Public Key

Return to Glossary

Definition 1

A **Public Key**[1]. is a cryptographic key used with a public -key cryptographic algorithm that is uniquely associated with an entity and that may be made public. In an asymmetric-key (**Public Key**) cryptosystem, the **Public Key** has a corresponding private key. The *Public Key **may be known by anyone and, depending on the algorithm, may be used, for example: - Verify a digital signature that was generated using the corresponding private key, - Encrypt keys that can be decrypted using the corresponding private key, or - Compute a shared secret during a key-agreement transaction. ==== Definition 2 ==== 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 ~~DISCUSSION:on|Outstanding Issues~~ ~~DISCUSSION:off~~**

1)

Elaine Barker, NIST, Recommendation for Key Management: Part 1 - General, NIST Special Publication 800-57 Part 1, Revision 5, May 2020, Accessed 18 January 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf