IMAGINE
THE POSSIBILITIES...
A Flexible and Scalable Architecture for Over-the-Air Credentials Provisioning

Alexander (Sasha) Medvinsky
Engineering Fellow
CommScope
Agenda

Over-the-Air Provisioning of Device Credentials

- The purpose for over-the-air credentials provisioning
- Online PKI Update System (OPUS) overview
- Basic Use Case: provisioning credentials based on operator and device model authorization
- Summary of additional use cases covered by the paper
- Conclusion
Why Over the Air Credentials Provisioning?

### Fielded Devices Additional Credentials Provisioning

- The network operator signs up for a DRM after devices are already manufactured.
- The network operator decides to switch to a new DRM system that wasn’t considered prior to device manufacture.
- The network operator wishes to install operator-specific device certificates which were defined after the start of device manufacture.
- Additional device credentials have an additional fee that the operator or consumer doesn’t wish to incur until a consumer subscribes to a specific service.
- A new DRM or copy protection technology is defined after device manufacture and network operator adds this new technology and new credentials via a field update.
- A secure application for a PC or mobile device requires new unique credentials.
  - Application provider has no control over general-purpose device manufacture.
Online PKI Update System (OPUS) overview

Cert & CRL Repository

Key Inventory MONITORING

Authentic & Encrypted Session

Internet

PRODUCT SDK

DEVICE

One ID for one device. Can download same set of keys multiple times if needed.

Ensure ID delivered to targeted device

Ensure OPUS server authenticated by device

SYSTEM SECURITY FEATURES

Anti-Cloning and/or Anti-duplication

Protection against key disclosure

Full traceability and audit logs

SDK and integration support

OPERATORS, FACTORIES

Authorized Device ID List

Secure Key Generation Facility

PKI LOADER

FIREWALL

OFFLINE GENERATION of Device Credentials REPACKAGING

EXTERNAL KEY LICENSING AUTHORITIES

DTCP, Netflix, Widevine, ...

OPUS SERVER

ADDITI ONAL SECURITY FEATURES

Internet

Cert & CRL Repository

Key Inventory MONITORING

Firewall

Cloning

Cloning

Cloning

Cloning

Cloning

Cloning

Cloning

Cloning

Authorized Device ID List

One ID for one device. Can download same set of keys multiple times if needed.
Over-the-Air Credentials Provisioning System Overview

- Online provisioning service must be hardened against all kinds of attacks
- Perimeter security: firewalls, IP address filtering, Intrusion Detection System (IDS)
- Physical security: controlled access to server room, video surveillance, guards, etc.
- Application security: vulnerability scanning on all software releases
- Network isolation: backend network protecting the most sensitive resources
- Hardware Security Module (HSM) to protect all private & secret keys

- Device credentials (secret & private keys) are encrypted in a separate air-gapped facility before being loaded to the online system
- Prevent cloning/duplication of device credentials:
  - Hardware-based random number generator
  - Additional session encryption and protocol-level anti-replay
  - End-to-end encryption with a unique per-device key
- System monitoring & audit logs
Operator and device model authorization

1. OEM generates factory credentials
2. OEM provisions factory credentials
3. Deploy to field
4. Configure security params
5. Authorized Device ID List
6. Generate/Import/Encrypt & load to OPUS
7. Key/Cert Request (ID)
8. OPUS retrieves uniquely encrypted Key/Cert based on ID
9. Key/Cert Response

Network Operator
Offline Key Generation Facility
OPUS
OPUS Admin
Credentials Provisioning Use Case #1

Operator and device model authorization (Continued)

- Device is manufactured with pre-existing factory-installed certificates
- Configure OPUS with trusted Root & Sub-CA for device model & credential type
- Credentials are initially processed or generated and encrypted in offline facility
  - Targeted to specific authorized devices or for all devices of a specific model
  - Then transfer to online server
- Fielded devices receive a software update to prepare for credentials provisioning
  - There may be an additional device management message (trigger)
- Device submits a credentials request to OPUS
  - Include device signature and cert chain (typically factory-installed)
  - And DH or ECDH device public key
- OPUS validates device and network operator, model and device ID authorization
- Derive one-time session key for additional encryption
Summary of Additional Use Cases

Additional Use Cases Described in the Paper

- Subscription-based authorization
  - A gateway device providing authorization token proving subscription
- Offline Matching Existing Device ID
  - Security provider obtains a list of authorized devices
  - Retrieves their factory-installed credentials, generates, packages and encrypts for specific devices off-line
- Online Matching Existing Device ID
  - The turnaround time between obtaining a list of authorized devices and getting credentials ready for download may be very short
  - The offline approach may be too slow and credentials are generated on the fly on a secure server
- Additional use cases in the planning
Summary

• There is a real need to provision credentials securely to today’s consumer devices and networking devices in the field
• There are many different use cases with a wide range of different requirements and challenges
• We demonstrate the flexibility and scalability of our field provisioning system to address these use cases
• New cases will keep coming, our system is constantly evolving to deal with them
Thank You!

Alexander (Sasha) Medvinsky
Engineering Fellow
CommScope
sasha.Medvinsky@commscope.com