Public vs. private keys

In a rapidly evolving world of technology, it is more critical than ever to establish security policies throughout an organization that safeguard valuable information and data assets. Asymmetric cryptography relies on public and private keys as its core building blocks to maintain data security and confidentiality in the face of dangers. However, to enable organizations to make wise decisions that will protect online interactions and information, it is important that we understand when public and private keys are used and how to do so effectively.

What is a public key?

A public key is frequently employed to establish secure communication through data encryption or to validate the authenticity of a digital signature. Safety is ensured because the public key comes from a trusted certificate authority, which gives digital certificates verifying the owner's identity and key. Public keys are created through an asymmetric algorithm that conducts several operations on a pair of connected keys before being transmitted over the internet.

What is a private key?

A private key is a secret and secure key that must be kept confidential and protected. Its role involves decryption and the creation of digital signatures, assuring the data's integrity and authenticity. It is the counterpart of the public key and is shared to decrypt encoded information. Any data encrypted using the private key can be decrypted using the corresponding public key.

How do public and private keys work together?

Public and private keys work together to ensure secure communication, data encryption, digital signatures, and key exchanges take place safely across various communication channels. This process encompasses:

1. Key generation: A public and private key is generated for both the sender and receiver.
2. Key exchange: The public keys are exchanged between sender and receiver.
3. Encryption: The sender encrypts their data using the recipient's public key.
4. Transmitting encrypted data: The encrypted data is transmitted to the recipient.
5. Decryption: The recipient decrypts the message using their exclusive private key.

Key takeaway

In summary, although public and private keys are distinct, they work together to create a powerful and flexible foundation for achieving data security, confidentiality, integrity, and authentication in a wide range of digital settings.

Go to next item ✓ Completed

Like Dislike Report an issue