Public Key

Return to Glossary

In cryptography, a **Public Key** is a large numerical value that is used to encrypt data. The key can be generated by a software program, but more often, it is provided by a trusted, designated authority and made available to everyone through a publicly accessible repository or directory.

A **Public Key** is also used to encrypt a message or check the legitimacy of a digital signature. It is accompanied by a corresponding private key, which is known only to its owner. Private keys are used to decrypt messages that were created with the corresponding **Public Key** or to create signatures. In other words, a **Public Key** locks up data from unauthorized use, while a private key is used to unlock it.

Public Keys are available from a certificate authority, which issues digital certificates that prove the owner's identity and contain the owner's **Public Key**. **Public Keys** are created using an asymmetric algorithm, which pairs the **Public Key** with an associated private key. The most common algorithms used to generate **Public Key** are Rivest-Shamir-Adleman, elliptic curve cryptography, and Digital Signature Algorithm.

A **Public Key** can be given to any person with whom an individual wants to communicate, whereas a private key belongs to the individual it was created for and isn't shared. The **Public Key** is typically stored on a Public Key Infrastructure (PKI) server and is used to encrypt data securely before it is sent over the internet.

Source: https://searchsecurity.techtarget.com/definition/public-key