Contact U

Products SSL Partners Company Resources Support

What is Public-key Cryptography?

What is public-key cryptography?

A look at the encryption algorithm and its security benefits

Public-key cryptography, or asymmetric cryptography, is an encryption scheme that uses two mathematically related, but not identical, keys - a public key and a private key. Unlike symmetric key algorithms that rely on one key to both encrypt and decrypt, each key performs a unique function. The public key is used to encrypt and the private key is used to decrypt.

It is computationally infeasible to compute the private key based on the public key. Because of this, public keys can be freely shared, allowing users an easy and convenient method for encrypting content and verifying digital signatures, and private keys can be kept secret, ensuring only the owners of the private keys can decrypt content and create digital signatures.

Since public keys need to be shared but are too big to be easily remembered, they are stored on digital certificates for secure transport and sharing. Since private keys are not shared, they are simply stored in the software or operating system you use, or on hardware (e.g., USB token, hardware security module) containing drivers that allow it to be used with your software or operating system.

Digital certificates are issued by entities known as Certificate Authorities (CAs). For more information on CAs, please see our related article - What are Certificate Authorities?.

Business Applications

The main business applications for public-key cryptography are:

Digital signatures - content is digitally signed with an individual's private key and is verified by the individual's public key

Encryption - content is encrypted using an individual's public key and can only be decrypted with the individual's private key

Security Benefits of Digital Signatures

Assuming the private key has remained secret and the individual it was issued to is the only person with access to it, digitally signing documents and emails offers the following benefits.

Authentication – since the individual's unique private key was used to apply the signature, recipients can be confident that the individual was the one to actually apply the signature

Non-repudiation – since the individual is the only one with access to the private key used to apply the signature, he/she cannot later claim that it wasn't him/her who applied the signature

Integrity - when the signature is verified, it checks that the contents of the document or message match what was in there when the signature was applied. Even the slightest change to the original document would cause this check to fail.

Security Benefits of Encryption

Assuming the individual's private key has not been compromised, encrypting data and messages offers the following security benefits.

Confidentiality - because the content is encrypted with an individual's public key, it can only be decrypted with the individual's private key, ensuring only the intended recipient can decrypt and view the contents

Integrity - part of the decryption process involves verifying that the contents of the original encrypted message and the new decrypted match, so even the slightest change to the original content would cause the decryption process to fail

ABOUT GLOBALSIGN
Company Profile
Blog
News & Events
Privacy Policy
Cookie Policy / DNT
Legal Repository

TOOLS
SSL Server Test
SSL Inventory Tool

LEARNING
Support Site
SSL Information Center
Resources
Customer Stories

CONTACT
1-877-775-4562
sales-us@globalsign.
Live Chat
Open Support Ticket
System Alerts

GlobalSign is the leading provider of trusted identity and security soluti
businesses, large enterprises, cloud service providers and IoT innovato
world to secure online communications, manage millions of verified dig
and automate authentication and encryption. Its high-scale Public Key
(PKI) and identity solutions support the billions of services, devices, pe
things comprising the Internet of Everything (IoE).

© 2018 GlobalSign. All Rights Reserved.

沪ICP备08025378号