DATASHEET

Sectigo Certificate Management for SSH Authentication

IT sys admins are often tasked with management of large numbers of servers and must authenticate securely with each one in compliance with the latest security best practices.

A typical enterprise may need to work with multiple certificate authorities. This may be for business reasons, or to ensure resilience, or it may be for historical or organizational reasons. Whatever the case, the flexibility to issue, manage, and renew certificates from a variety of public CAs is a common ask from Sectigo customers.

As a leading Certificate Lifecycle Management platform Sectigo Certificate Manager is designed to issue, discover, manage and control certificates to support a variety of use cases and capabilities across the enterprise. Sectigo is dedicated to ensuring openness and interoperability to help customers consolidate platforms, reduce costs and maximise resources.

While Sectigo provides a wide range of certificate options, there are several reasons why customers may choose to continue to purchase certificates from another vendor such as DigiCert or Entrust. SCM now includes the capability of issuing certificates from third party public CAs including Entrust and DigiCert. This means that IT departments can have a single full featured platform providing Certificate Lifecycle Management across multiple vendors. Enterprises can continue to employ certificates from other vendors or can transition to Sectigo certificates if and when they choose.

Other CLM vendors support multiple Certificate Authorities, but only Sectigo provides the complete solution of a top tier multi-vendor CLM solution combined with a leading Certificate Authority and a rich set of available certificate types.

By leveraging Sectigo's extensive experience in certificate management and certificate issuance, and by implementing a more robust SSH authentication strategy, enterprises will see greater efficiencies in IT administration, reduced risk of security breaches and more control of critical resources.

SECTIGO®

Advantages of Certificates Over Key-Based Approach:

Controlled Validity

SSH certificates can be set to expire when they are no longer required. They can also be revoked, unlike SSH keys, in case the access needs to be ended before the expiration date.

Single Platform Management

SSH certificates are easier to manage from end-to-end, from issuance to revocation. The certificate rollout is simpler than a key rollout, especially using the Sectigo Certificate Manager platform.

Reduced Labor Costs

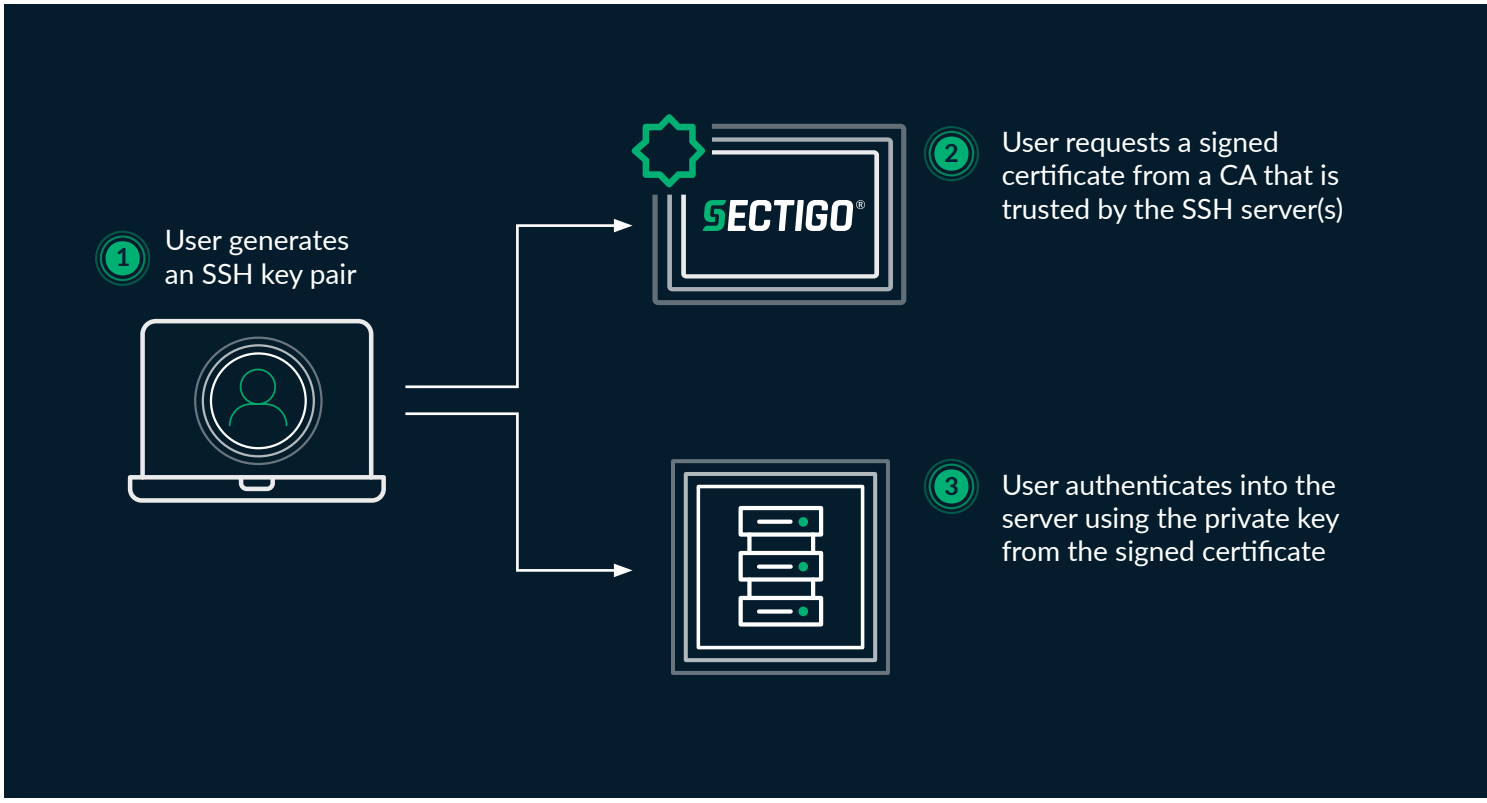
The cost of managing many keys across multiple servers is prohibitive. Certificates ensure a cost effective, scalable approach.

SSH Authentication Certificates

As a leading provider of certificates enabling a range of security and encryption solutions, Sectigo brings a wealth of experience in issuing and managing certificates to enable solution deployment at scale. Sectigo Certificate Management for SSH Authentication is a new module within the SCM platform that reduces the complexity of SSH certificate management for large and small enterprises.

It provides the following capabilities:

- Private certificate authority (CA)
- Cloud-hosted Hardware Security Module (HSM) for storing keys
- A command line tool used to generate user and host SSH certificates
- Convenient service subscription management



Users download a CLI tool from Sectigo which they run to generate the SSH key pair and client-side certificate. The CLI also validates the legitimacy of the user making the request. Because the certificate is trusted by the server via the Private CA, the user can authenticate to the server with the private key and the signed certificate. When the certificate expires or is revoked, that trust no longer exists and the authentication is refused.

Sectigo Certificate Management for SSH Authentication provides the following benefits:

Visibility: View all authorized users and assigned principals in a single dashboard.

Trust: SCM enables implementation of a single chain of trust via the certificate authority. If a valid certificate is signed from that authority, it is legitimate.

Lower maintenance: SSH certificates are easier to maintain and manage.

Control: Defined and documented processes for revocation of certificates to enable response to threats.

Powerful tools: By providing tools to facilitate the distribution of certificates to clients and servers, businesses can reduce costs, risks and human error.

Flexibility: Users can easily move from machine to machine as there is no limit on the number certificates that can be issued.

Customizable expiration: SSH certificates can be set to expire after a certain time period, reducing the security impact of stolen certificates. Short lived certificates are increasingly popular as a mechanism to reduce risk. (Coming Soon)

By leveraging Sectigo's extensive experience in certificate management and certificate issuance, and by implementing a more robust SSH Authentication strategy, enterprises will see greater efficiencies in IT administration, reduced risk of security breaches and more control of critical resources. Sectigo Management for SSH certificates significantly reduces the costs of managing authentication for SSH servers by making it easy and scalable to deploy certificates as the authentication mechanism of choice.

Sectigo Certificate Manager

Sectigo Certificate Manager (SCM) is a universal platform purpose-built to issue and manage the lifecycles of public and private digital certificates to secure every human and machine identity across the enterprise, all from a single platform. In addition to providing tools for automation of client and server certificates, SCM provides management tools for code signing, document signing and SSH certificates. As certificates are increasingly recognized as being the foundation formsecure communication between systems, a single platform to manage these digital identities is an essential tool in the modern enterprise. SSH certificates are an example of how SCM provides immediate and compelling value to the enterprise.

For more information on Sectigo Certificate Management for SSH Authentication and other solutions enabled by Sectigo's certificate lifecycle management platform, please reach out to Sectigo Sales at sales@sectigo.com.

About Sectigo

Sectigo is the leading provider of digital certificates and automated Certificate Lifecycle Management (CLM) solutions trusted by the world's largest brands. Its cloud-based universal CLM platform issues and manages the lifecycles of digital certificates issued by Sectigo and other Certificate Authorities (CAs) to secure every human and machine identity across the enterprise. With over 20 years of experience establishing digital trust, Sectigo is one of the longest-standing and largest CAs with more than 700,000 customers, including 36% of the Fortune 1000.