SSL Automation

SECTIGO

Single platform to serve all varieties of use cases

All the applications in the enterprise

VPN
SSH
DevOps
Networking Gear
Public & Private Web Server
Mobile Devices
Email Signature Encryption
Cloud Key Vaults
Code Signing
Digital Sign Forms
Cloud Access
IoT

Identity Assurance
Issuance
Reporting
Revocation
Renewals

100% automated certificate provisioning via Industry Standard Protocols

Breaks out to these components

Public CA	Private CA

Certificate Manager

Encryption Key Vault

100% Automation delivers Crypto-Agility, example:
- Cryptography compromised by Quantum computing
- Find all keys/certs which are compromised
- Automatically replace immediately

SECTIGO

Enterprise Demand for Automation

- **Browsers have reduced the SSL certificate validity period to 398 days, effective Sept 2020**
  - *Doubles the number of employees required to manually install certificates*
  - *The more activity, the more chance of error, leading to a service outage*
- **Browsers will be used to access Web Servers and Load Balancers behind the firewall**
- **DevOps demands 100% automation for the setup of Web Servers and Load Balancers**
  - *Automation to reliably and efficiently compile, build and deploy their code in the DevOps pipeline*
  - *Need support on a wide variety of DevOps tools*
- **Enterprise requires customized workflows for approvals as part of the automation**
- **Enterprise requires the integration with ServiceNow to automate approval workflow**
- **Enterprise using web servers and load balancers with Cloud Key Vault(s), requires key management**
- **Criticality of services requires 7x24x365 support**
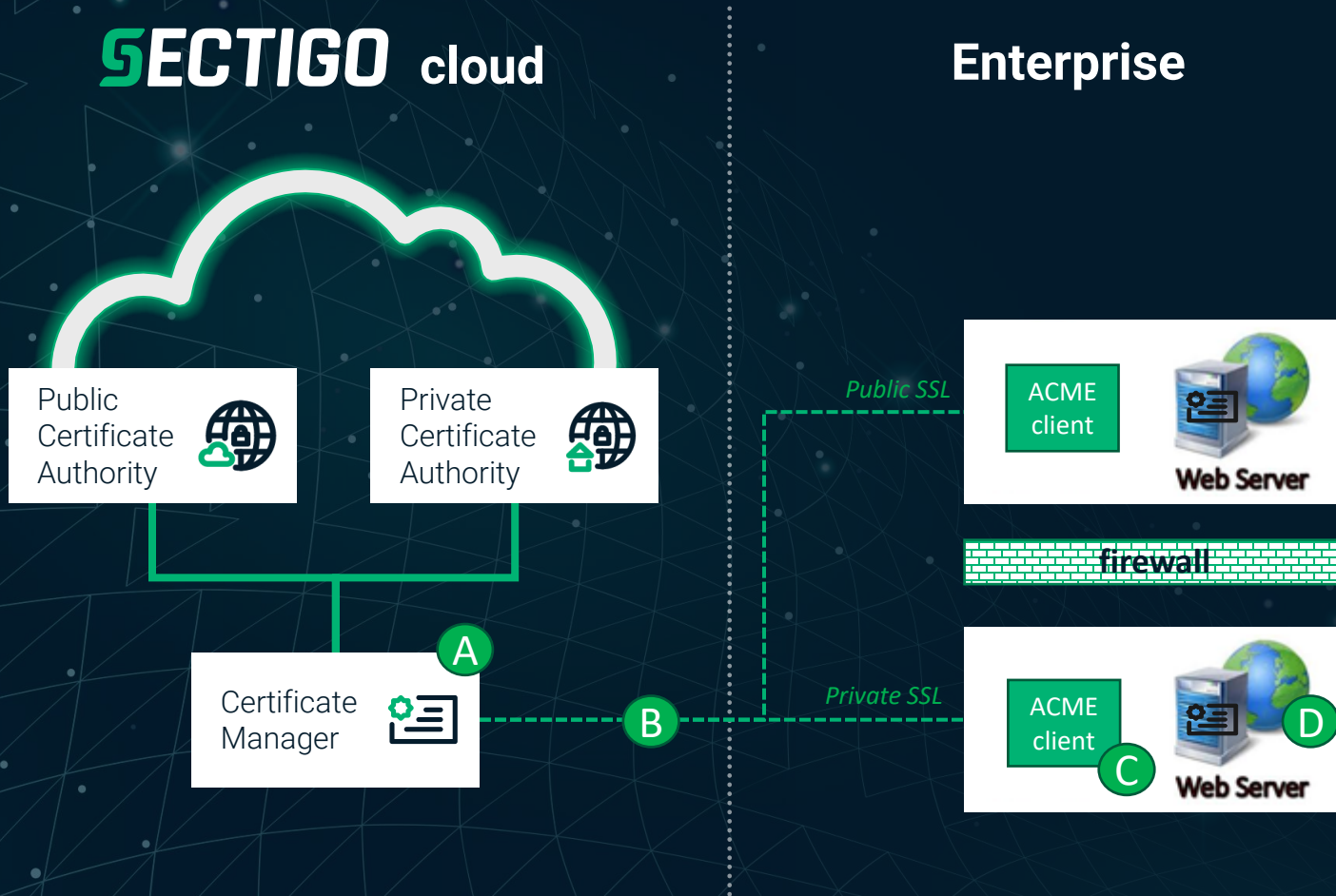
SECTIGO

Automation – Solution

Sectigo is the only vendor to provide the customer all these options:

1. Automated Certificate Management Environment (ACME) an open standard, RFC8555
2. Sectigo customer premise agent
3. Sectigo open source integrations with all the popular DevOps tools
4. REST API for customer authored automation, with custom workflow
5. Azure Key Vault
6. ServiceNow integration

For Public & Private Web Servers & Load Balancers

Automated SSL installation - ACME

SECTIGO cloud

Enterprise

Public Certificate Authority

Private Certificate Authority

Certificate Manager

A

B

Public SSL

Private SSL

ACME client — Web Server

firewall
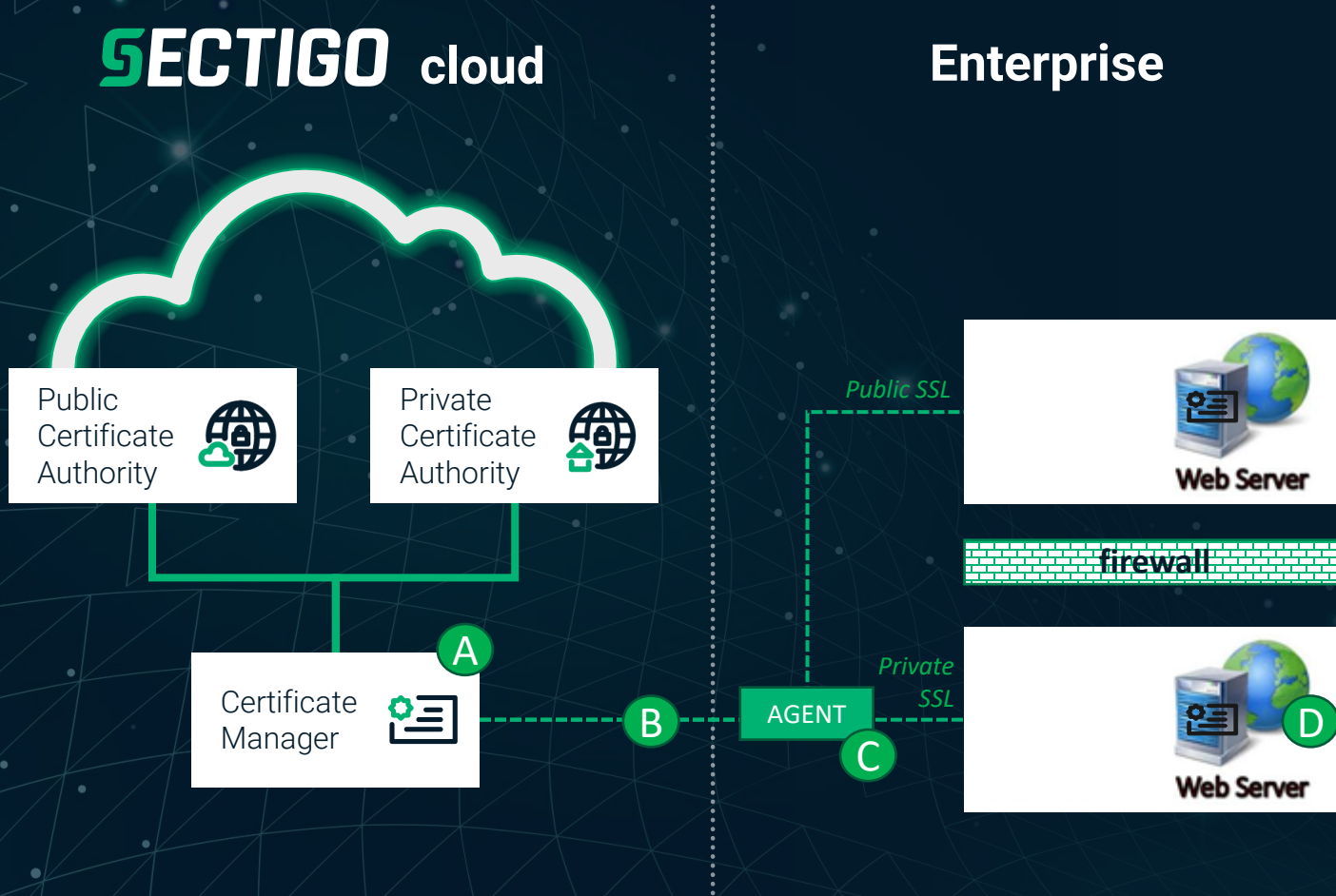
ACME client **C** — Web Server **D**

Current State

- Excessive cost to purchase multiple tools
- Excessive cost to integrate different tools
- Slow certificate replacement in the event of an immediate threat

Sectigo Value

A. Single Pane of Glass for all identity management

B. Automated certificate creation and installation

C. ACME client collocated with web server or load balancer
   - *ACME is an industry standard between Certificate Authorities and applications using SSL (RFC8555)*

D. Web Servers (Apache) are building ACME into their product. It is the future.

SECTIGO

Automated SSL installation - AGENT

SECTIGO cloud

Enterprise

Public Certificate Authority

Private Certificate Authority

Certificate Manager

A

B

AGENT

C

Public SSL

Private SSL

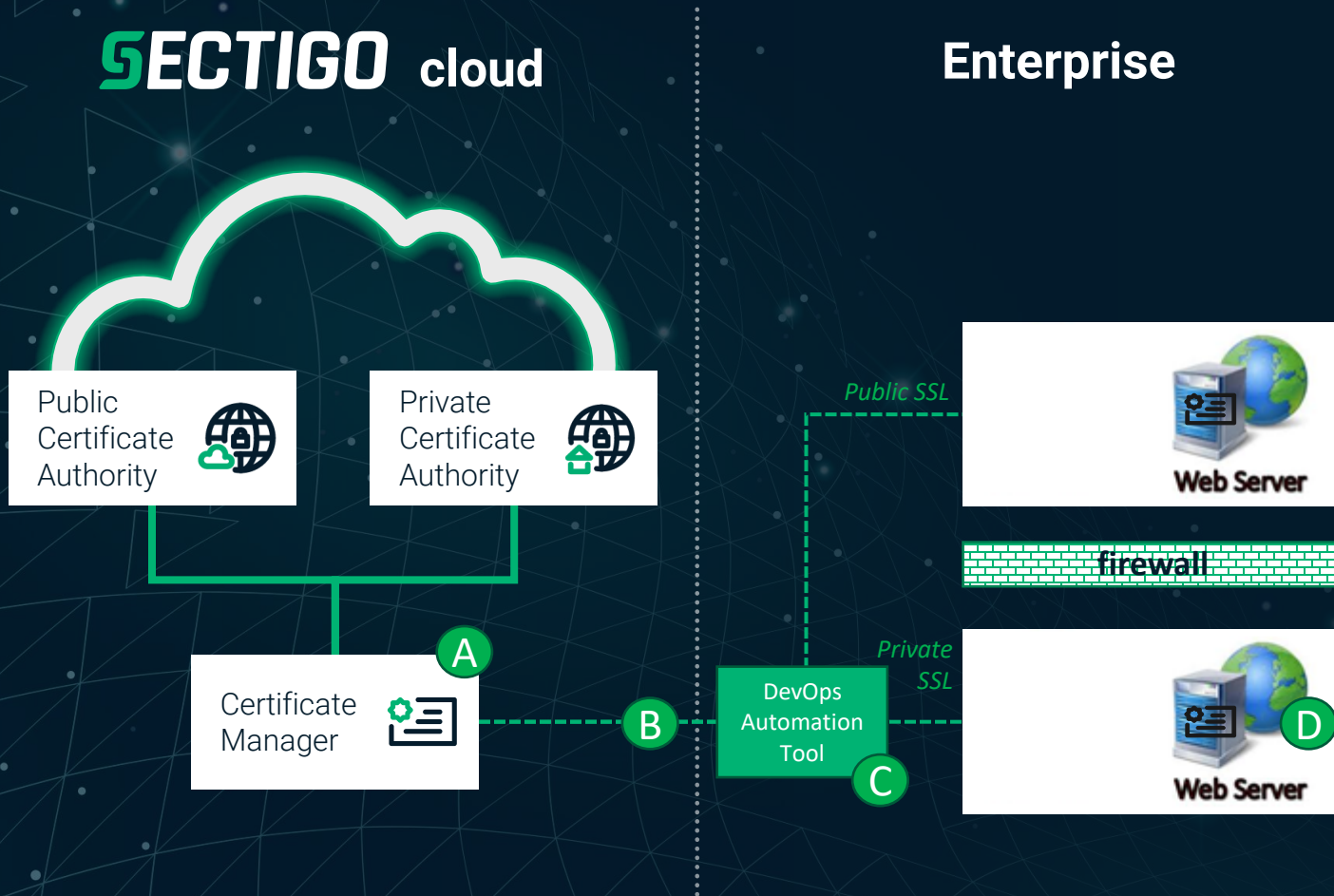**Web Server**

firewall

Web Server

D

Current State

- Excessive cost to purchase multiple tools
- Excessive cost to integrate different tools
- Slow certificate replacement in the event of an immediate threat

Sectigo Value

A. Single Pane of Glass for all identity management
B. Automated certificate creation and installation
C. Agent manages several web servers, load balancers, migrates private keys across multi-domain/wild card certs
D. Supported:
   - Apache
   - IIS
   - Tomcat
   - F5

SECTIGO

Automated SSL installation − DEVOPS Automation Tools

SECTIGO cloud

Enterprise

Public Certificate Authority

Private Certificate Authority

Public SSL

Web Server

firewall

Certificate Manager

A

B

DevOps Automation Tool
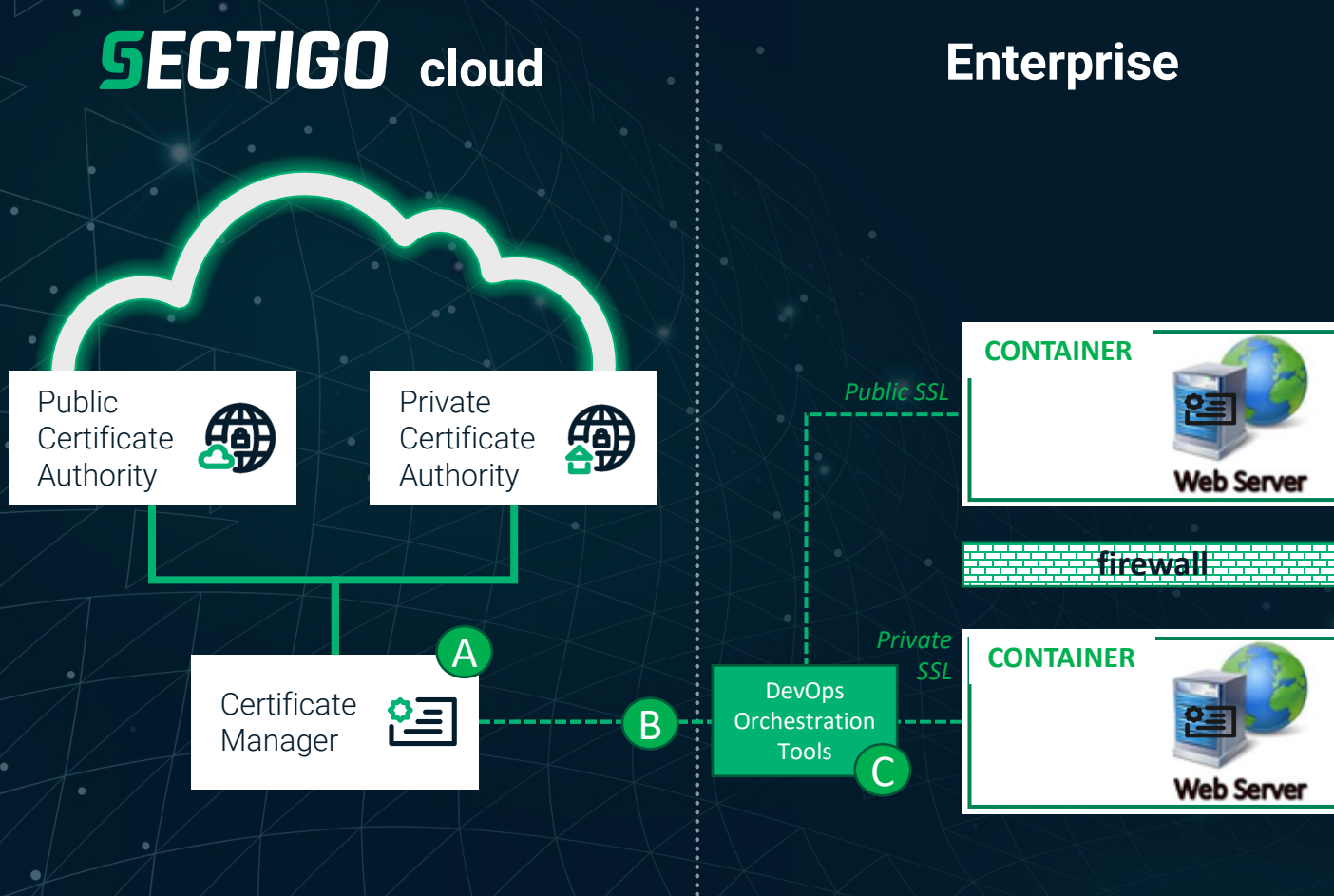
C

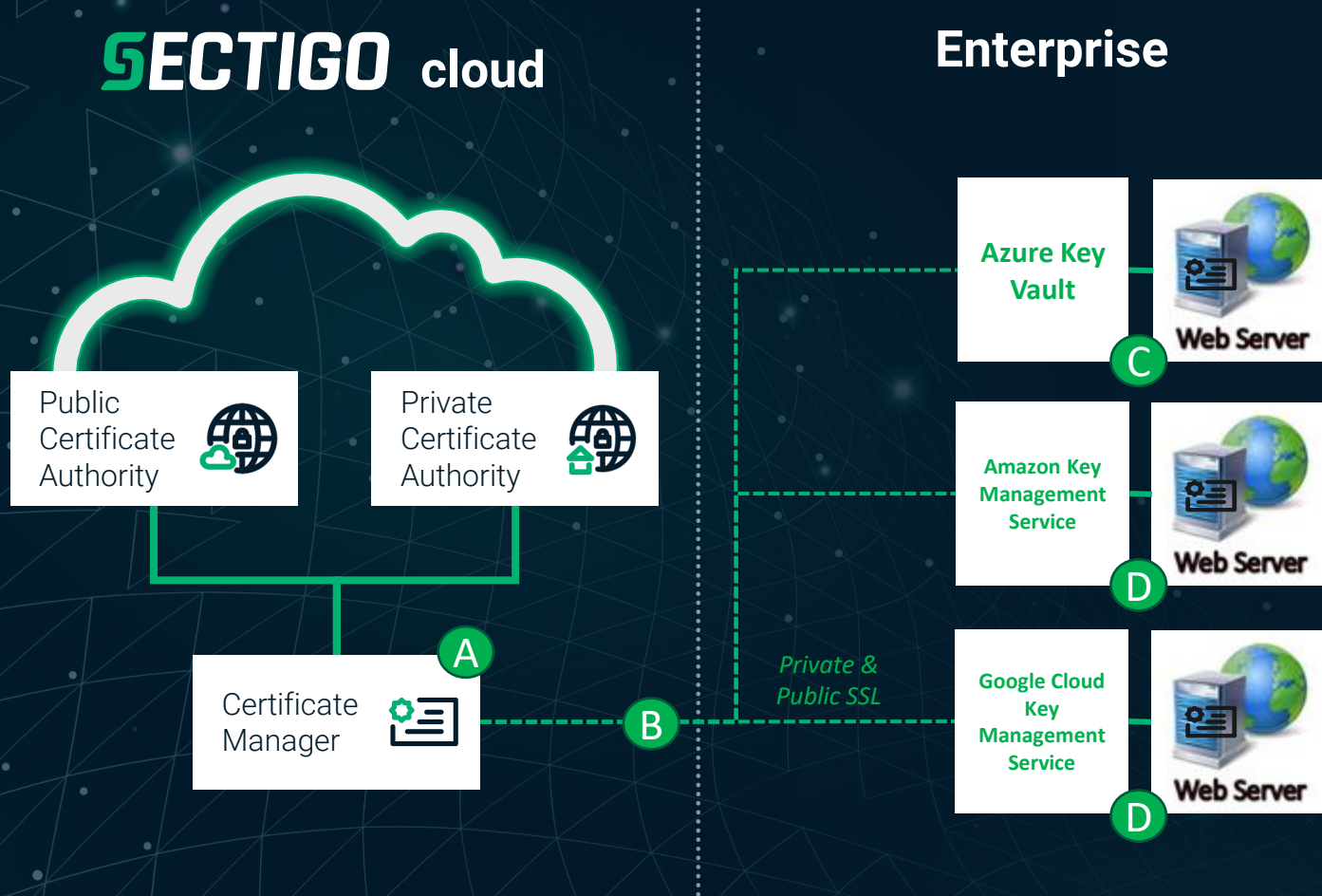Private SSL

Web Server

D

Current State

- Excessive cost to purchase multiple tools
- Excessive cost to integrate different tools
- Slow certificate replacement in the event of a threat
- DevSecOps team cannot enforce compliance without slowing the pipeline
- Requirement to setup the webserver or load balancer, including SSL
- Free SSL rate limit impacts enterprise

Sectigo Value

A. Single Pane of Glass for all identity management
B. Automated certificate creation and installation
C. Out of the box DevOps automation tool integrations
   - Ansible
   - Chef
   - Puppet
   - Jenkins/Saltstack

SECTIGO

Automated SSL installation – DEVOPS Orchestration Tools

SECTIGO cloud

Enterprise

Public Certificate Authority

Private Certificate Authority

Certificate Manager

A

B

DevOps Orchestration Tools

C

Public SSL

CONTAINER

Web Server

firewall

Private SSL

CONTAINER

Web Server

Current State

- Excessive cost to purchase multiple tools
- Excessive cost to integrate different tools
- Slow certificate replacement in the event of a threat
- DevSecOps team cannot enforce compliance without slowing the pipeline
- Requirement to provision certificates into containers for SSL and inter-container TLS across cloud platforms
- Free SSL rate limit impacts enterprise

Sectigo Value

A. Single Pane of Glass for all identity management
B. Automated certificate creation and installation
C. Out of the box DevOps Orchestration tool integrations
    - Docker
    - Kubernetes
    - Istio/Citadel
    - Terraform
    - Hashicorp vault

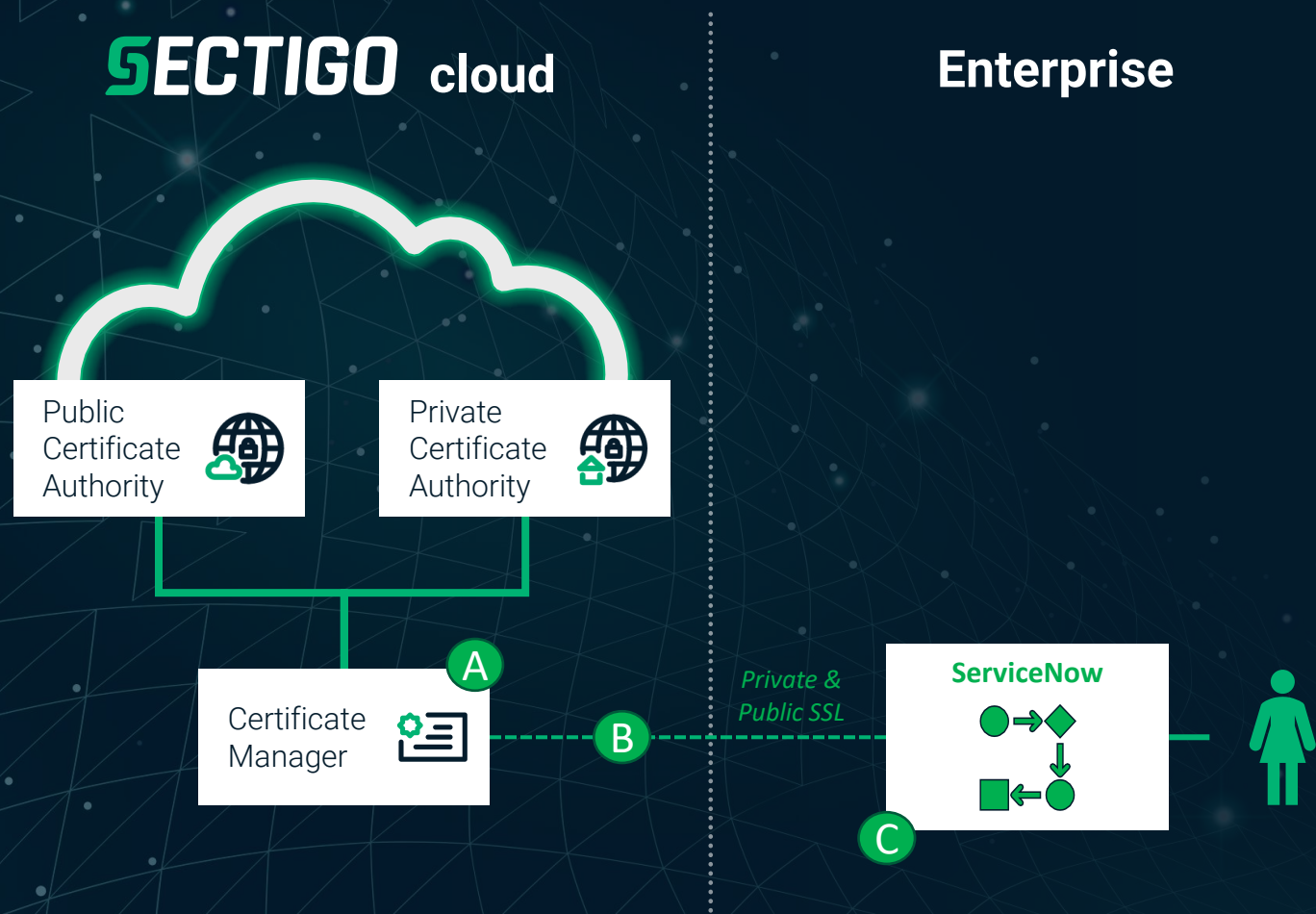**SECTIGO**

Automated SSL installation − Azure Key Vault

SECTIGO cloud

Public Certificate Authority

Private Certificate Authority

Certificate Manager

A

B

Enterprise

Private & Public SSL

Azure Key Vault — Web Server **C**

Amazon Key Management Service — Web Server **D**

Google Cloud Key Management Service — Web Server **D**

Current State

- Manual, expensive process to provision keys and certs to Azure Key Vault
- Lack of management leads to certificate expiry
- Slow certificate replacement in the event of a threat
- Requirement to provision certificates into key vaults which span cloud providers

Sectigo Value

A. Single Pane of Glass for all identity management
B. Automated certificate creation and installation
C. Web Servers, load balancers or applications do not need to embed certificate renewal logic
D. Amazon and Google are on the roadmap
E. Same platform for other enterprise applications (document signing, encryption)

SECTIGO

Automated SSL Approvals Workflow – ServiceNow

SECTIGO cloud

Enterprise

Public Certificate Authority

Private Certificate Authority

A

Certificate Manager

B

Private & Public SSL

ServiceNow

C

Current State

- Enterprise policy requires sophisticated approvals process, in common corporate tool, ServiceNow
- Lack of management and slow approvals leads to certificate expiry
- Slow certificate replacement in the event of a threat

Sectigo Value

A. Single Pane of Glass for all identity management
B. Automated certificate creation and installation
C. Employee initiates change, executes workflow, obtains approvals, certificate issued
D. Only vendor that allows for all reporting and management from ServiceNow UI

SECTIGO

Why Sectigo

- **Single Platform to discover, manage, report and install all your certificate & key needs**
- **Public, Private Certificate Authority, option to continue to use ADCS**
  - SSL, Code Signing, SMIME, Document Signing, eIDAS, Users, Devices, Servers, Applications, Encryption
- **Fastest setup of certificate manager, certificate authority in the industry**
- **Largest number of integrations**
  - Windows applications
  - DevOps tools: *Ansible, Chef, Puppet, Jenkins/Saltstack, Docker, Kubernetes, Istio/Citadel, Terraform, Hashicorp vault, etc.*
  - Mobile Certificate Manager: *Apple, Android, MCM portal, Intune, Airwatch, Blackberry, Citrix, etc.*
  - Mail Applications: *Outlook, Apple Mail, etc.*
  - IoT devices
  - Azure KeyVault, Google, AWS key vault
- **Largest breadth of automation**
  - Industry standard, no vendor locking, no proprietary solutions
  - EST, SCEP, ACME, REST API
- **High service availability**
- **Best in class 7x24x365 day support across the entire solution**

SECTIGO

Sectigo by numbers *(get the latest from corporate deck)*

100M+

Certificates issued. **Critical** to businesses worldwide.

Used by over

700,000

businesses **worldwide.**

99%

Enterprise customer **retention** rate.

20+

years of **experience** in digital trust solutions.

>36%

Fortune 1000 companies use our solutions.

#1

market leader based on top 10M websites according to Alexa popularity rankings.

SECTIGO

Trusted by leading brands globally (get the latest from corporate deck)
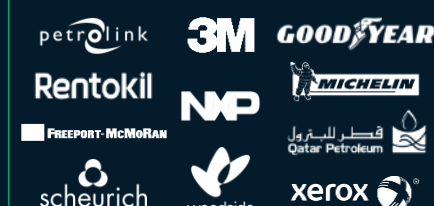
What to learn more?

Written

https://sectigo.com/uploads/resources/Automation_datasheet.pdf

Video

https://sectigo.com/resource-library/sectigos-acme-automation
https://sectigo.com/resource-library/digital-certificates-in-the-modern-enterprise

Podcast

Quantum: https://sectigo.com/uploads/resources/Quantum-Resistance-Whitepaper.pdf?token=1575326951
DevOps: https://sectigo.com/resource-library/all-about-agility-pki-in-devops-matters
1 year SSL certs: https://sectigo.com/resource-library/be-prepared-for-one-year-ssl-certificate-duration
SSL & Netscaler: https://sectigo.com/resource-library/enable-certificate-management-automation-for-citrix-adc-with-sectigo
ACME: https://sectigo.com/resource-library/automated-certificate-management-is-no-longer-a-nice-to-have-its-essential
SSL Automation options: https://sectigo.com/resource-library/when-it-comes-to-ssl-certificate-automation-sectigo-provides-plenty-of-options

SECTIGO

Questions…

SECTIGO