Configuring RSA Keypairs In IOS

Keith Bogart

CCIE #4923

- kbogart@ine.com
- @keithbogart1
- linkedin.com/in/keith-bogart-2a75042

CCIE Routing & Switching

Topic Overview

- What Are RSA Keys
- Generating RSA Keypairs In IOS
- Validating & Erasing Keypairs In IOS

RSA Keypairs

- RSA = Rivest, Shamir and Adleman
  - Original creators of the RSA Asymmetric Encryption Algorithm
- Utilizes a pair of keys
  - Both keys are mathematically related to each other.
  - Information encrypted with one key can only be decrypted with the other key.
- Public Key
  - Typically made publicly available, or shared via email or other methods
  - Peers will encrypt information they want to send to you with your Public Key
- Private Key
  - Kept on your local machine and kept very secret
  - Information you send to your peers will be encrypted with your Private Key
  - Peers will decrypt with your Public Key

RSA Keypairs

- Digital Certificates require creation of a Public/Private RSA Keypair.
  - The keypair must be generated prior to submitting a CSR to a CA.
  - The Public Key will be sent within the CSR.
- On Cisco IOS devices, RSA Keypairs can be created as either:
  - General-Keys
  - Usage-Keys
- Selecting either of the above will work for usage with Digital Certificates.

CSR = Certificate Signing Request
CA = Certificate Authority
-
More details on the differences between “general-keys” and “usage-keys” coming up.

Generating RSA Keypairs

- Below is the minimum configuration you'll need to create an RSA Keypair on your router/switch;
  - Router(config)#hostname Payroll1
  - Payroll1(config)#ip domain-name <name>
  - Payroll1(config)#crypto key generate rsa
- Using the above commands, the name of the RSA Keypair will be:
  - <device hostname>.<domain-name>
- You will be prompted to select a key size;
  - The larger the keysize, the more secure it is.
  - The larger the keysize, the longer it will take the CPU to generate it…and encrypt/decrypt packets with it.

When using the command, "crypto key generate rsa" (and ONLY using those keywords) the minimum prerequisites are a domain-name, and a non-default hostname on the Router.

-

Using the command "crypto key generate rsa" will result in the creation of "General Keys". This means that the same exact keypair will be used whether implementing Digital Certificates…or utilize RSA Encrypted Nonces (Diffie Helman) for authentication between peers.

-

Some argue that creating "Usage-Keys" is safer. This option creates two PAIRS of keys…one pair used only for signing (Digital Certificates) and the other pair used only for RSA Encrypted Nonces. This limits the exposure of either keypair.

Generating RSA Keypairs

- The "crypto key generate" command has additional options:
- Crypto key generate (A) _____ (B) _____

(A)
- ***General-keys***
- ***Usage-keys***

(B)
- ***Exportable*** – when selected, no other options will follow.
- ***Label*** – Allows you to assign a descriptive name to the keypair and removes the need for the "ip domain-name" command.
- ***Modulus*** – Allows you to set the key size.

See previous note on the differences between "General-Keys" and "Usage-Keys". Usage-keys are really only relevant when you are utilizing features (like crypto isakmp policies) that allow you to select multiple authentication methods.

-

More on this topic:
https://learningnetwork.cisco.com/thread/14376

-

Exportable: Only choose this option if you will need to have two-or-more routers sharing the same public/private keypair. This is used in redundancy situations when one router is backing up the other. Using this keyword allows one to export the keypair to a .pem file (Privacy Enhanced Mail) which they can then import onto other routers. However be aware that this exposes your Private Key by having it on more than one device.

Confirming Your Keypair

- To view your keypair;
  - Router#***show crypto key mypubkey rsa***
- To delete all RSA Keypairs:
  - Router#***crypto key zeroize rsa***

If, when the keypair was created, you did not specify “exportable” then there is no way to view (or export to another device) the Private Key.