

Digital Certificate

PKI

CA

X.509

Wild card

CRL

OCSP

OCSP Stapling

Key strength

Randomness (entropy)

Key length

Password

Biometric

Key Fob

Geo location



'Trust'

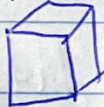
Identity

Authentication

Authorization

Accounting

Amazon server



?



3rd party.

Trust



Certificate

Chain of Trust

TPM

HSM

CRL

or

OCSP

or

OCSP Stapling

YTB-

Cryptography; Key management.

Strength depends on: randomness & Length.
Entropy.

Pseudo RNG (PRNG) - software approximates entropy. True random # generator (TRNG)

YTB

What is TPM trusted Platform module & what does it do.

Hardware Security Module (HSM)

YTB

What are hardware security module?
learn. cantrillo.io

Certificate authorities Digital cert. Root of	Data masking tokenization
---	------------------------------

YTB - Data state, Data at rest, Data in transit, and in-use.

Data at rest *data in a persistent storage media*
Data in transit (*data in motion*): *data is transmitted over network.*

Data in use (*data in processing*): *data is present in volatile memory.*

Bulk data encryption (*hybrid encryption*).

Encrypt entire database, field,

Prof. messer
YTB

Perfect forward Secrecy

Cipher suit:

- Hash
- Symmetric
- Asymmetric

D-H - key exchange.

RSA - ECC

Credential:

Something you are
Something you know
Location
Something you have

YTB

YTB

YTB

Steganography Practice | Steganography examples
Password hashing, salts, Peppers | Explained
How to salt & pepper passwords

sunny classroom.