Introduction to Cryptography - Part 1

Technical Article

Table of Contents

1.Introduction

In this article we discuss the several facets of cryptography and how it can be effectively used for maintaining privacy and integrity of data in computer storage and network systems. We cover the various primitives, principles, and services offered by crypto systems which operate with the main purpose of providing utmost security to data and prevent any kind of undesirable attacks from intruders and adversaries. We explore the different types of security attacks and understand how crypto systems are designed to circumvent such attacks. Finally, we dwell deep into the details of public key and private key systems to evaluate their key benefits, challenges and scenarios where these systems are deployed for safeguarding data and securing communication against any malicious attacks

With the rapid growth and advancements in IoT, Networking, Cloud and AI/ML technologies, future systems will encompass billions of interconnected devices which shall generate and share unprecedent amounts of data with local and central systems round the clock. With such deluge of data transactions occurring across the ecosystem, many of these systems are vulnerable to security breaches and form an attractive target for attackers. **Cryptography** is one of the most essential techniques implemented in modern systems to secure confidential and private data during rest or transit, authenticate devices and identity and provide protection against any kinds of tampering. Some of the fundamental services provided by Cryptography are as follows:

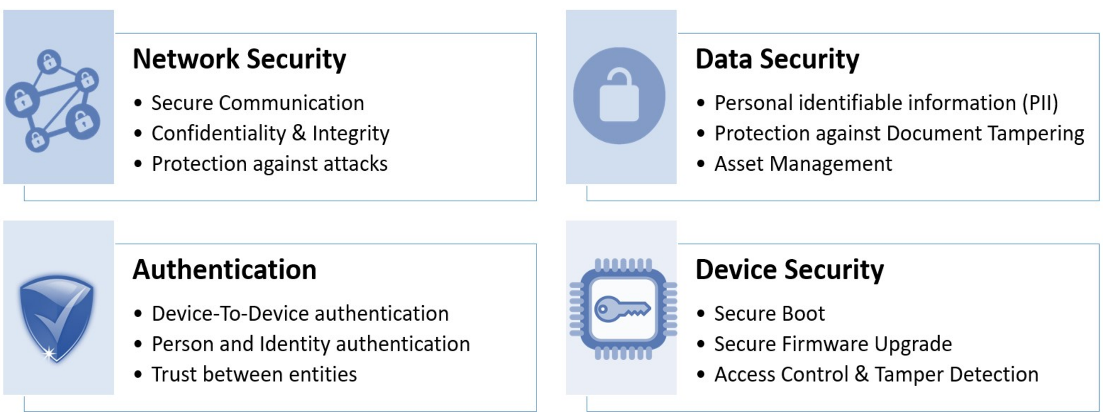


Figure 1: Cryptography Security Services

2.Cryptographic Features

The word ‘*cryptography*’ was coined by combining two Greek words, ‘*Krypto*’ meaning hidden and ‘*graphene*’ meaning writing. Over the many years the field of crypto has undergone a huge transformational evolution. Modern cryptography is based on various concepts of mathematics such as number theory, probability theory and quantum theory. The primary objective of cryptosystems is to provide one or more of the following capabilities in a system

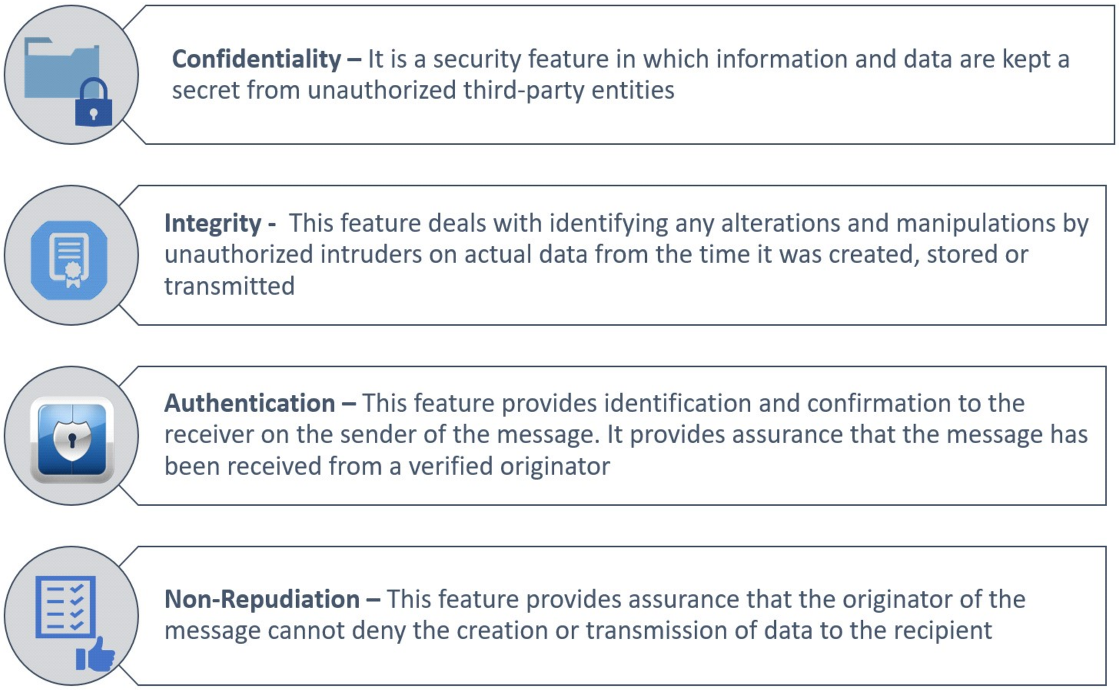


Figure 2: Fundamental features of Cryptography

2.1 Cryptographic Algorithms

The algorithms used in cryptographic systems encompass tools and techniques for providing one or more of the security services as mentioned above. The four major algorithms used in conventional systems are: -

- Encryption
- Hash functions
- Message Authentication codes (MAC)
- Digital Signatures

Below table shows the security features supported by each of these algorithms. In order to achieve the necessary security functionality, systems should incorporate one or more of these features in their design

	Confidentiality	Integrity	Authentication	Non-Repudiation
Encryption	✓	✗	✗	✗
Hash Function	✗	✓	✗	✗
MAC	✗	✓	✓	✗
Digital Signature	✗	✓	✓	✓

Table 1: Cryptography Algorithms and their Security Features

2.2 Cryptography Terminologies

Before we proceed with the details of cryptosystems, we need to be aware of some of the basic terminologies which are widely used in this context

Plaintext

It is the data which is easily readable and needs to be protected during storage or transmission

Ciphertext

It is the encoded or encrypted version of plaintext which is not readable in direct form. It is produced by using an encryption algorithm and a unique encryption key on the plaintext

Encryption Algorithm

It is a cryptographic algorithm which takes plaintext and an encryption key as input and outputs a ciphertext which is in unreadable format

Decryption Algorithm

It is a cryptographic algorithm which takes ciphertext and decryption key as input and outputs a plaintext which is in readable format

Encryption / Decryption Key

It is a unique value used as one of the inputs by cryptographic algorithm to transform plaintext data to ciphertext. The encryption key is known to the sender and the decryption key to the receiver

Alice & Bob

Two fictional characters commonly used as placeholders in discussions about cryptography and protocols

2.3 Cryptography Systems

Cryptosystems are broadly classified into two categories based on the relation between the encryption and decryption key used in the system

- Symmetric Key (Private Key) System
- Asymmetric Key (Public Key) System

3.Symmetric Key Systems

Cryptosystems in which the sender and receiver use the same secret key to encrypt and decrypt the information are known as Symmetric Key Systems. These systems require the private key to be shared safely and securely between the sender and receiver entities before exchange of information

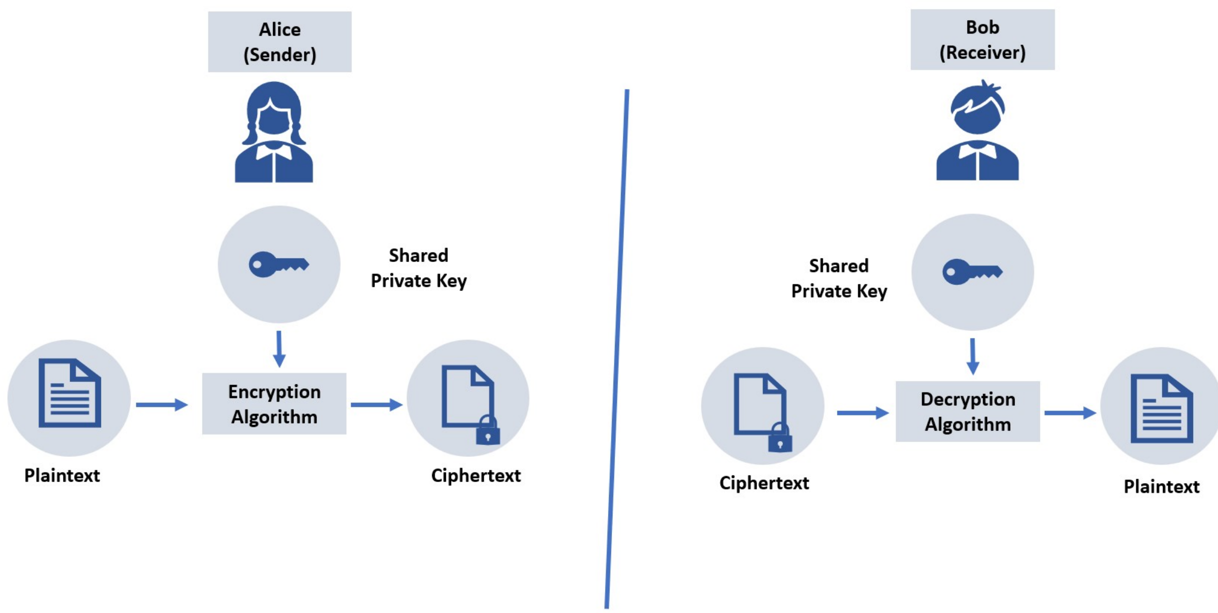


Figure 3: Symmetric Key Cryptography

3.1 Salient Features

- The systems involved should share the key using a secure distribution manner prior to the encryption and decryption process
- It is recommended to change the keys regularly to prevent any kind of attacks in the system
- Length of Key (number of bits) in this encryption is smaller and hence, process of encryption-decryption is faster than asymmetric key encryption.

3.2 Limitations

- Key generation and secure distribution among the communicating parties becomes challenging when the number of participating entities increase
- The encryption process provides data confidentiality services only and doesn't support integrity or authentication checks

3.3 Use Cases

- Protecting Data at Rest – Encrypting and storing data in computer storage devices like SSD, Flash Drives. On Linux OS dm-crypt is used for this purpose and in Windows OS Bitlocker etc

- Protecting Data in Transit – Encryption/Decryption techniques that are employed for data transmission and reception in remote systems communicating via Ethernet or Wi-Fi include IPSec (IP Security) protocol, TLS (Transport Layer Security) protocol and HTTPS protocol

Symmetric Key systems are often used in conjunction with Asymmetric Key systems to provide end-to-end security services. Some of the most widely used Symmetric Key Encryption Cryptography techniques are AES-256/192/128, DES, 3DES etc

4. Asymmetric Key Systems

Cryptosystems in which different keys are used for encryption and decryption of information are known as Asymmetric or Public key systems. In public key systems a keypair consisting of public and private keypair exists which are mathematically related to each other. The sender uses the public key of the receiver to encrypt the data and the receiver who has full-ownership of the private key uses the same to decrypt the data. These systems are also known as Public Key Encryption (**PKE**) systems

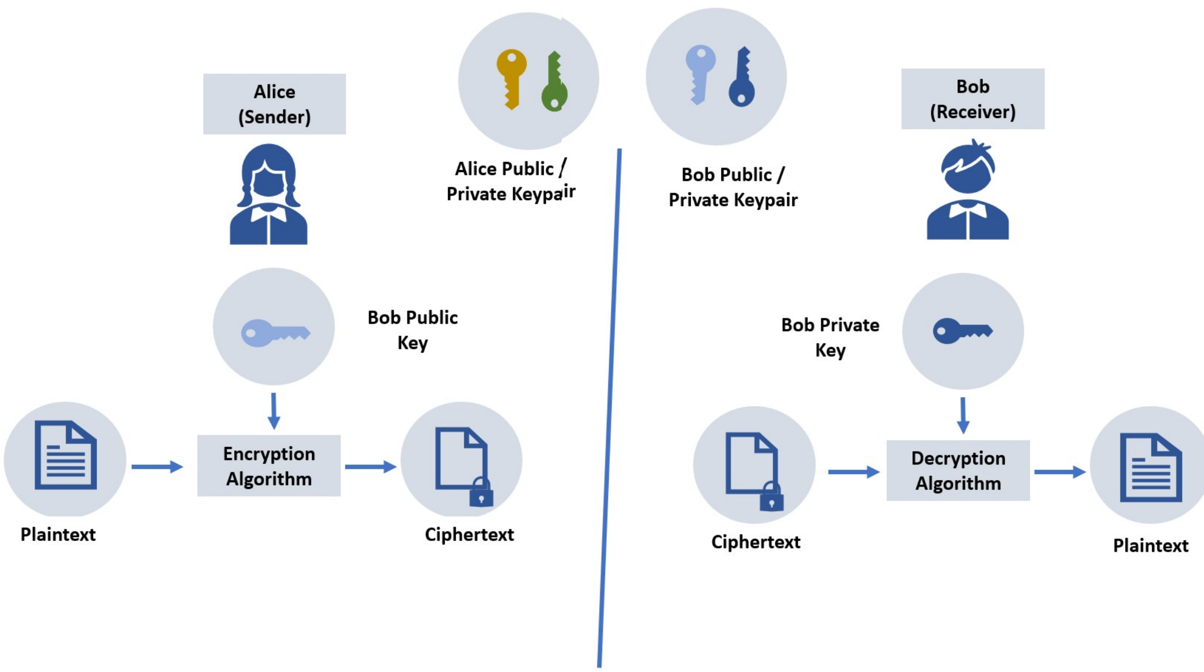


Figure 4: Public Key Cryptography for Encryption / Decryption Purpose

Another scenario where public key systems are deployed is to generate and verify digital signatures of message or identity for authentication purposes. In such systems the sender uses the private key part to sign a message and append a digital signature along with the message. The receiver uses the public key part to verify the digital signature from the message and confirm the integrity and authenticity of the received message

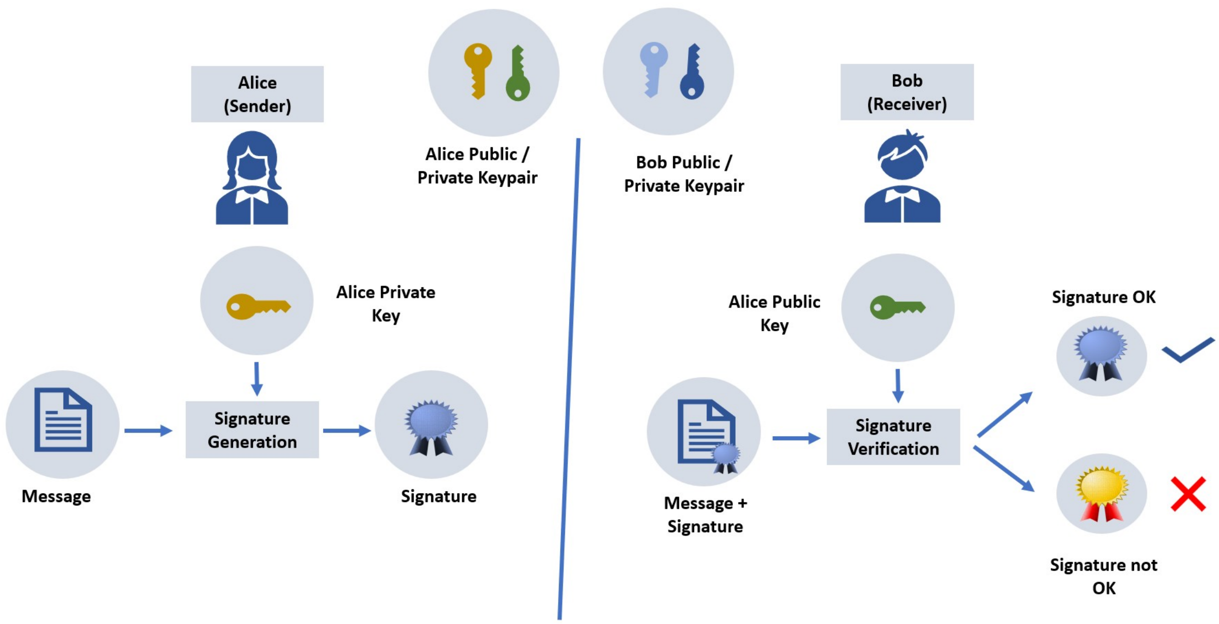


Figure 5: Public Key Cryptography for Digital Signature Verification Purpose

4.1 Salient Features

- Each user in a public key system contains a public/private key pair. While public key is distributed to all other users of the system, the private key is a well-guarded secret and known only to the owner of the keypair
- Though the public and private keys are dissimilar to each other they are related mathematically and thus form a unique pair such that information encrypted using one key can only be decrypted by its counterpart
- Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption

4.2 Limitations

- Public keys used in these systems are distributed among multiple users and hence need to be protected from malicious third-party spoofing attacks against tampering of the keys. This necessitates a provision for a trusted third-party authority which certifies all keys in the system
- PKC functions are computationally intensive when compared with symmetric functions, hence they are commonly used to process small amounts of data

4.3 Use Cases

- Encryption for Confidentiality – A sender uses the public key of the receiver to encrypt a message, which the receiver can decrypt using the private key from the keypair. Since the private key is known only to the receiver no other third-party will be able to decode the message

* Digital Signature for Message / Device Attestation – A message or a device attestation can be created by generating a digital signature. This is usually done by signing the hash of the message / unique identification block by the sender's private key. At the receiver side, the public key part is used to verify the signature and hence the authenticity of the sender
* Secure Boot – The boot image is signed by the manufacturer or OEM using a private key and the boot image along with the signature certificate is flashed onto the device. Upon power-on the BootROM verifies the integrity of the image by validating its signature using Root-Of-Trust (RoT) keys accessible only to the SoC. The device boots the image only if the signature is verified

Some of the most widely used Asymmetric Encryption Cryptography techniques are RSA (Rivest-Shamir-Adleman), ECC (Elliptical Curve Cryptography), ECDSA (Elliptical Curve Digital Signature Algorithm), ECDH (Elliptical Curve Diffie Hellman) etc

5.Cryptographic Attacks

A cryptographic attack is a way of disabling the security of the system by exploiting the loopholes in the system such that the attacker is able to break the code, cipher, protocol or key management scheme. Based on the type of attack it is broadly classified into two categories:

5.1 Passive Attack

The main objective of a passive attack is to get unauthorized access to information without altering the information or disrupting the communication channel. Two basic examples of passive attacks are interception and eavesdropping where an unidentified third-party intruder covertly accesses all information being shared without getting noticed by the sender or receiver

5.2 Active Attack

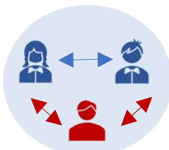
The main objective of an active attack is to alter and modify the information being shared or disrupt the communication channel such that the original participants are denied of access to information or quality service. In these types of attacks, the attacker attempts to alter the system resources or affect the operations by performing one or more of the below actions:

* Modifying the information in an unauthorized manner
* Initiating unintended transmission of information
* Alteration of authentication data such as originator name or timestamp
* Unauthorized deletion of data
* Denial of access to information for legitimate users

Based on the component of the system under attack we can further classify security attacks as follows

Denial-of-Service (DoS)

In this type of attack a component is flooded with enormous amount of information such that the system is overloaded thereby preventing processing of information from legitimate users



Man-In-Middle (MIM)

In this type of attack, the attacker sits between the sender and receiver spoofing the identity and intercepting and replaying the packets that are transmitted in the communication channel

Repudiation / Impersonation Attacks

The attacker conceals the real identity and impersonates as a legitimate user gaining unauthorized access to system resources and information

Malware and Tampering Attacks

False information or images are sent to components which introduce malware in the system and tampers with data and functionality

Cryptosystems adhering to the principles of confidentiality, integrity, authentication and non-repudiation, by using the right combination of symmetric and asymmetric cryptography are well-equipped to counter and defeat such malicious attacks

6. Public Key Infrastructure

In Public Key Cryptography (PKC) systems each user is associated with a keypair consisting of a private key and a public key. While the private key is a fully confidential and secret key known only to the user, the public key which establishes the identity of the user is available in the public domain and accessible to all participating entities in the system. Since public keys are in open domain, they are likely to be misused. The role of a **Public Key Infrastructure** (PKI) is to establish and maintain some kind of trusted infrastructure to manage these keys

A PKI defines the binding between the public keys and an entity or organization. It consists of a third-party trusted body that can attest and certify the identity of the participating entities and assure a safe distribution of public keys in the public repository of the system. A PKI comprises of various components which includes:

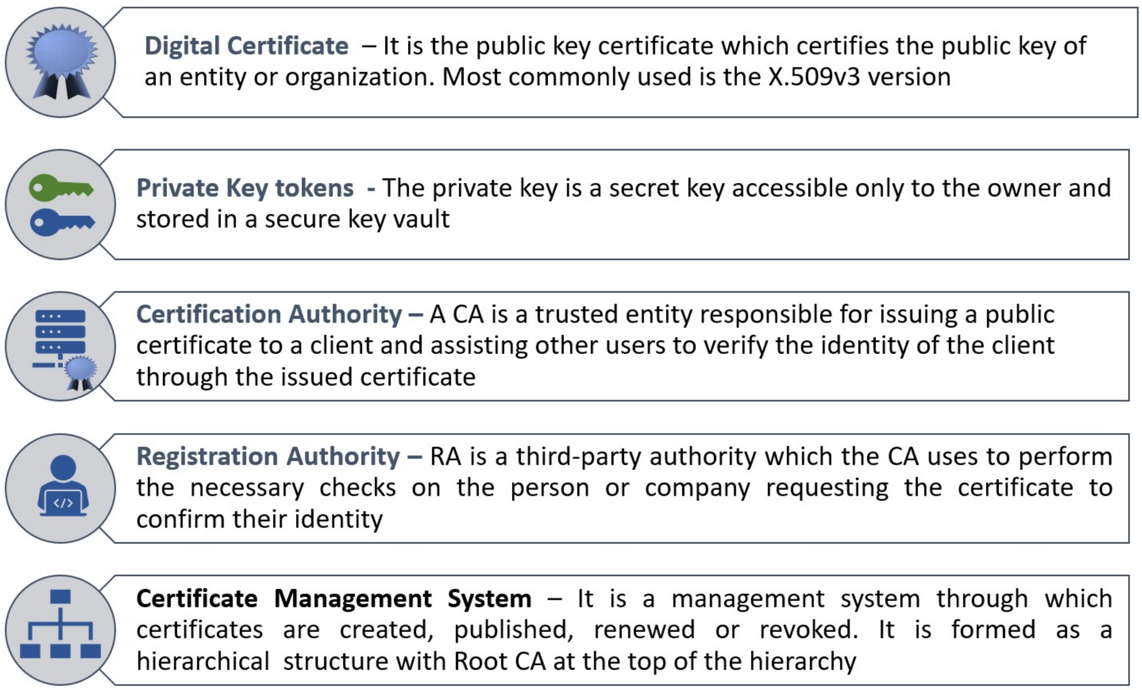


Figure 6: Components of Public Key Infrastructure

A typical workflow for a client to obtain a Digital certificate from an issuing CA is as illustrated below:

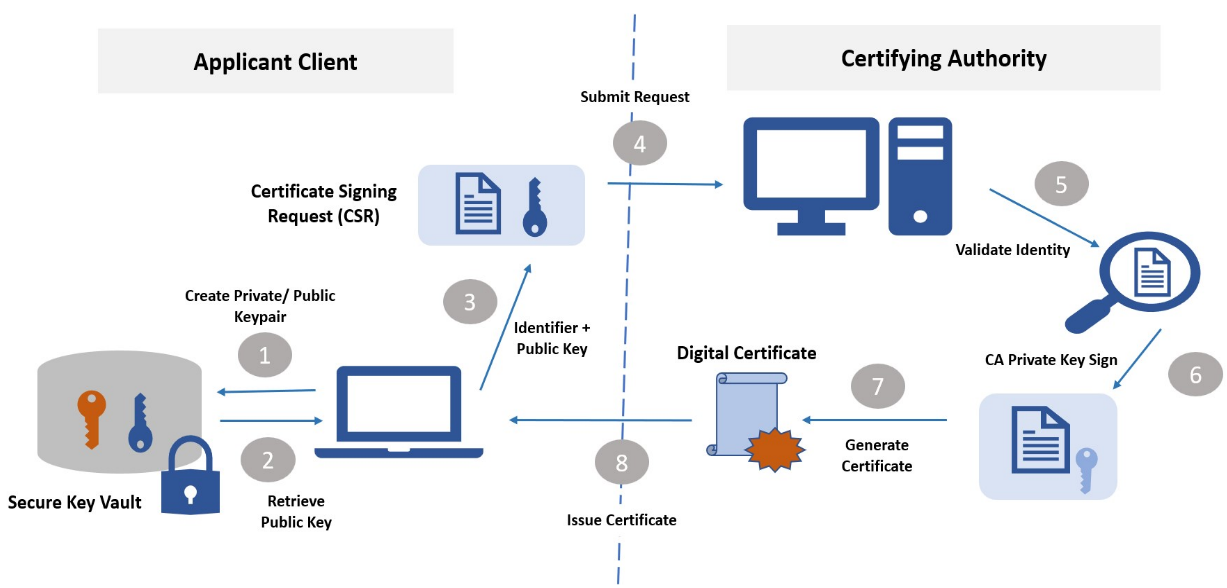


Figure 8: Digital Certificate Issue by Certificate Authority

A PKI is basically a combination of hardware and software components with a set of well-defined guidelines and policies based on which CAs can generate, publish, distribute, renew and revoke certificates from field. A standard X.509v3 certificate when issued by a CA comprises of start date, end-date, signature, revocation flag etc such that the user can check the validity of these certificates before accepting any transactions from the entity

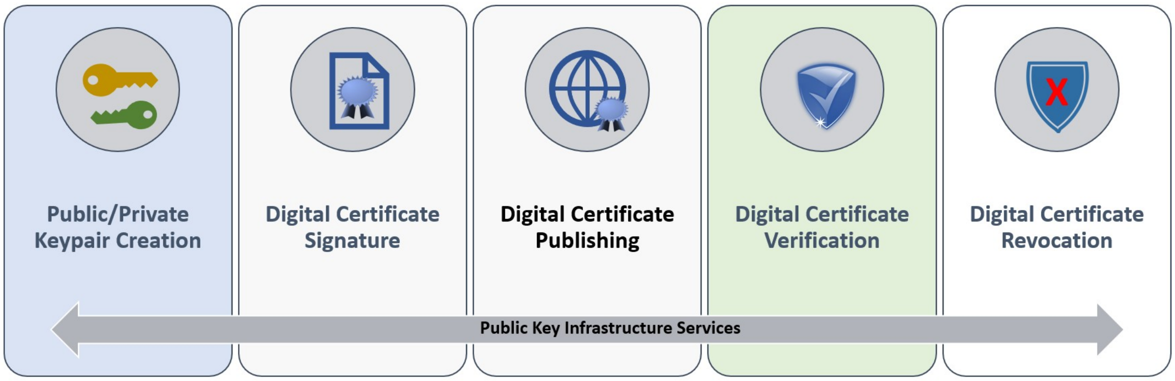


Figure 9: Services of Public Key Infrastructure

7. Conclusion

With the evolution of robust, computationally intensive and high-performance systems, modern cryptography is rapidly adopting sophisticated mathematical equations, algorithms and secret keys in its design which are extremely complex to break, hack or compromise. Security has become an integral part of modern-day systems and it can no longer be considered as an add-on feature. System security architects must envision the use cases of the system and conduct a risk and threat analysis. From this analysis, the required security features must be identified and combined in the design

In the **next part of this article**, we will explore the Hardware support available in modern day System-On-Chips to cater to various security functions as described in this article. We will majorly focus on the security infrastructure provided by ARM architectures and how these features can be leveraged in our software and product design for achieving a robust and **secure system design**

8. References

1. Essentials of Edge Computing eBook - Robert Oshana, Editor-in-Chief NXP
2. https://www.nist.gov/publications/advanced-encryption-standard-aes
3. https://www.tutorialspoint.com/cryptography/index.htm