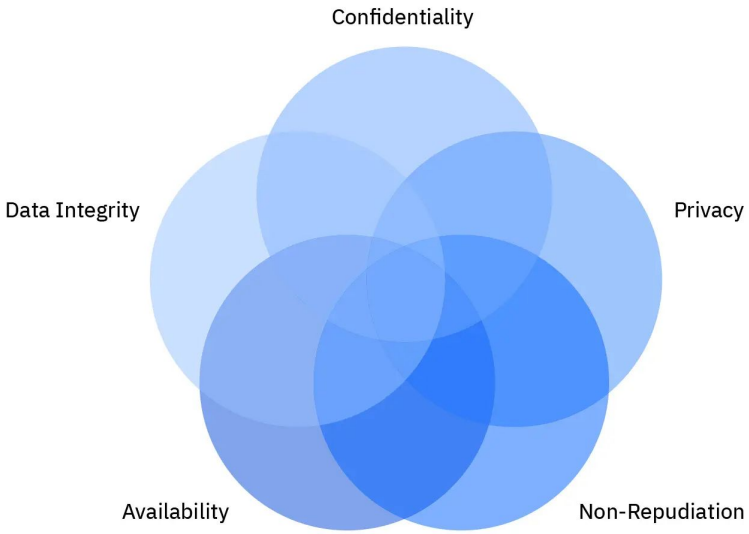
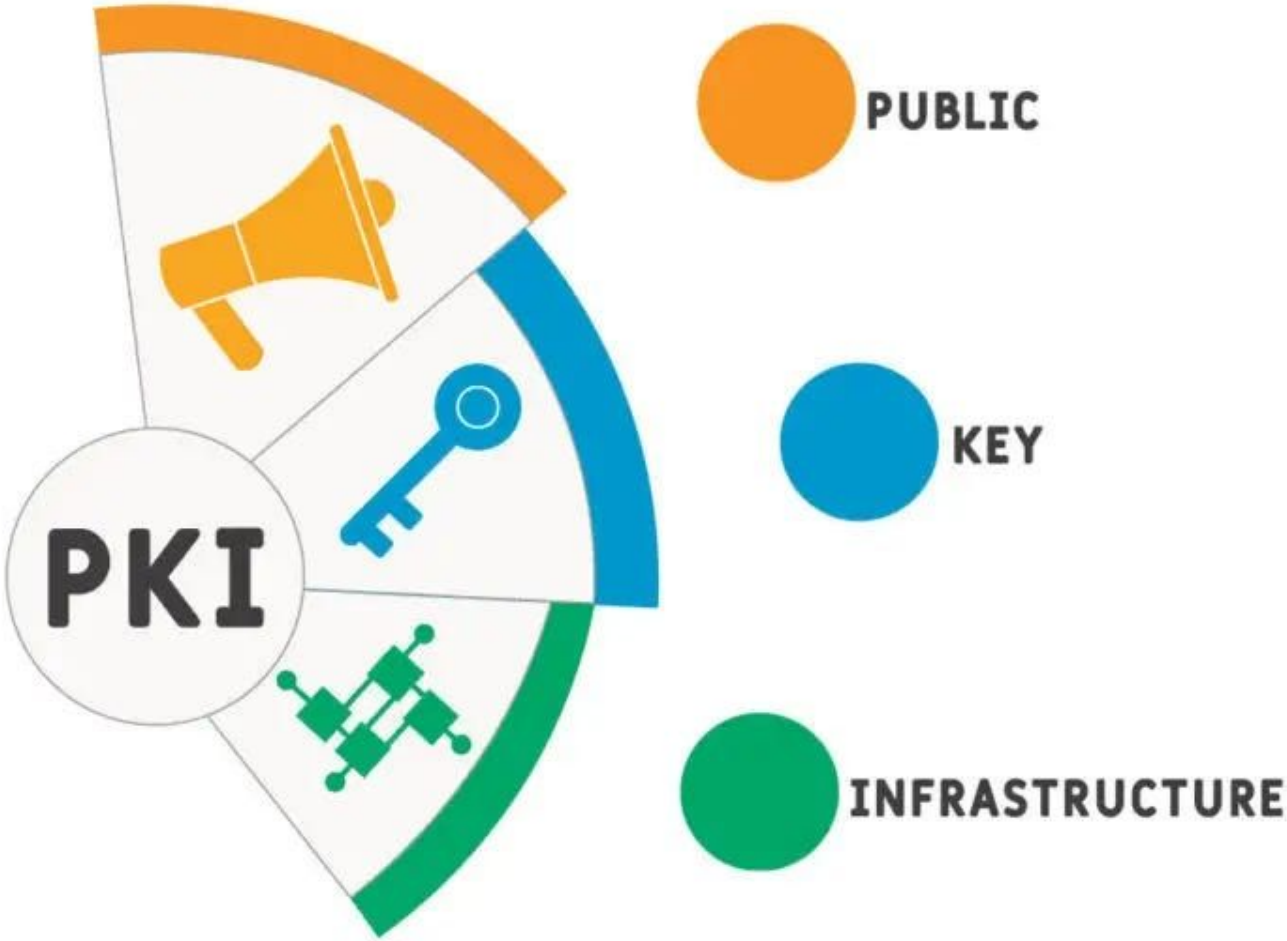
Cryptographic Solutions

What is Cryptography?

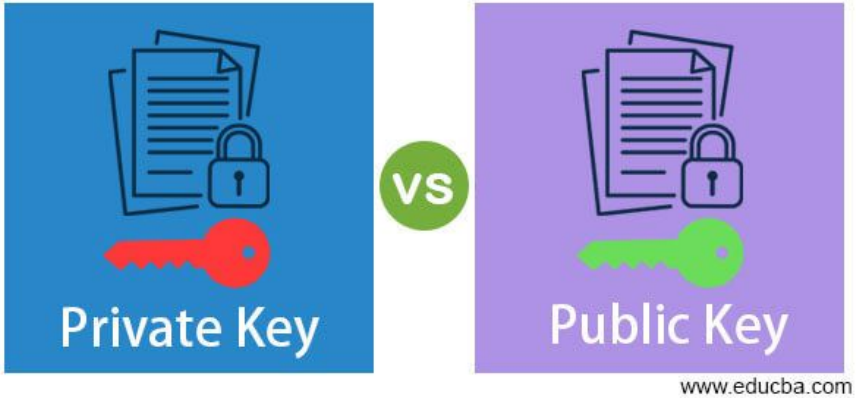
Cryptographic Solutions



- Public Key Infrastructure
- Encryption
- Algorithms & Exchange
- Tools
- Obfuscation
- Blockchain
- Hashing & Salting
- Certificates


PKI
PUBLIC
KEY
INFRASTRUCTURE

Public & Private Keys



Private Key:

- Must be kept secret
- Used to decrypt data encrypted with the corresponding public key
- Creates digital signatures

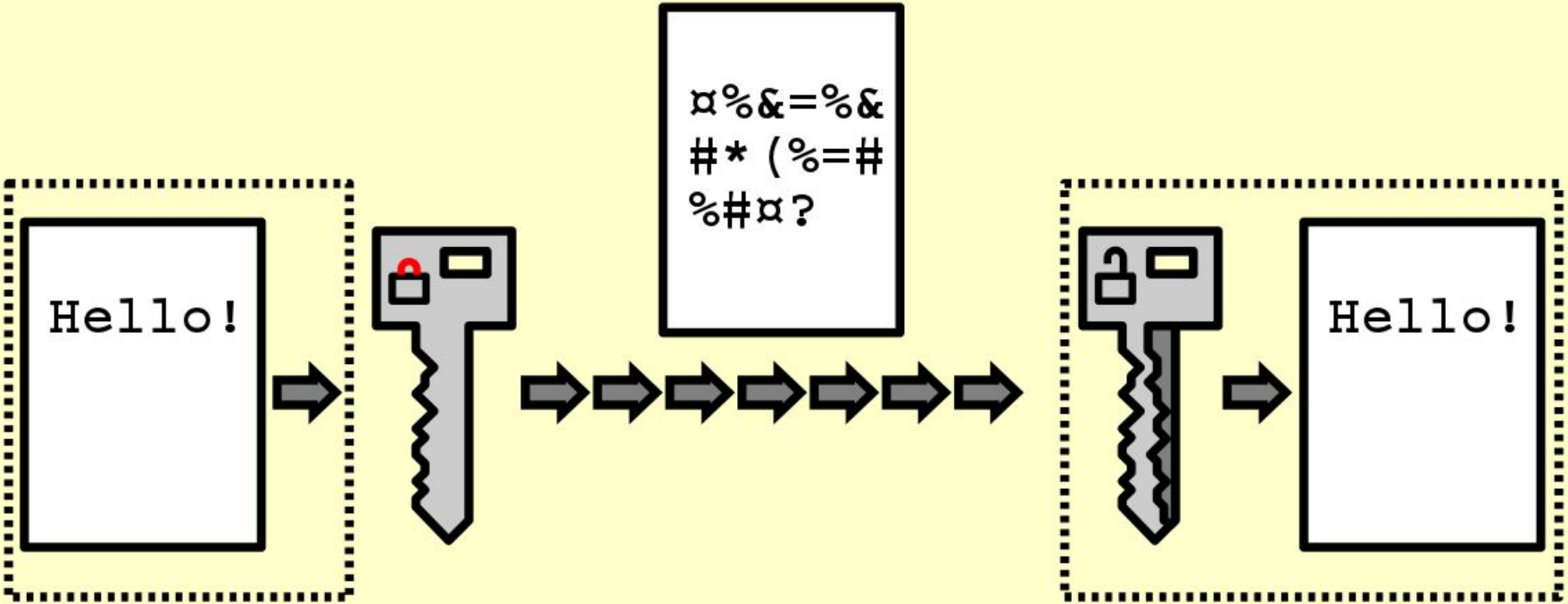
Public:

- Shared openly
- Used to encrypt data or verify a digital signature

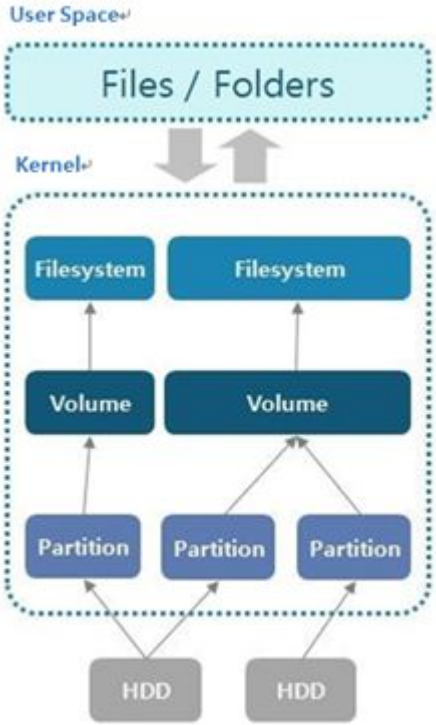
Key Escrow

- Third party
- Securely stores cryptographic keys
- Allows authorized entities to access the keys
- Ensures keys can be recovered in emergencies

Encryption



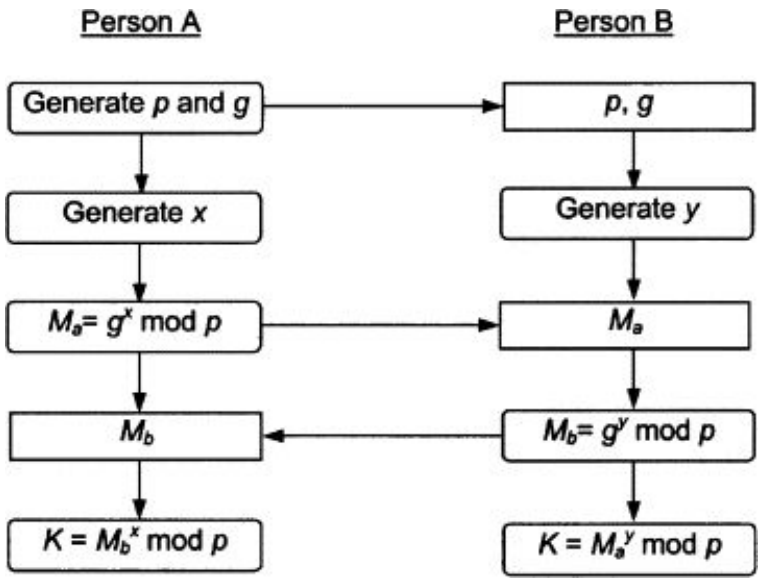
Levels of Encryption



- FDE
- Partition
- File
- Volume
- Database
- Record
- Transport/Communication:
  - TLS, HTTPS, VPN…

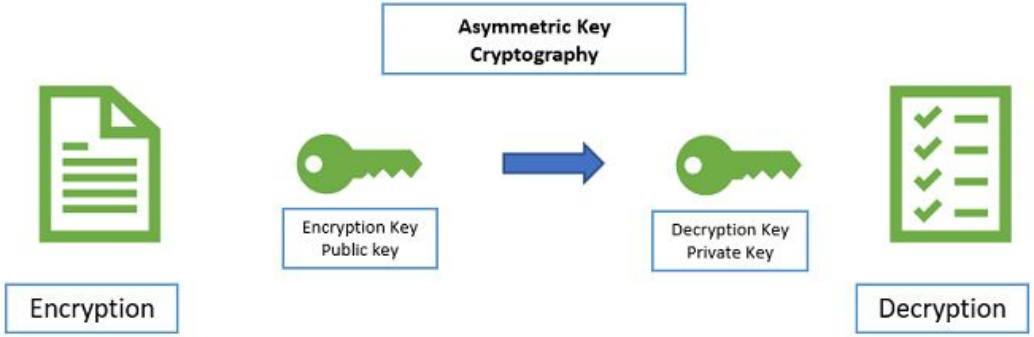
Algorithms & Key Exchange

Algorithms



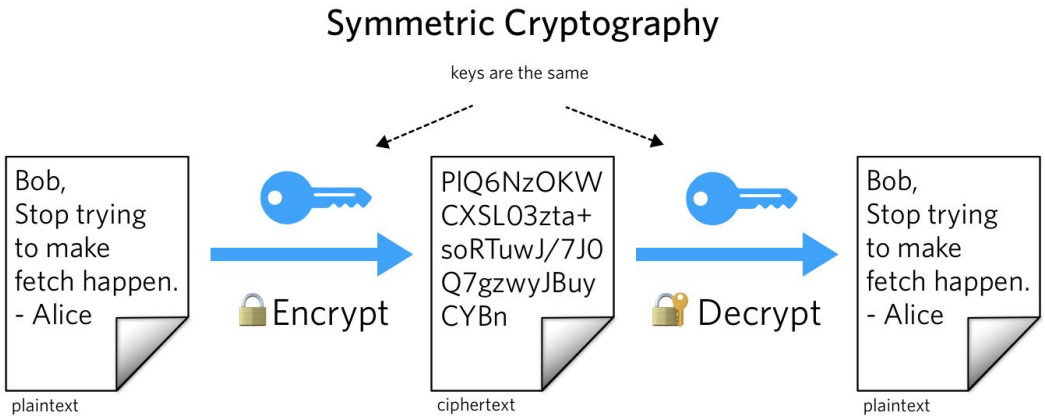
- Mathematical procedures/rules for encryption and decryption operations
- Both sides of an interaction agree on the algorithm before a transfer
- Often hidden from the user
- Well known and often public
- Only unknown entity is the key

Asymmetric



- Also known as public-key cryptography
- Uses pairs of keys (public and private) for encryption and decryption
- Private keys, due to the math involved, are underivable from the shared public keys

Symmetric



- The key used to encrypt a message is the key used to decrypt the message
- Known as a single, shared key
  - “shared secret”
- Faster than asymmetric encryption

Key Exchange

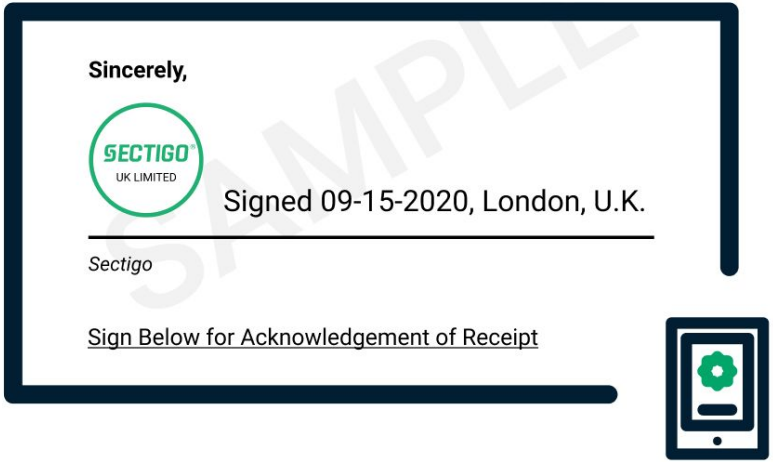
- Exchanges could be physical and in-person (Out-of-Band)
- In-Band key exchange is on the network and provides keys with additional encryption and fast security
  - e.g.: sharing a symmetric key using asymmetric encryption

Key Length

Key Size (bits)	RSA (ms)		MDRSA (ms)	
	Encryption time	Decryption time	Encryption time	Decryption time
128	8.388608	5.24288	12.582912	12.582912
256	14.68006	12.582912	74.4489	68.15744
512	134.2177	134.2133	536.8709	536.8709
1024	536.8709	402.6532	3087.0078	3087.0078
2048	3489.661	3355.443	26172.457	26575.11

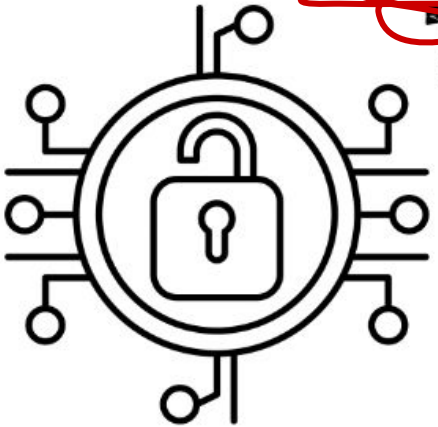
- The size of keys measured in bits
- Longer keys provide stronger security against brute-force attacks
  - May require more computational resources
- Make weak keys stronger with key stretching/strengthening

Digital Signatures



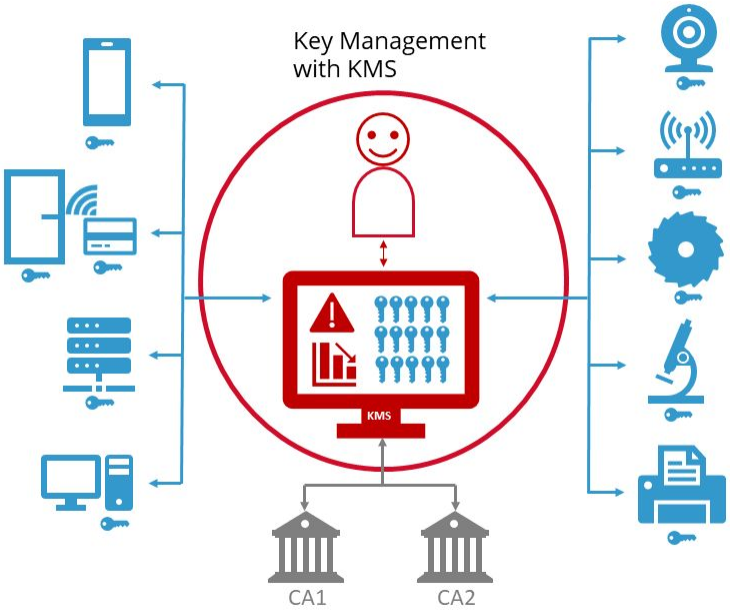
- Use public-key cryptography to sign messages
- Provides integrity and non-repudiation
- Signer uses their private key to generate signature
- Verified by anyone with access to the corresponding public key

CRYPTOGRAPHY TOOLS ~~AND TECHNIQUES~~ (just tools)



codestudio POWERED BY CODING NINJAS

Key Management System



- Software or hardware solutions used to generate, store, distribute, and manage keys
- Ensure secure key handling, access control, and compliance with encryption policies

Trusted Platform Module

- TPM is a dedicated microcontroller for hardware-level security
- Contains a cryptographic processor that provides random number and key generators
- Persistent memory
- Versatile memory to store and manage keys

Hardware Security Module

- HSM is a dedicated hardware device
- Generate, store, and manage cryptographic keys
- Used for large environments
- High-level hardware and accelerators for cryptographic operations
- Secure backup

Secure Enclave

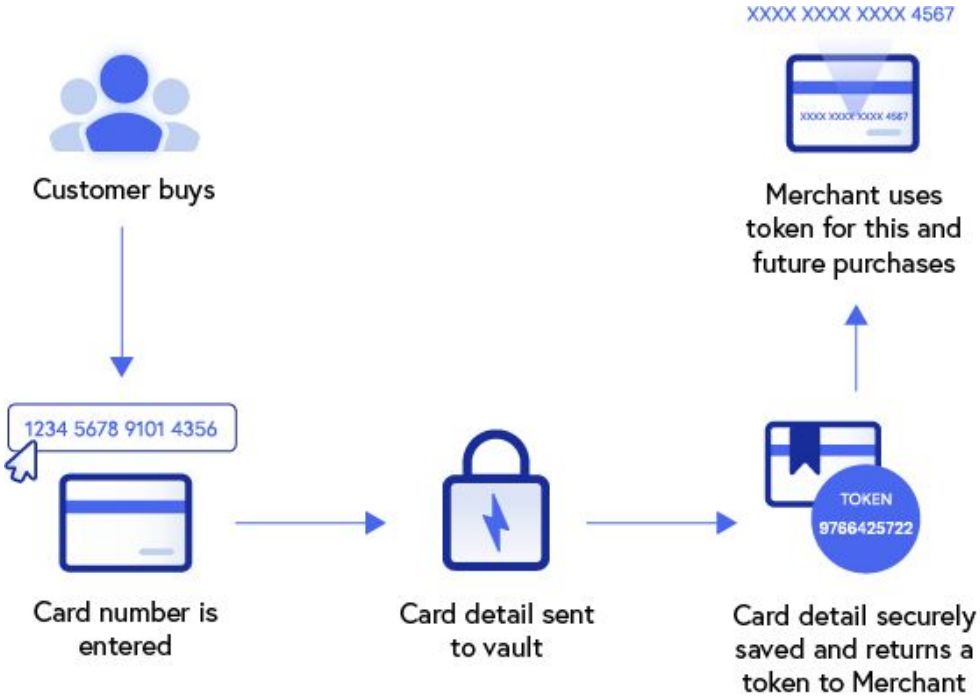
- Hardware-based secure processing environment isolated from OS and memory
- Provides an environment for key management, secure bootstrapping, and data protection
- Separation of data on connected systems

Obfuscation

Steganography

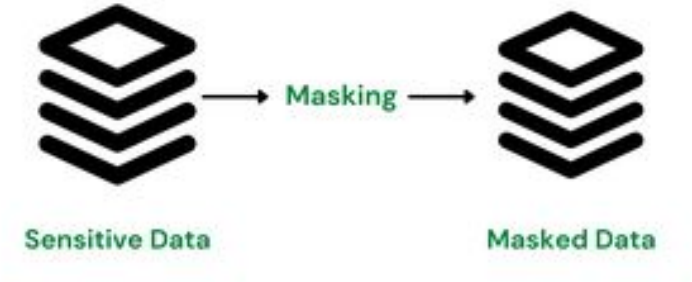
- Hiding secret information within seemingly innocuous data, such as images
- The message's container is called the "covertext".

Tokenization



- Replace sensitive data with unique identifiers called tokens
- Tokens have no meaningful value outside the context of the tokenization system

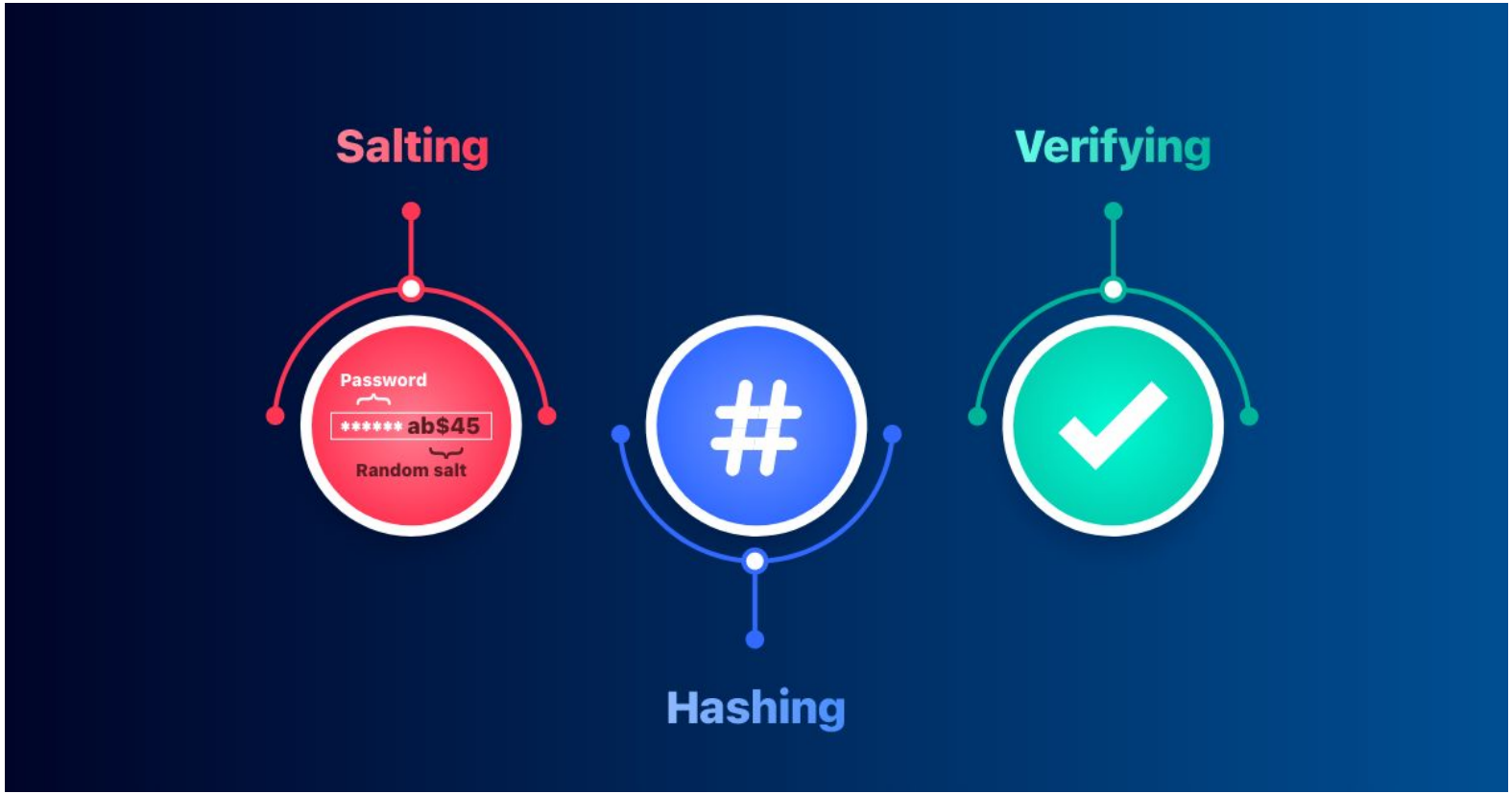
Data Masking



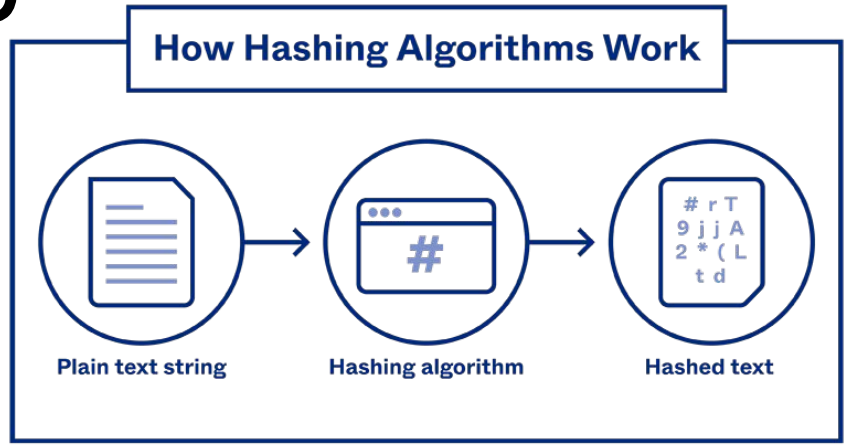
Visual to help understand the complex processes behind masking

- Obscures sensitive information by replacing real data with fictional values
- For example, a social security number may be displayed as: ***-**-1234

Hashing & Salting



Hashing

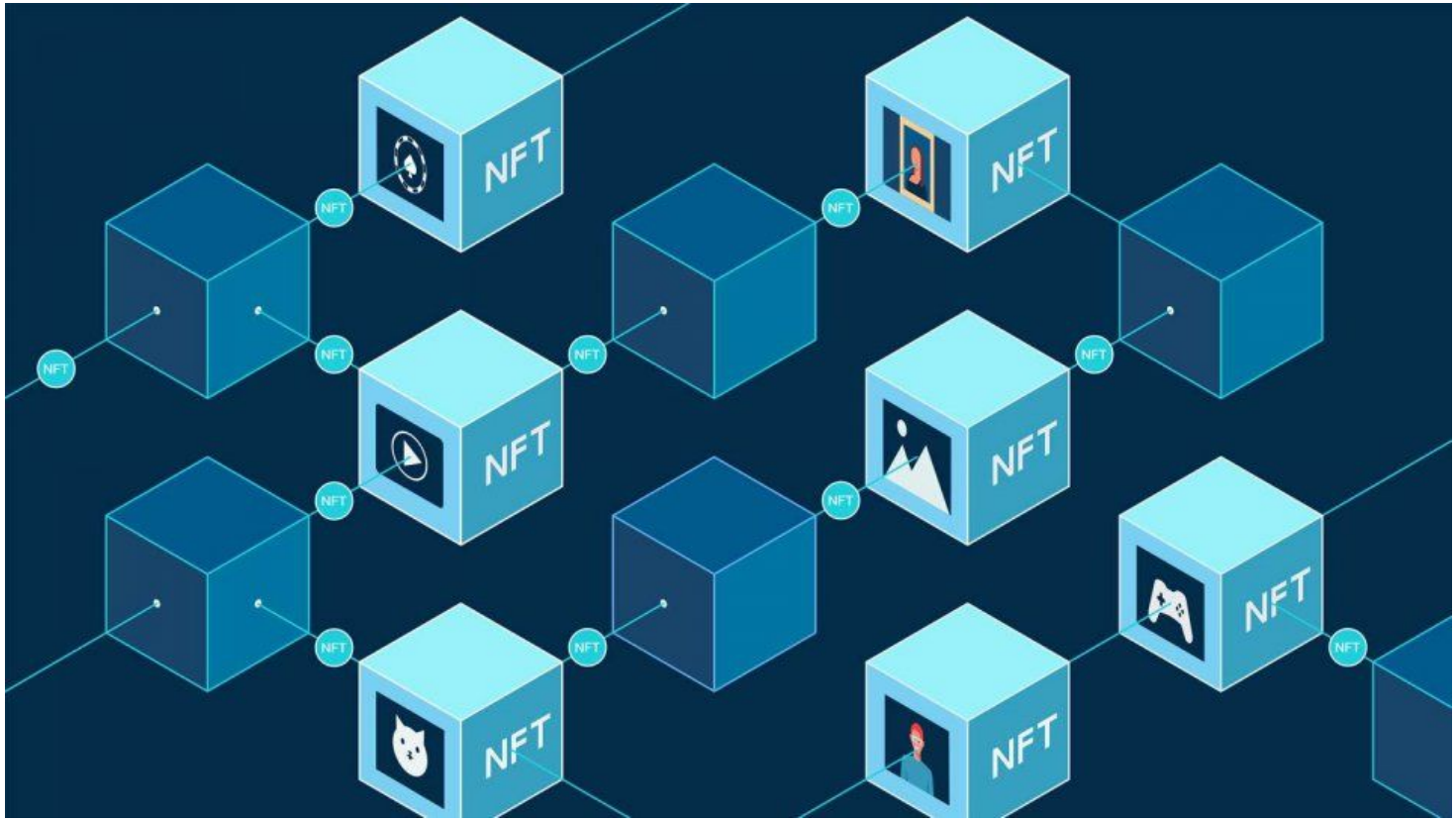


- Transforms input into a fixed-length hash value using a hashing algorithm
- Used to verify data integrity, create digital fingerprints, and securely store passwords
- Irreversible

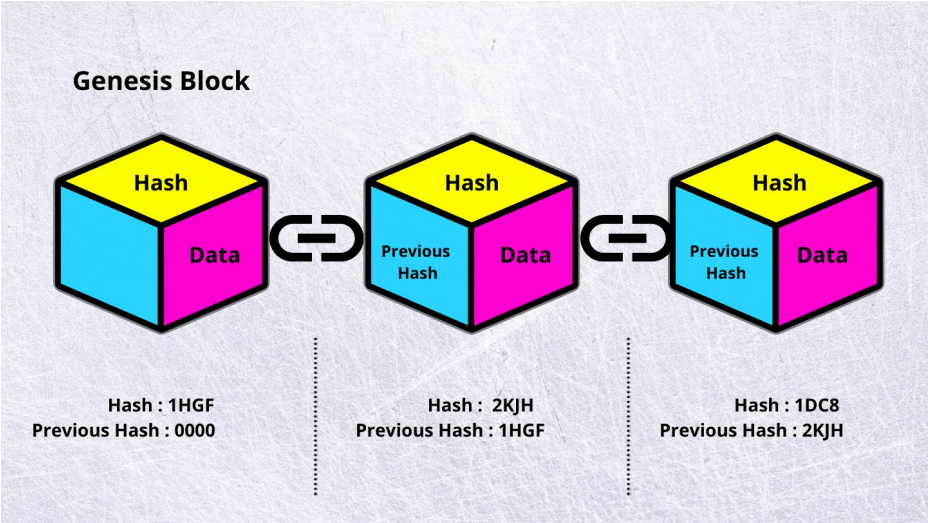
Salting

- Used in password hashing
- Random value (salt) is added to the password before hashing
- Each hash is unique even for identical passwords
- Prevents attackers from using rainbow tables

Blockchain & Public Ledgers

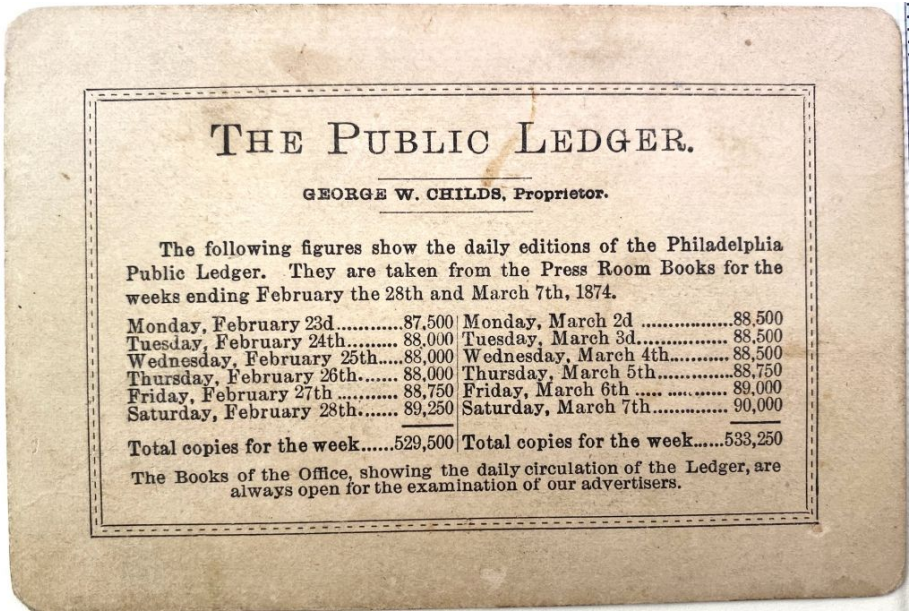


Blockchain



- Decentralized and distributed digital ledger
- Records transactions in such a way that they are impossible to be tampered with
- Each transaction block is linked to the previous one, forming a “chain of blocks”

Open Public Ledger



THE PUBLIC LEDGER.

GEORGE W. CHILDS, Proprietor.

The following figures show the daily editions of the Philadelphia Public Ledger. They are taken from the Press Room Books for the weeks ending February the 28th and March 7th, 1874.

Monday, February 23d	87,500	Monday, March 2d	88,500
Tuesday, February 24th	88,000	Tuesday, March 3d	88,500
Wednesday, February 25th	88,000	Wednesday, March 4th	88,500
Thursday, February 26th	88,000	Thursday, March 5th	88,750
Friday, February 27th	88,750	Friday, March 6th	89,000
Saturday, February 28th	89,250	Saturday, March 7th	90,000
Total copies for the week	529,500	Total copies for the week	533,250

The Books of the Office, showing the daily circulation of the Ledger, are always open for the examination of our advertisers.

- Transparent and publicly accessible record of transactions or data entries
- Maintained using blockchain
- Allows anyone to view and verify transactions

Certificates

X.509

Public Key Info

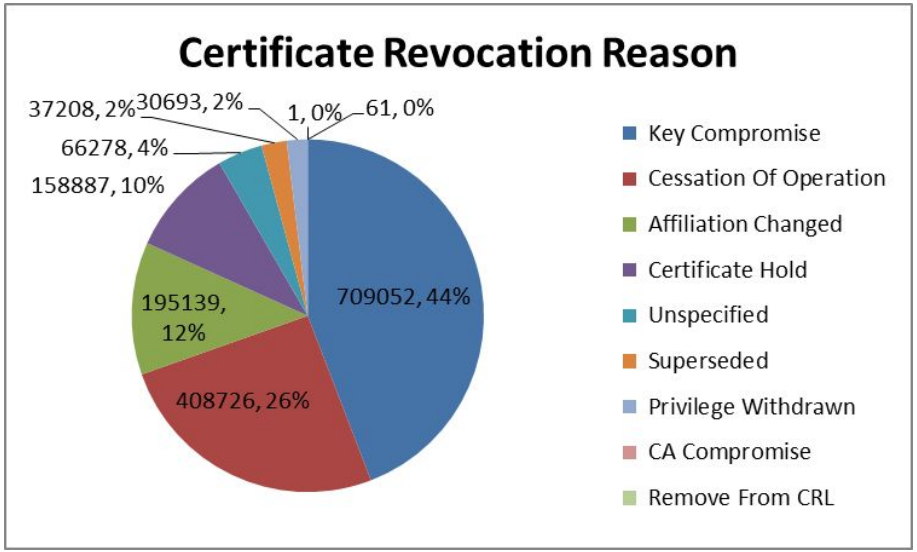
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	256 bytes : AD 0F EF C1 97 5A 9B D8 1E B0 44 8D C6 C9 A0 28 C3 0E 68 1B 94 91 2E 77 EC AC AE BE 6C 78 04 5B A4 78 04 CE FB 07 4B 5D 34 F3 57 E5 0F FB 6B A4 2A A5 53 D3 D5 7F 3A 3C 54 4C EB 73 7B 5E A1 0A D9 7E 5F A9 5A C0 71 71 43 9D 6F BD 4C CC CC 43 8C CF 77 4B 9D 1A 75 CB 1F BD F7 3B D3 66 C6 CE 7C B0 5A FC D4 14 24 3A 2A C5 A8 61 6D 04 4D A6 36 2D B0 FC C4 B0 BF FC 41 27 71 E4 C3 90 AD 37 07 67 BE 5A 1A 81 9D AB 8A 71 92 A3 85 1D 99 E7 20 19 CF C4 FD AD 9F 6E 98 9F 5B CE 17 A1 FE 7B 4A 4F C9 F2 AD 21 C8 F7 1B 5D 10 79 59 85 DF 7E B8 A8 FE 3A D7 2F E2 02 DF D8 67 67 F4 63 9F FA B3 E7 47 63 48 3A C1 98 73 3D 9A 8D 8D DA AC C8 DF 50 32 BC A1 21 A6 10 56 AE E6 C6 10 2A 4E 54 41 5D 38 C1 37 77 78 1E 43 F8 70 2A 4B 4D EA B7 F9 51 CC 1C 17 4F 2A 1B 67 1C 2E E0 E0 2D 7C 59
Exponent	65537
Key Size	2,048 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	512 bytes : 36 07 E7 3B B7 45 97 CA 4D 6C B0 2A 3F 3F 38 43 12 3D 1C 4C 8E F6 87 18 5C 66 54 C5 E2 5B 4B ED ED DC 4C 23 EC 93 21 A1 19 28 DD 78 6D A6 0D E7 F4 F5 64 2E 1B 49 22 B4 EE FE E7 D3 0B 34 85 6A 12 14 09 33 4F 4E 52 FD 6B B0 04 9A EF 62 3C E3 78 6C 08 7A 87 25 63 61 28 B2 2C 22 10 5E 51 0F 03 7B 53 41 48 74 47 7D 3C 06 C3 E6 56 4D 96 9C 09 62 B2 76 00 9F 1A 3C C8 08 67 05 A1 C1 55 48 C2 37 EA 32 69 6A 12 E2 53 26 DB AC AB 79 94 88 8B 5B 5A 72 76 04 76 0D 53 CC 3D A9 38 95 E6 C1 BE E0 A4 C8 7E F6 AC 7E FF 34 ED 3B 5D 38 46 67 1C C5 79 D4 A8 81 8E 9C D0 CA F7 75 64 4F DC F8 4A 38 7C 88 18 DC D1 9B 50 F1 DB E8 61 D4 7D AE D8 9E 6E 86 E9 73 4A D4 2A F1 C7 CA 69 19 89 56 B5 FC BE 8D 90 F4 5A 21 89 A4 9A B7 3B F5 BA 24 34 A0 FD 5E 59 80 7A 45 93 3B 56 89 62 E3 4E E3 7E EB 13 2B 28 24 B9 86 EC DA 93 49 A1 0F 14 EF 54 93 BE 1E F4 55 CF 17 20 C5 01 C5 84 62 D5 64 38 1D 1C 59 08 D1 31 F8 AE 05 A4 1B BA 0A 67 51 9E A8 15 F2 E8 CF 8E 9E D8 88 52 21 89 CC 4F 98 13 0A 41 40 71 69 79 B0 A5 6A BE 77 AB 5E A1 D4 89 66 6C 02 C2 D1 43 0D A2 CA D7 7A 71 01 8B F7 98 21 74 89 E8 8B 27 38 28 CD 3E EA A7 78 AD 2A 3A 63 DB 3A D0 05 6B 4F C9 20 4E 01 38 DF 05 75 49 F7 9F 2E DC 19 31 A9 96 D7 2F 2D 4E 84 7C FA 7E F6 67 5A A1 E7 5C A1 72 3B 22 DC A5 FA F2 E7 DC D6 A8 6D A0 4D FD 78 C5 5C DC 34 D9 86 76 5B 1C 0D BB B1 E5 DB 64 2A 55 7F 20 4D 5D 4D 44 01 1D 79 A3 2D EC F5 6B CD BE 7B 52 67 1D FF 05 42 FB 42 7A A1 BC 4C 23 DF AF 16 B9 76 C9 69 86 02 34 F2 A9 CB B8 15 39 BA A5 F1 E6 72 7C 1D 5E 0C 48 D7 99 1F 50 98 2B 75 2D 67 58 79 A1 1A 05 5A

- Standard format for a web server digital certificate
- Contains a serial number, version, signature algorithm, issuer, name of certification holder, public key, etc.

Certificate Authorities

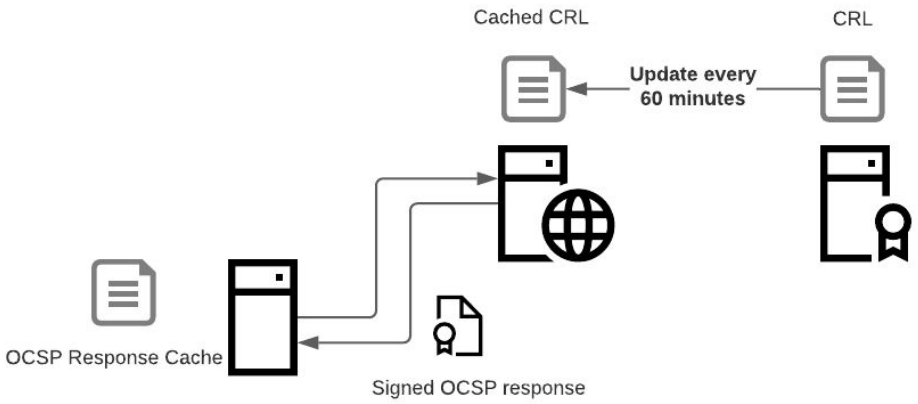
- Trusted entities
- Issue digital certificates
- Verify the identity of individuals, organizations, or devices.

Certificate Revocation Lists



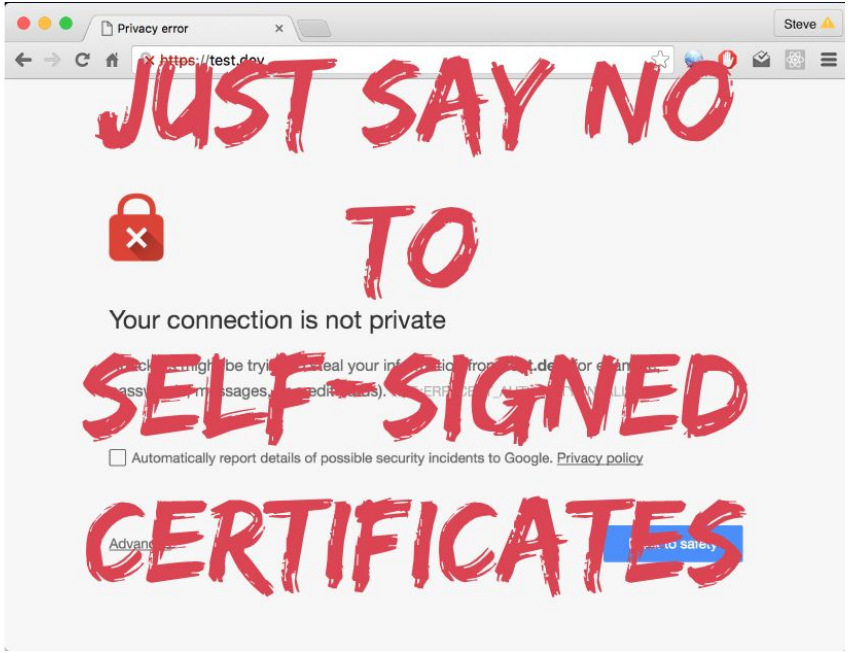
- Lists maintained by certificate authorities
- Contain information about revoked or invalid digital certificates
- Allow systems to check if a certificate has been compromised

Online Certificate Status Protocol



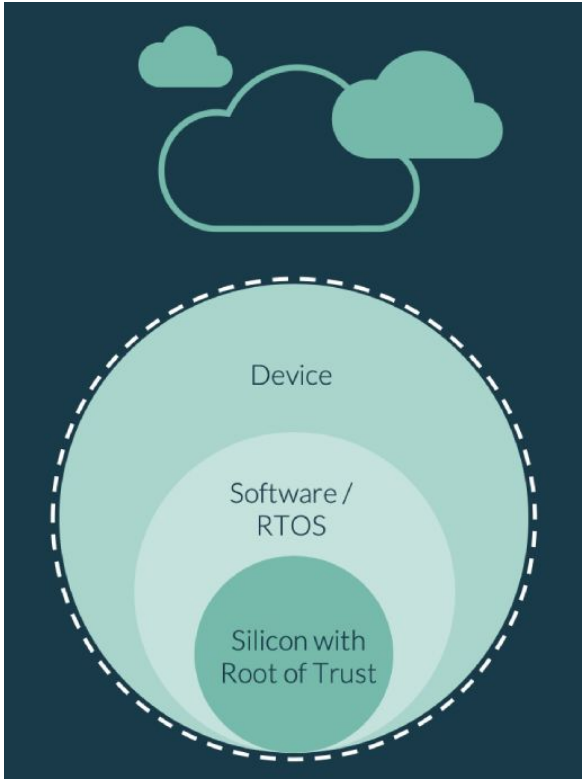
- OCSP is a protocol used to check the current status of digital certificates
- Having the CA verify every OCSP request leads to scalability issues
- OCSP stapling: certificate holder can verify their own status

Self-Signed vs. Third-Party



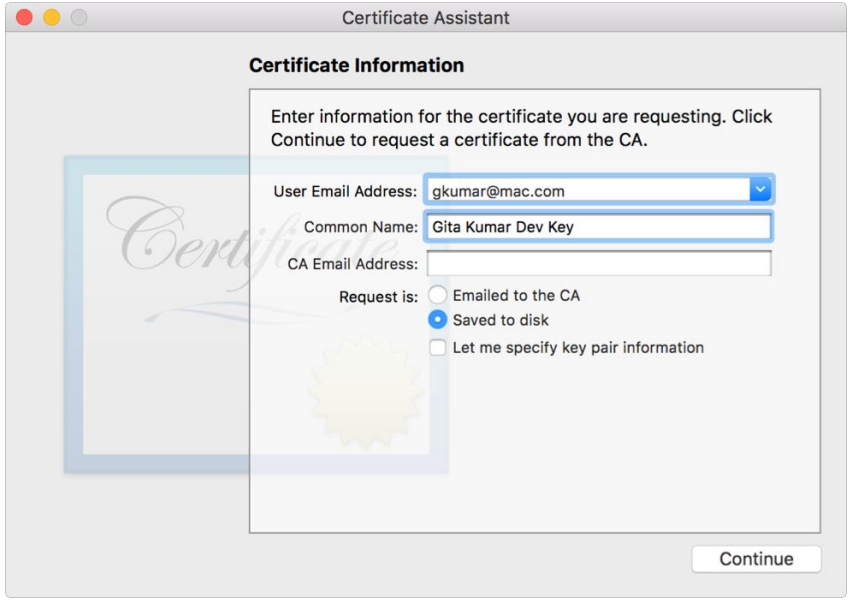
- Self-signed is where the entity generating the certificate also acts as the certificate authority, signing the certificate
- Third-party certificates are issued by trusted certificate authorities (CAs)

Root of Trust



- An entity or component in which our system bases its trust of other entities on
- Inherently trusted
  - CA
  - Secure Enclave
  - HSM
- Forms the basis for trust in other certificates and systems

Certificate Signing Request Generation



- Request generated by an entity to obtain a digital certificate from a CA
- Includes the public key and relevant information
- Requesting a wildcard certificate can secure multiple subdomains
- *.exam.com secures:
  - www.exam.com
  - mail.exam.com
  - ___.exam.com