SUBMITTED BY

ANISH FAUZDAR

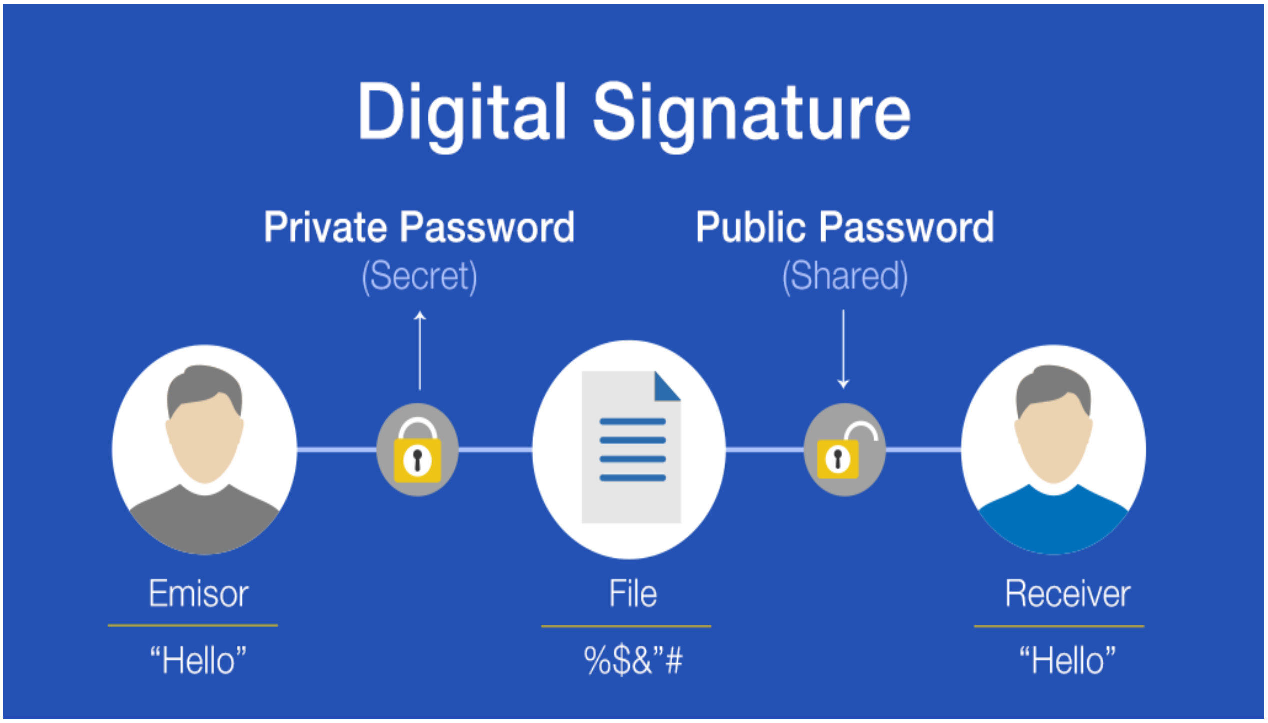
SUBMITTED TO

KRITISH DHUNGEL

DIGITAL SIGNATURE

Introduction:

Whitfield Diffie and Martin Hellman introduced the idea of a digital signature scheme in 1976, albeit they only hypothesized that such systems existed based on trapdoor one-way permutation-based functions. The RSA algorithm was developed shortly after by Ronald Rivest, Adi Shamir, and Len Adleman. It could be used to create simple digital signatures, but only as a proof-of-concept because "plain" RSA signatures are not safe. The RSA method was employed in Lotus Notes 1.0, the first widely advertised software program to provide digital signatures, which was introduced in 1989. Digital signatures are like the electronic fingerprints. They use a standard protocol called Public Key Infrastructure(PKI). PKI requires a provider to use a mathematical algorithm to generate two long numbers which are basically called keys. One key is public and on key is private. Digital signatures can provide the evidences of the origin and the status of the electronic documents, transactions or the digital messages. In other words, It is a cryptographic value which is calculated from the inserted or given data and a secret key known only by the signer to legally access it. As we know that, Digital signatures are based on the concept of the public key and the private key. It is also known as Asymmetric cryptography. Digital signatures work through the public key cryptography which has two mutually authenticating cryptographic keys.



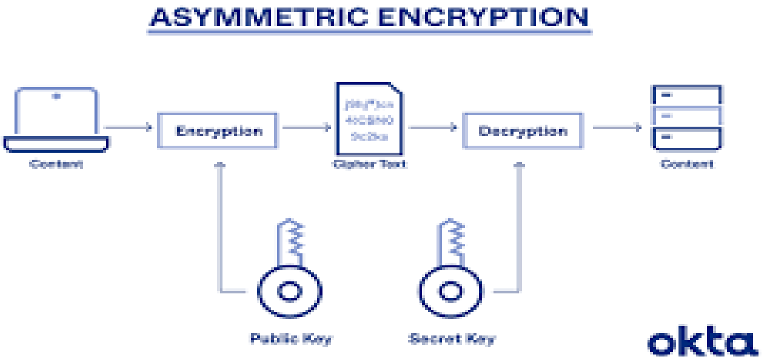
The individual who creates the digital signature uses a private key and that authentic individual is the only one who can decrypt the data by the use of his public key. In a case if the user or the individual is unable to decrypt or open the document using his/her public key then that's a sign that there is something problem with the document or the signature. And this is how the digital signatures are authenticated. The private key must be secret within the authentic individual or if someone else has access to the private signing key then, that individual could create a duplicate or fraud digital signatures in the name of the private key holder.

Benefits:

The main benefit of the digital signature is privacy, security and authenticity. It ensures that the document is genuine and the integrity of the document is maintained. The security features and methods used in the digital signatures includes the following things:-

Security Features:

- Personal identification numbers(PINs):
  In this method of security, the password and codes are used to identify the owner's identity and the signature is approved. Username and password, Email are the most common methods used in the authentication.
- Asymmetric cryptography:
  It is also known as the public key cryptography. It is a process that uses a pair of related keys in which one is private and other is the public key for the authentication.



- Cyclic redundancy check(CRC):
  It is an error-detection and the verification feature that is used in digital networks to detect the changes to raw data. It is given as a kbit message and the transmitter creates an(n-k) bit sequence called frame check.
- Certificate Authority(CA) validation:
  CAs issue digital signatures and act as the third parties by accepting, authenticating, issuing and maintaining digital certificates. The use of CAs helps to prevent the creation of the unauthorized fake digital documents or certificates.
- Trust service provider(TSP):

A trust service provider is a legal person or an entity that validates the digital signatures on the behalf of the company and offer's the validation of the digital signatures.

- Time savings:
  While signing physically it may take a lot of time to do so but with the use of the digital signature the documents can be signed at once and which saves alot of time and also helps from forgetting our signatures
- Cost savings
  As digital signature is done digitally, so no paper or pen is required to do the signature which makes the company spend way less money in buying the paper and pens.
- Positive impact on the environment:
  As it is a digital method the and no paper usage is required which reduces the physical waste generated by the waste papers which creates a positive impact on the environment and helps in keeping the environment clean.
- Traceabilty: (Lutkevich, 2022)
  Digital signature creates an audit trial that makes internal record- keeping easier for the business. With being everything recorded and stored for the digitally, there are fewer opportunities for a manual signee or a record-keeper to make a mistake or misplace or something.

Creation of Digital signature:

A digital signature is base on a hash value of the data. To create it signing a software such as email program is used to provide a one way hash of the electronic data to be signed. A hash has a fixed-length string of letters and numbers generated by an algorithm. The private key which is owned by the creator of the digital signature is used to encrypt the hash. The value of the hash is unique to the hashed data. Any change in the data, even a change in the single character will result in the different value of the hash.

Classes and types of digital signatures:

There are three different classes of the digital signatures. They are as follows:-

- Class 1:
  It cannot be used for the legal business documents as they are validated based only on an email ID and username. Class 1 signatures provide a basic level of security and are used in the environments with low risk of the data compromise. It carries the name and email id of the DSC holder.
- Class 2:
  It is often used for electronic filing of tax documents, including income tax returns and goods services tax (GST) returns. Class 2 digital signature authenticate a signer's identity against a a pre-verifies database. It is used in the environments where the risks and the consequences of the data compromise is moderate.
- Class 3:
  The highest level of the digital signatures, require a person or organization to present in front of a certifying authority to prove their identity before signing. Class 3 digital signatures are used for e-auctions, e-tendering, e-ticketing, court filings and in the other environments where threats to the data or the consequences of a security failure are high or there is a security breach.

References:

Lutkevich, B., 2022. *What is a Digital Signature?*. [online] SearchSecurity. Available at: <https://www.techtarget.com/searchsecurity/definition/digital-signature> [Accessed 19 October 2022].

Okta UK | The Identity Standard (2022) *Okta.com*. Available at: https://www.okta.com/ (Accessed: 2022).