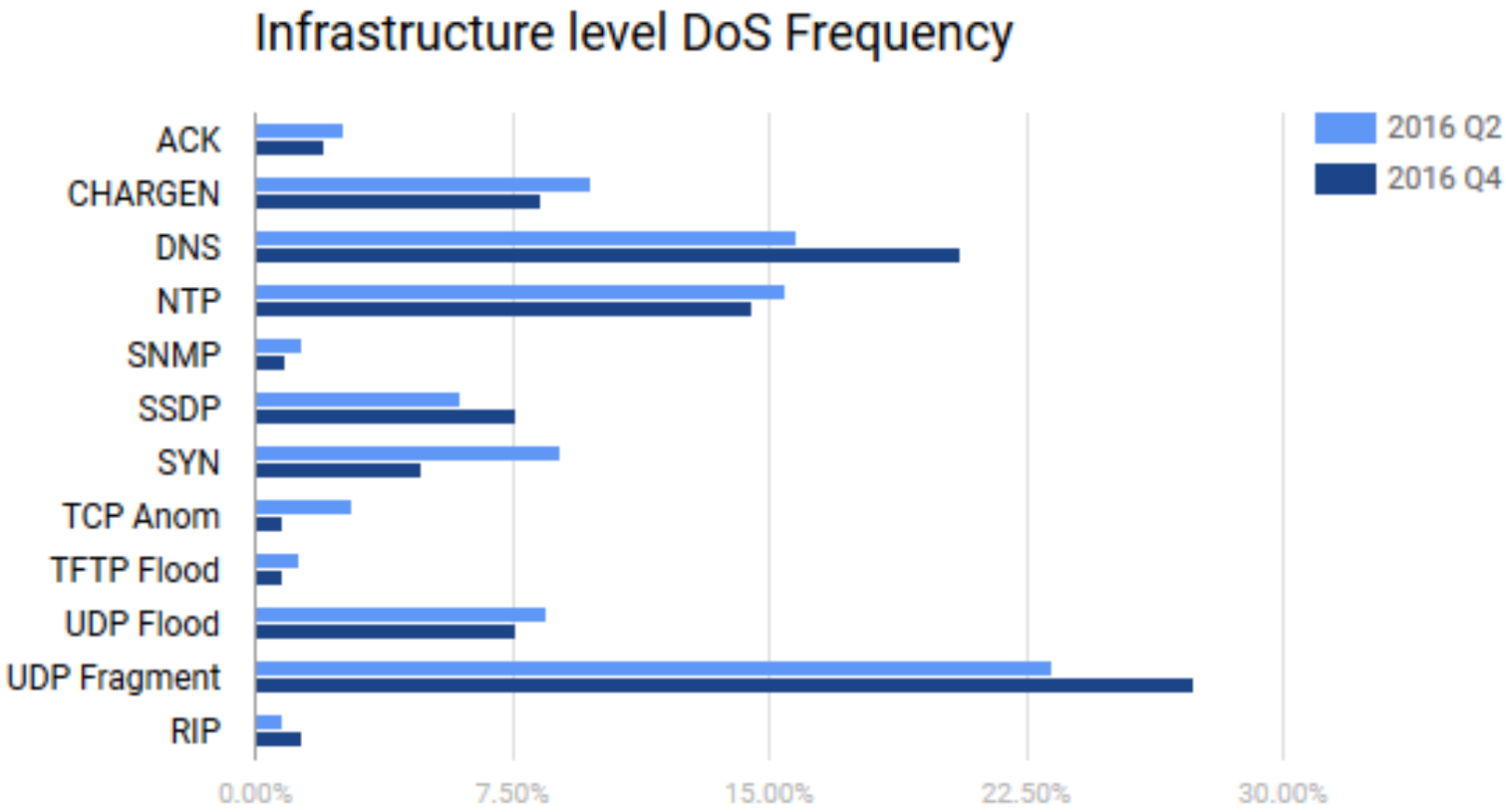
Az információ-biztonság alapelvei



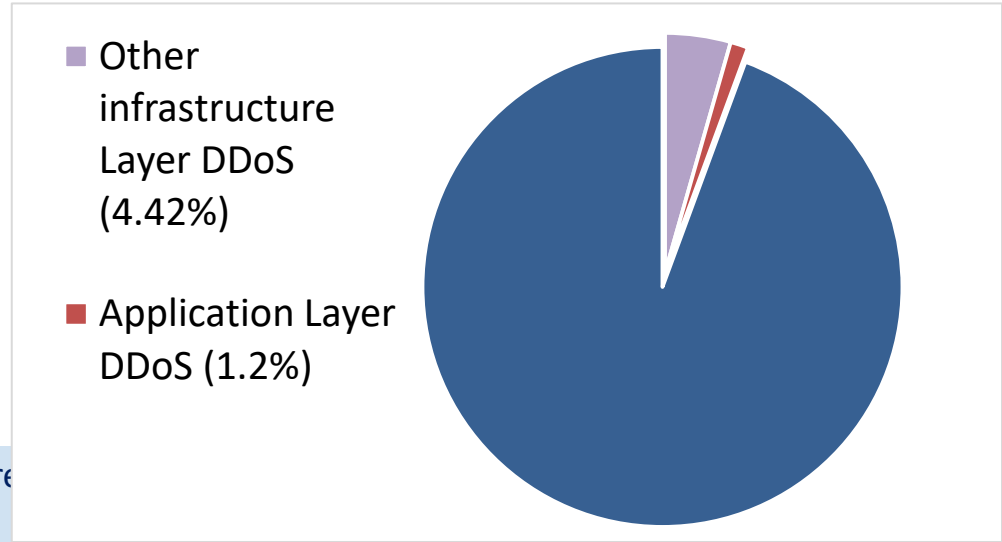
- CIA
  - Confidentiality
  - Integrity
  - Availability

Fenyegetések és védelmi stratégiáik

Layer	Threat type	Mitigation
Physical	Tampering	tamper-resistant packaging
	Eavesdropping	encryption, authorization
	Denial of Service	spread-spectrum techniques
Networking	Exhaustion	active firewalls, passive monitoring (probing), traffic admission control, bi-directional link autentication
	Collision	
	Unfairness	
	Spoofing	
	Selective forwarding	
	Sinkhole	
	Wormhole	
	Sybil	
	Flooding	
Data processing	Exhaustion	traffic monitoring
	Malware	malware detection
Application	Client app.	anti-virus filtering
	Communication	
	Integrity	testing
	Modifications	validation
	Multi-user access	process planning and design
	Data access	Traceability



Gyakori DDoS támadástípusok

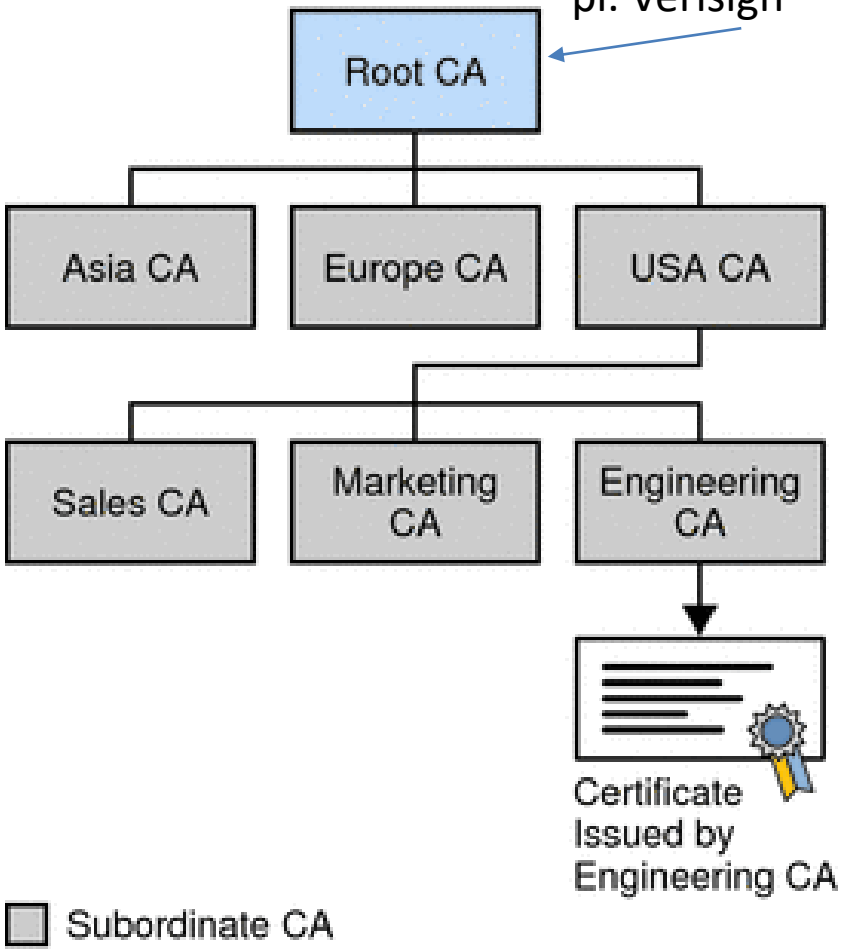


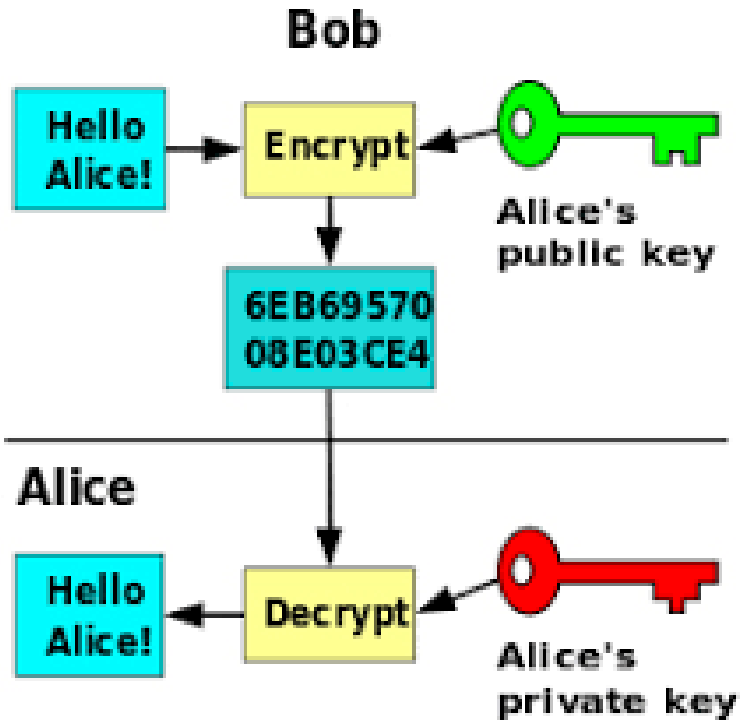
AAA

- Authentikáció
  - Az-e, akinek mondja magát: identitás ellenőrzése
  - Pl. username/password, certificate segítségével (PKI)
- Authorizáció
  - Van-e jogosultsága az adott cselekvést végrehajtani
  - (adott felhasználó hozzáférési/változtatási jogosultságának kezelése)
- Accounting
  - mit, mennyit, hogyan, mennyiért csinált
  - számlázást, adatnyilvántartást általában külön rendszer végzi

Public Key Infrastructure

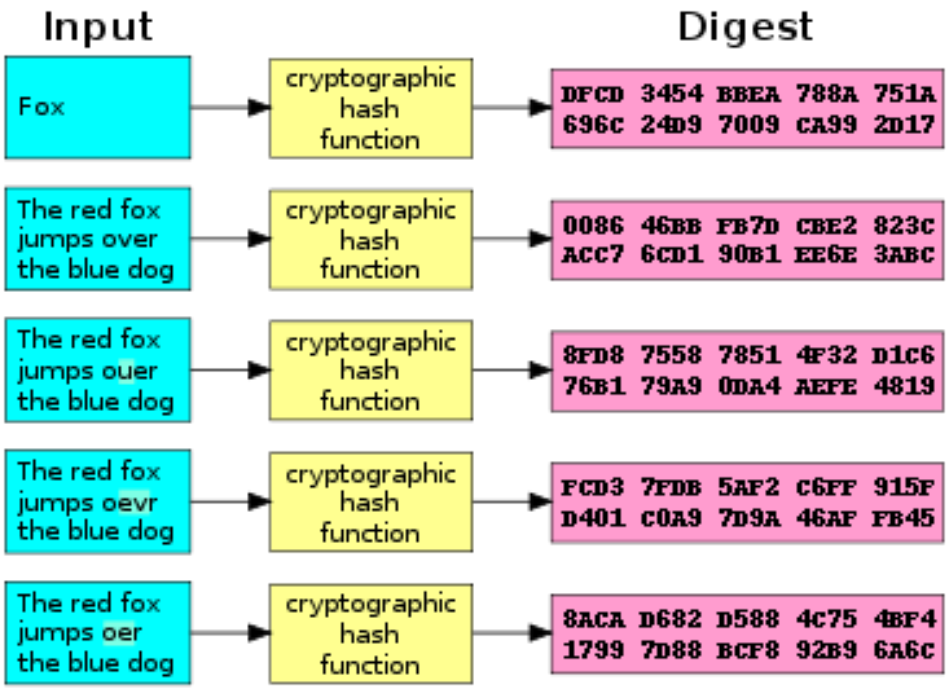
Trusted root CertAuth,
pl. Verisign

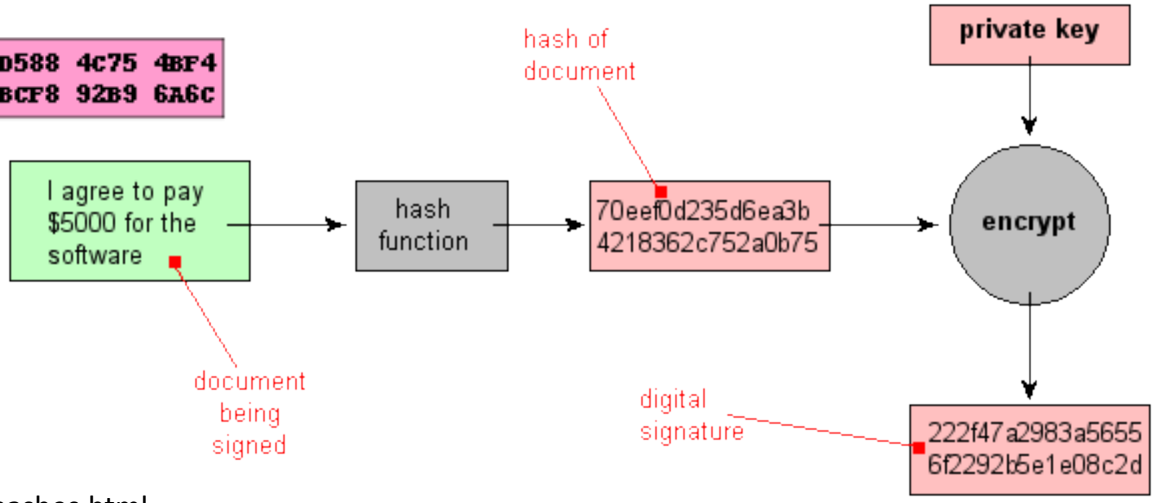




from oracle.com

Cryptographic hash function

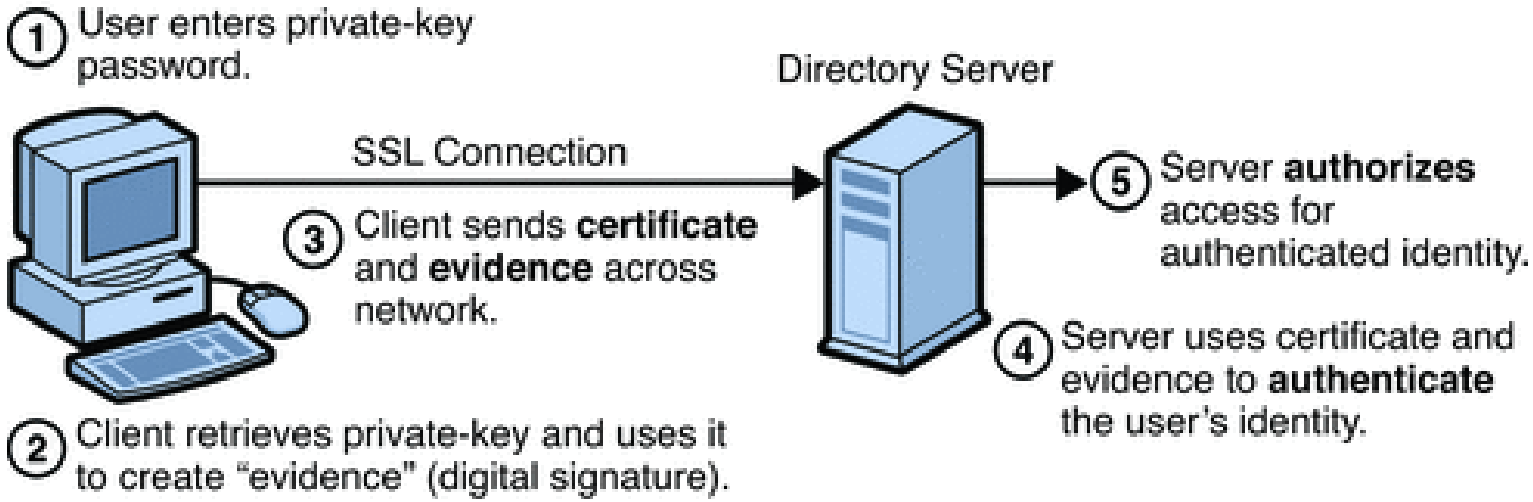




Steve Friedl's Unixwiz.net Tech Tips
An Illustrated Guide to Cryptographic Hashes
http://www.unixwiz.net/techtips/iguide-crypto-hashes.html

Cerfificate-alapú authentikáció

- A folyamat



from oracle.com

Certificate-alapú Authorizáció

- Miket ellenőrzünk?
  - Has the Digital Certificate been issued/signed by a Trusted CA?
  - Is the Certificate Expired – checks both the start and end dates
  - Has the Certificate been revoked? (Could be OCSP or CRL check)
  - Has the client provided proof of possession?

Modern AA módszerek

- SSO: Single Sign On
- oAuth2
- JWT: JSON Web Token