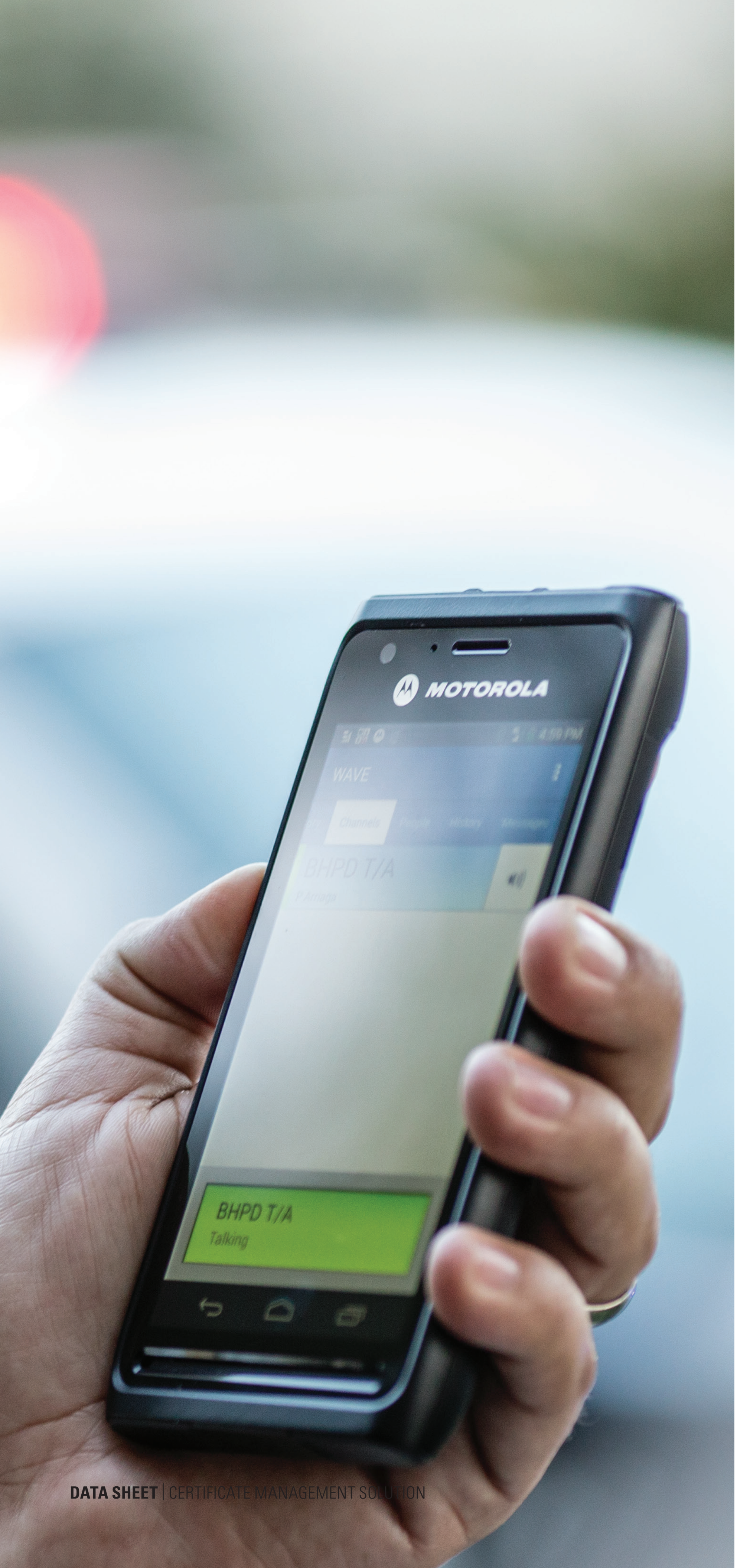
CERTIFICATE MANAGEMENT SOLUTION

CERTIFICATES MADE MANAGEABLE ACROSS PUBLIC SAFETY LTE

MOTOROLA SOLUTIONS



EFFICIENTLY AUTHENTICATE AND MANAGE YOUR CERTIFICATES

As the dual trends of cloud and mobility accelerate, the traditional means of securing networks are rapidly evolving. Today, your personnel are using more smart devices on the job to enhance productivity, collaboration and safety. Those devices are running six or more applications on average per day, from secure messaging, WAVE, mapping and CAD.

Managing security across this growing number of devices and applications while ensuring your mobile workforce has instant access to the people and information they need can be a daunting task. Now, more than ever, you need a reliable and secure certificate-based authentication mechanism to verify trusted devices and applications. Additionally, you need to be able to effectively manage the entire certificate lifecycle, enroll devices remotely and automatically, and have complete visibility into your certificate deployment including which users are authenticated and what information and applications are accessible.

Without the above, your security environment is susceptible to unauthorized system access, data vulnerabilities, falsified authentication Distributed Denial of Service (DDoS), and man-in-the-middle attacks. Our Certificate Management Solution (CMS) addresses your end-to-end digital certificate needs – making it easy to distribute and manage digital certificates.

EXPERIENCE AN END-TO-END NETWORK CERTIFICATE SOLUTION ON PREMISE, ACROSS INFRASTRUCTURE, ON-DEVICE, AND OTA OPERATING NEEDS

Our CMS is designed to meet your digital certificate needs across your entire Public Safety LTE network.

CMS allows you to save time and resources as well as prevent errors, you can also remotely enroll your mobile devices' client certificates with our CMS' over the air certificate enrollment (OTA CE). This unique feature reduces your fleet's certificate enrollment challenges quickly identify any unauthorized equipment, prevent vulnerable connections, and better enforce security policies. It also provides enhanced visibility across all digital certificates throughout your entire Public Safety LTE network including all devices. Your devices and system servers are who they say they are and your network is less prone to certificate-related security compromises.

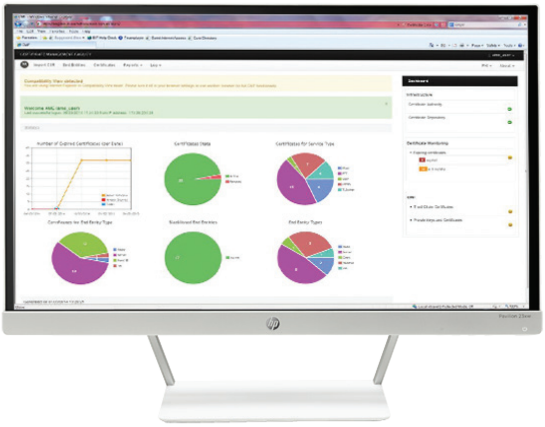
CMS OVERVIEW

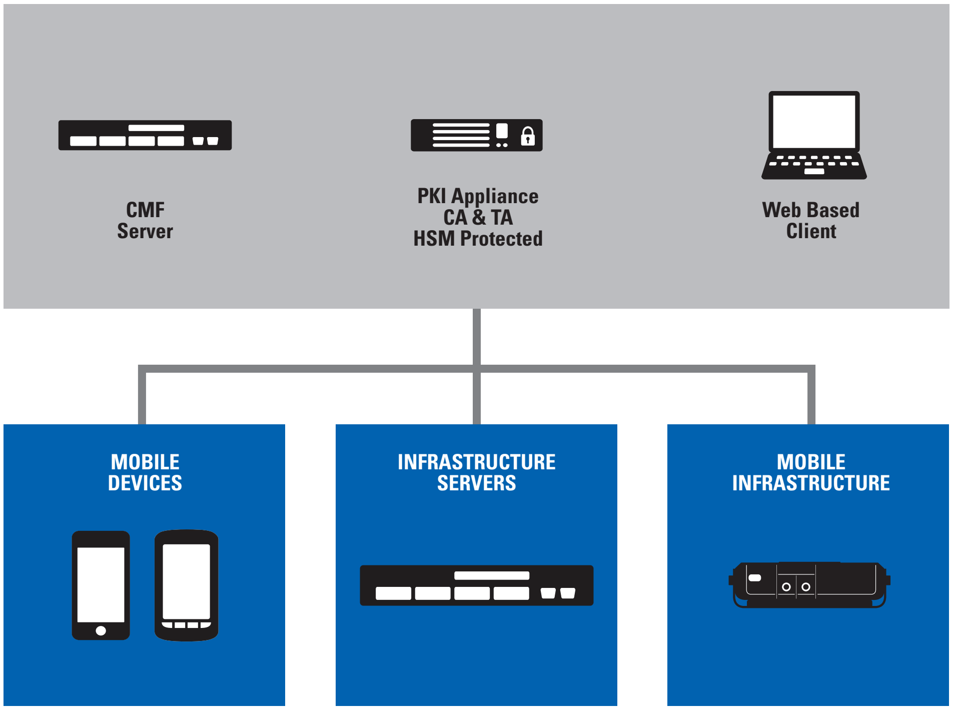
The CMS includes two primary components: the Certificate Management Facility (CMF) and end entities (e.g. Mobile Devices, Application Servers, PSX Cockpit etc.).

- The CMF consists of two separate servers. One is the Public Key Infrastructure (PKI) appliance which contains the Trust Anchor (TA) and issues Certificate Authority (CA), as well as a Hardware Security Module (HSM) that securely stores private encryption keys. This HSM is FIPS 140-2 Level 3 validated by National Institute of Standards and Technology (NIST). The second server houses the Virtual Machines (VM) running the Certificate Manager (CM).

  [NOTE: For agencies that are more risk adverse, the root CA may be housed in an offline standalone PKI appliance].

- The Certificate Manager (CM) enhances the management and capabilities of the PKI and provides the main user interface to monitor the status of certificates system-wide. The CM's intuitive web based portal allows administrators to issue, monitor, manage, and revoke deployed certificates along with advanced reporting functionality on issued certificates and end entities.





CMS FEATURES AND CAPABILITIES

The Certificate Management Solution provides the infrastructure and processes to quickly create and efficiently manage and distribute certificates across all of your secure entities. It offers:

- Remote and automated certificate enrollment
- Efficient, centralized management of certificates for systems of all sizes
- Robust certificate monitoring and reporting
- Support for the complete certificate lifecycle: creation, issuance, revocation or expiration
- A PKI hierarchy according to your specific needs
- Detailed records maintenance for each device or server and its issued certificate(s)
- Certificate revocation in case of compromised, stolen, or lost devices
- Basic certificate lifecycle management for mobile devices
- "At a glance" system certificate status and reporting via an intuitive user interface
- The ability to sort, view and manage certificates by device, application, group, and validity date

THE CMS ADVANTAGE

- Over the air certificate enrollment (OTA CE)
- Initial setup process has been preconfigured for all applications from Motorola Solutions
- Easier and faster issuing process than standard CAs
- Intuitive general processes and helpful documentation
- Intuitive user experience for ease of use and short learning curve
- Built-in detailed expiration notification
- Easy and intuitive certificate location by device
- Predefined and configurable reports
- Easy and intuitive revocation process
- Accessible live certificate status & details

TECHNICAL SPECIFICATIONS

Infrastructure System	Public Safety R11 and Stand Alone Systems
Supported Applications	Secure VoIP, Secure PTT, VPN, OMA-DM, OSP, Identity Services
Supported Devices	Infrastructure Servers, Windows PCs, VLM, LEX L10 and Android Devices
Security	FIPS 140-2 Level 3 Validated HSM, Common Criteria EAL 4+, FIPS validated crypto libraries
Certificate Management Facility	CMS utilizes a HP DL380 [2x2.5GHZ 64GB 16NIC 2x1.2HD ND] PrimeKey PKI Appliance
OTA CE Compatibility	Android devices (M, N), WAVE 7000, Idm , RSA-2048
OTA CE Requirements	CMF (Version BSR 4.0 or later), PSX Cockpit app on Device (BSR Version 4.0 or later), Android (M, N), Network connection from device to CMF, Camera or Keypad

For more information, please visit:
www.motorolasolutions.com/publicsafetylte

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**