PKIS: End-to-End PKI Provisioning System

Introduction

The CommScope Public Key Infrastructure (PKI) Center provides a variety of security-related services spanning several different markets. Our security services are provided to operators as well as manufacturers and are utilized in numerous ecosystems. The main security offerings include:

- Operation of Certificate Authorities (CAs) that issue digital certificates for high-volume manufactured products (such as cable set top boxes, cable modems and mobile phones), as well as for high-value infrastructure applications and server machines.
- Secure delivery and installation of digital certificates and cryptographic keys into products at manufacturing facilities.
- Obtaining secure data from external licensing authorities such as CableLabs, DTLA, DCP, Google, Netflix, etc., as well as packaging, secure delivery and installation of these data into products in factories.
- Software platform security services, including secure code signing and debugging services for product software platforms and application code.
- On-line Personalization Update System for creation and secure delivery of renewable security and personalization data to fielded devices on a mass-scale.
- Security consulting to variety of system engineering, product management and development teams in matters of network, application, and platform security for both secure and non-secure products.

The CommScope PKI Center evolved from the company's broadband Conditional Access experience, beginning in the 1980s at predecessor company General Instrument (GI). Our team has over 30 years of experience of managing the complete lifecycle of product security. Figure 1 illustrates the evolution of the CommScope PKI Center through the years. The CommScope PKI Center has grown to become an industrial leader and expert in secure provisioning and has accumulated its experiences from dealing with a wide variety of use cases and security requirements for a broad range of products such as set top boxes, cable modems, home gateways, mobile devices, System-On-Chips (SOCs), etc. We work extensively with manufacturers, factories, repair and service centers to provide a seamless provisioning solution.

In 2018, the CommScope PKI Center received the WebTrust seal of assurance for Certificate Authorities. This allows the PKI Center to offer PKI services with an extremely high level of assurance that require WebTrust standard compliance. The CommScope PKI Center undergoes yearly audits by

outside auditors in order to maintain the WebTrust seal. The seal is required by numerous ecosystems, including the WInnForum 3.5GHz Citizens Broadband Radio service (CBRS) and all of the PKI ecosystems defined by CableLabs.

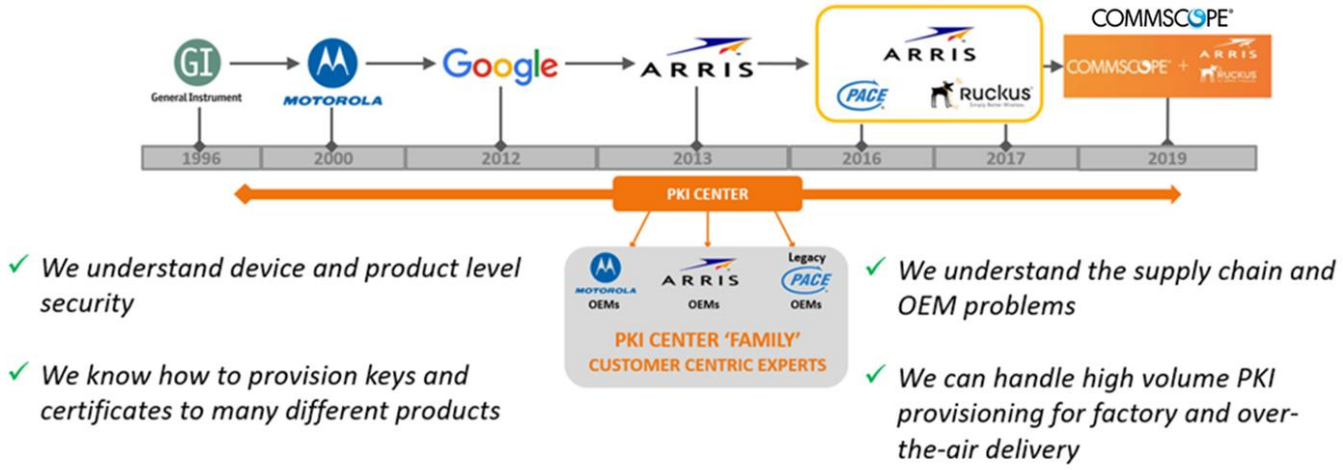

Figure 1 CommScope PKI Center Evolution

This whitepaper describes the End-to-End PKI Provisioning System provided by the CommScope PKI Center.

Turnkey Provisioning Solution

The CommScope PKI Center operates and maintains a proven large-scale certificates and keys provisioning system consisting of secure offline key generation and packaging facilities, hardened key servers with high availability, reliable and secure keys distribution networks, and thousands of programming stations at hundreds of factory locations. With the infrastructure and experience, The CommScope PKI Center is able to offer a turnkey solution to customers with secure keys and identity provisioning needs.

The CommScope PKI Center's provisioning solution covers the entire key and identity lifecycle management, from key generation and packaging, product development, distribution of keys and identities to factories and repair centers. In the case of digital certificates in a public key infrastructure, The CommScope PKI Center also offers standard revocation mechanisms in the case of a key compromise.

The CommScope PKI Center also provides Software Development Kit (SDK) support for rapid development and easy integration. The CommScope PKI Center can help device manufacturers to get quickly set up for secure factory provisioning by offering provisioning SDKs, making security transparent

to product software. The SDKs include built-in support for securely handling, validating, and processing of device keys downloaded from the provisioning system. The CommScope PKI Center's provisioning SDKs are available in a wide variety of popular platforms and programming languages.

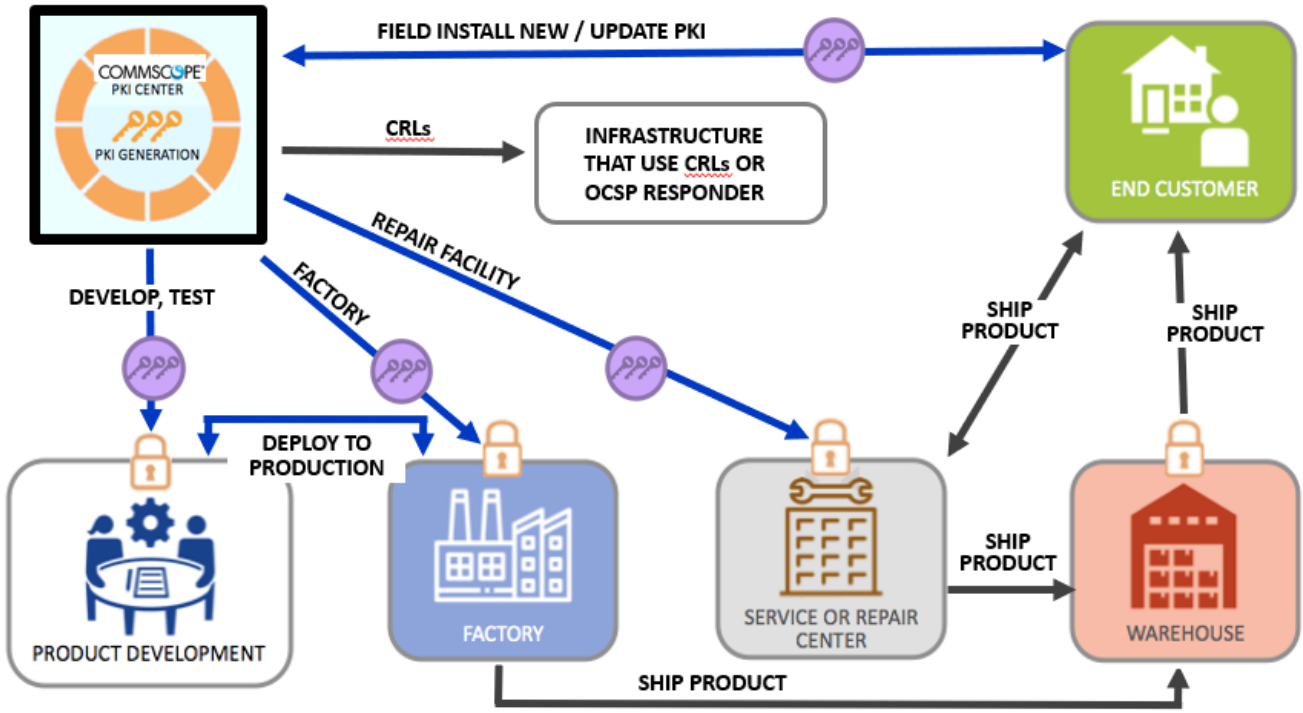

Figure 2 Full Identity and Key Lifecycle Management

Reality Motivates Strong Security

Provisioning of keys and identities in factories call for strong security measures for several reasons:

- **Globalization has extended supply chains:** Manufacturers are vulnerable to potential interruptions beyond their control.
- **Semi-secure environment:** Factory environments are by nature less tightly controlled, with factory staff having a high turnover rate. Factory engineering and IT personnel may not be well-trained in information security and may not be sensitive to the need to protect cryptographic material.
- **Security procedures vs. normal manufacturing process:** Security procedures are typically very different from normal manufacturing processes. For instance, normal data and code may be freely copied and backed up. Copying and backing up device credentials, however, could result in cloning, a very serious security risk.

The CommScope PKI Center's End-To-End PKI Provisioning System offers the following security features:

- **Protection against disclosure of secret and private keys**
  - Extensive use of hardware security modules (HSMs) in various portions of the system for professional grade security.
  - Multiple layers of encryption - device keys are encrypted for specific site and location in addition to the end-to-end encryption applied per product or chip.
  - Optional device SDKs for data decryption and validation to ensure proper handling of received device keys on the product.
- **Protection against cloning**
  - The CommScope PKI Center incorporates various mechanisms to prevent device identities from being copied and reused during generation, distribution and provisioning**.**
- **Protection against unauthorized factory sites**
  - The CommScope PKI Center provides additional hardware and software components to harden manufacturing stations in the factories.
  - The CommScope PKI Center maintains full traceability of provisioning activities to each online and factory server, manufacturing stations and target device.

Global System Deployment and Support

The CommScope PKI Center interfaces with approximately 200 factory servers and systems deployed to over 30 sites in 14 countries, including the San Diego main facility and Disaster Recovery (DR) sites. Figure 3 depicts the global footprint of the PKI Center. PKI Center is highly experienced in global logistics, including import/export of equipment and Customs support. Many countries, including USA, China, Mexico, have very specific and stringent import and export requirements for both hardware and software. For someone not familiar with the process, this could take significant time and effort. It may often times incur unexpected delay and additional cost and fines in the deployment process.

The CommScope PKI Center has an experienced operational team that covers systems, networks, databases, and security operations. We provide managed software and database deployment, pre-production validation, and 24-7-365 support.

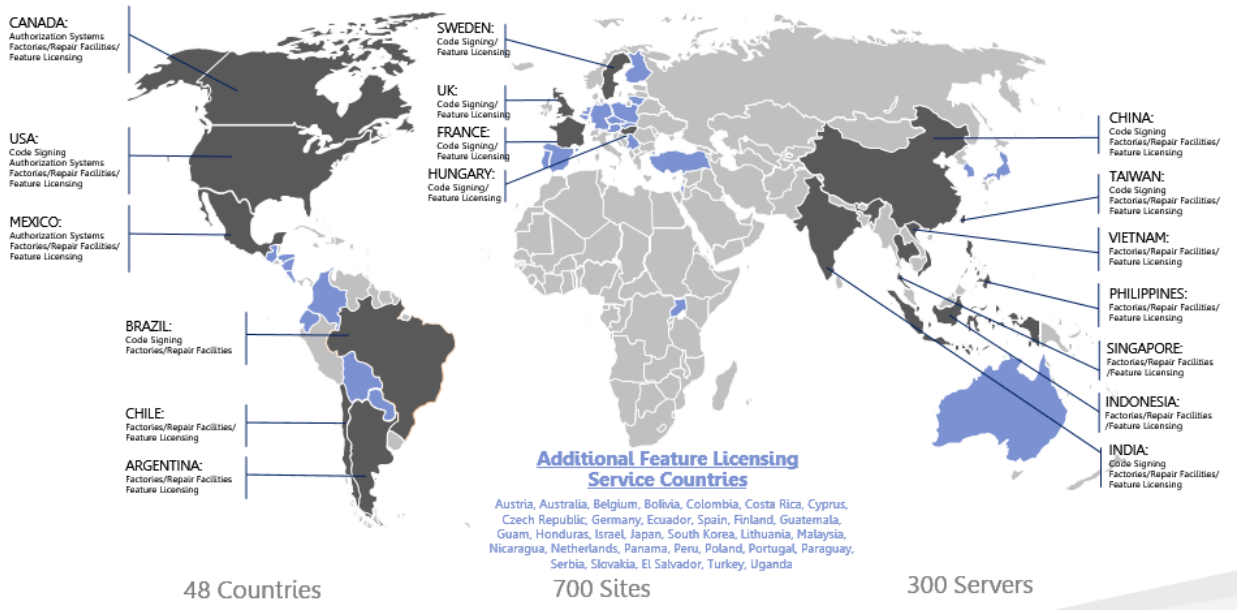

Figure 3 CommScope PKI Center Global Footprint

Inventory Monitoring

Imagine all the factory production lines were forced to a complete standstill, only to find out it is due to key depletion. The CommScope PKI Center provides an accurate and easy-to-use real-time monitoring system for managing key inventory for the various key types needed for the manufacturing of a device. By setting up inventory thresholds for each key type, system notifications will be delivered automatically to our operational teams to replenish the corresponding key pools. With the CommScope PKI Center inventory monitoring system, customers are free from the tedious task of managing the key pools and can rest assured that key provisioning will be running smoothly.

Reporting

The CommScope PKI Center provides seamless generation, distribution, and provisioning of various key types. As keys and identities are provisioned into each device, provisioning logs are captured and delivered back to the central provisioning database. The CommScope PKI Center's reporting system provides tracking of various keys and identities. A real time health and inventory monitoring system is maintained by the CommScope PKI Center, making provisioning data available at the convenience of your fingertips. Standard reports include key provisioning counts by key type, factory location and time period in the form of usage charts and graphs. Provisioning events associated with a specific device are also searchable.

In addition to the standard real-time and periodic reporting functionalities, the CommScope PKI Center is also capable of generating custom provisioning reports tailored for specific needs. This may be used to better interface with customers' manufacturing back offices. Custom reporting has been proven to be extremely useful for troubleshooting manufacturing errors.

Commercial Separation

The CommScope PKI Center maintains WebTrust audit verified commercial separation from CommScope's Device Businesses.

Competitive Differentiators

The CommScope PKI Center's End-to-End Provisioning System provides the following advantages over competing systems:

- **Low incremental cost for new customers**
  - Low entry cost through reuse of existing key provisioning services and types.
  - A flexible and extensible system allowing easy customization and evolution, introduction of new types of keys, certificates, devices and cryptographic algorithms.
  - Fine-tuned integration and deployment processes.
- **Massive scale**
  - Current capacity greater than 30 billion device keys provisioned per year.
  - A scalable architecture to support an even higher volume if needed.
- **Extensive direct experience**
  - Actual worldwide product manufacturing with secure key and certificate provisioning, including 24-7-365 technical support, hot standbys and disaster recovery.
  - A large variety of products, including set top boxes, modems, gateways, cell phones, chips, software, infrastructure, etc.
  - Operation of variety of highly secure and highly scalable Certificate Authorities and Registration Authorities
  - Applied cryptography, secure product and protocol design and information assurance.

Summary

The CommScope PKI Center's End-to-End PKI Provisioning Service is one of many different security services that are provided by the CommScope PKI Center team. The design and operation of this

service is extremely resistant to both outsider and insider attacks. This service securely provides personalization data to manufactured products in factories, distribution centers and service centers. The underlying provisioning system of the service is highly flexible and fully extensible for new types of devices and personalization data. This system provides a turnkey solution for secure key and identity provisioning for high volume manufactured products.