PUBLIC SAFETY NETWORK
TE KUPENGA MARUTAU

Public Safety Network Appendix 4.4 Services Guidelines Device and Application Management

Contents

1. Introduction 3
2. Document Purpose 3
3. Services Scope 3
4. Services Outline 4
   4.1 Approach 4
      4.1.1 Security *5*
      4.1.2 Agile, Cloud and Software as a Service (SaaS) *5*
      4.1.3 User Community *5*
   4.2 Mobile Device Management Service 6
   4.3 Mobile Application Management Service 8
      4.3.1 MAM Features *8*
5. Risks, Issues, Dependencies and Assumptions 8
   5.1 Device and Application Certification 8
   5.2 Application Sourcing 9

Appendix One. MDM and MAM Current State 9

1. Introduction

The Public Safety Network (PSN) programme is an Emergency Services initiative of behalf of Fire and Emergency New Zealand (Fire and Emergency), New Zealand Police (Police), St John New Zealand (St John), and Wellington Free Ambulance (WFA). The PSN programme is tasked with delivering Mission Critical communication services to the Emergency Services sector.

This document should be read in conjunction with the *Appendix 1. Service Requirements* document.

2. Document Purpose

This document is one of a set of Services Guidelines which outlines the network services required for the successful delivery the PSN and should be read as a guide (except where items are specified) for potential suppliers to propose their own solutions for PSN's requirements.

3. Services Scope

This document outlines the required Mobile Device Management (MDM) and Mobile Application Management (MAM) services. These services provide Emergency Services agencies with the ability to access PSN's Digital Land Mobile Radio, Satellite and Cellular Services and the tools to manage user accesses, devices and applications securely in real-time.

The Emergency Services agencies are evolving to data-driven and cloud-based systems and processes. The increase in remote access to information increases the need for mechanisms and systems to ensure data security is maintained as well as provide consistent capability across each agency.

MDM and MAM are key to ensuring the integrity and security of public data and agency data. Agency data includes Emergency Services personnel information as well as incident, public, criminal and medical information. Limiting access to this information is mandatory as is securing emergency services property against inappropriate or unauthorised usage.

Features associated with MDM include:

- Security policy management;
- Data management including ability to containerise, encrypt and secure agency data separately from personal and public data on device;
- Inventory management;
- Deployment management;
- Remote monitoring, management and location verification;
- Remote stun and disable;
- Software management including application and OS version control, as well as, automated patching, business policy configuration and security policy changes;

- Remote configuration and firmware updates;
- Set a regular interval for the device to ‘check in’;
- Report devices that have missed updates and patches;
- Remote Over the Air Re-keying (OTAR); and
- Remote Over the Air Programming (OTAP).

The MAM platform (and its App Store) will enable Emergency Services agencies to control the applications used within their organisation to ensure the latest pre-approved and standardised applications are being utilised and are readily available for a dispersed workforce to deploy. Functionality within the MAM will enable the ability for agencies to control the deployment of new applications to a targeted group of users before a widespread release.

Current agency applications include OnDuty and RSA[1] (security token) for Police, Mobile Device Terminal (MDT) application, Electronic Patient Report forms (ePRF), Clinical Procedures and Guidelines for St John and WFA, and Availability and Messaging System for Fire and Emergency. Applications in the scope of this procurement may include Mission Critical Push-to-Talk (MCPTT). See *Appendix 4.2 Services Guidelines Mission Critical Push-to-Talk (Cellular).* It is anticipated that agencies will develop future applications to leverage the PSN communications capability.

4. Services Outline

4.1 Approach

A process will be required to review devices and applications to ensure they are appropriate for use by Emergency Services, technically work with the PSN communications capability and meet security requirements before they can be made available in the MDM and MAM. The MDM and MAM will be set up to ensure that each agency can only manage and access the devices and applications appropriate to that agency.

The MDM and MAM solutions may be one or multiple solutions, the generic difference being that MDM takes a device approach to securing Emergency Services data and information whilst MAM takes an application approach to these same security requirements. A single MDM platform may not be possible due to the range of devices to support, especially around LMR. If multiple MDM or MAM services are required, access and usage should be, if possible, through a common portal.

Individual agencies will need to manage their own devices, so multi-tenancy is a requirement for the MDM and MAM services. Any multi-agency functions must be explicitly authorised. Service Providers may already have MDM and MAM service offerings which are cloud based, multi-tenanted platforms.

The services may be provided on a shared platform provided that functional, security and availability requirements can be met (including offline management of critical device functions).

Agencies need to be able to manage applications used on Bring Your Own Devices (BYODs) based on device type and security arrangements. This means there is an ability to control

[1] Security token to support remote access to agency enterprise systems.

where and how applications can be deployed in different settings (e.g. corporate devices vs BYOD devices).

MDM and MAM services must have a form of federated identity and access to provide common access policies to any system for simple and straightforward authentication for the agency users. The access management will ensure that changes to existing, adding new or removing exiting users is easily manageable either internally to the agency or via request to the service supplier.

4.1.1 Security

When delivering services via an MDM and MAM, consideration needs to be given to agency security policies that will apply.

Any MDM or MAM solution must comply with agency specific information security and system policies and, where appropriate, any relevant New Zealand Information Security Management (NZISM) and Protection Security Requirement (PSR) guidelines and policies.

Individual agency and government security policies and standards must be followed to ensure that information cannot be intercepted, created, modified or deleted by unauthorised personnel.

See *Appendix 5.5 Functional Guidelines Security and Risk Mitigation*.

4.1.2 Agile, Cloud and Software as a Service (SaaS)

Given the continued Information Communications Technology (ICT) industry acceleration towards SaaS cloud-delivered web apps, and the agile application development that comes with this, finding the balance between updating applications as soon as patches are available, and ensuring a stable platform for Emergency Services' operational needs is critical. The policies available through cloud-based MDM and MAM systems are crucial to the delivery of a reliable frontline service, both in keeping up with functionality and app supportability, and managing the potential instability that can come with agile development. Differing policies by different agencies regarding devices and applications are essential for managing critical applications in this context.

Device software won't always require real-time cloud-based data to operate when internet access is not available, indeed support for offline operation (and data caching) of some apps will be a requirement.

4.1.3 User Community

MDM and MAM systems will require a range of users to access the services for a variety of roles. These roles include but not limited to:

- Information Security;
- Service Desk;
- End Users;
- ICT Administration;
- ICT Testing and Operations;
- Application Development/Deployment; and
- Device Logistics.

4.2 Mobile Device Management Service

MDM should support all cellular devices including feature phones, smartphones, tablets, laptops, in-vehicle routers and specialist devices. At a minimum, operating systems supported should include Android (multiple variants), iOS, Mac OS, and Microsoft Windows. Multiple versions of each operating system will need to be supported. Cellular device management capability will need to include agency supplied and owned devices as well as staff, contractor and volunteer supplied devices (BYOD).

MDM will also need to support devices such as in-vehicle multi-network routers, and these may be provided by suppliers such as Cisco, Sierra Wireless and Nokia. Multiple versions of each device operating system need to be supported.

LMR device management will ensure application software, firmware, calibration files and configuration files are managed and deployed with confidence and accuracy. LMR MDM capability is historically specific to the hardware supplied by the manufacturer. A common MDM supporting multiple LMR terminal devices may not be possible.

Device management for satellite devices is required to manage security policies, asset management and remote configuration.

Any combination of LMR, satellite and Cellular devices will need to be controlled and enabled by MDM.

Secure containers for agency information and applications for shared or personal (BYOD) devices, including for agency specialist devices, should be supported where required.

Mobile, handheld and portable devices need to be regarded as inherently insecure. Emergency Services agencies will need to apply an appropriate level of security using a combination of:

1. Access controls (e.g. passcode access and/or biometrics, balanced against the usability needs of an operational person in stressful or time-constrained situations).
2. Device hardening (e.g. disabling unused services).
3. Device capability (e.g. ability to store data locally or services/applications device can access).
4. Centralised configuration management and Over the Air control (e.g. standardised build and application set, remote disable and wipe capability).
5. Security applications and settings (e.g. end-point protection).

The features and policies expected to be available in the MDM service are listed below, but this is not an exhaustive list:

- All device types:
    - Security policy management;
    - Inventory management;
    - Deployment management;
    - Remote monitoring, management and location verification;
    - Antivirus and malware protection;
    - Remote stun and disable;

- Control device on-boarding and initial configuration;
- Control removal from service, deactivate from network;
- Policy enforcement at multiple levels including:
  - Personal policy: according to corporate environment, highly customisable;
  - Device platform specific: policies for advanced management of Android, iOS, and Microsoft operating system devices;
  - Compliance policies/rules;
- Manage asset inventory;
- Diagnose and troubleshoot equipment remotely;
- Query device status, location, usage and current policy; and
- Manage pre-defined Wi-Fi and hotspot settings (ability to use in LMR context is dependent on network/device)

- Cellular devices:
  - Data management, including ability to containerise, encrypt and secure agency data separately from personal and public data on device;
  - Software management, including application and operating system, version control as well as automated patching, business policy configuration and security policy changes;
  - Push applications and software updates;
  - Report errors from the device;
  - Manage the application catalogue;
  - Provide remote wipe of corporate data;
  - Provide remote wipe of entire device;
  - Provide jailbreak/root detection;
  - Disable native apps on device; and
  - Provide device remote locking
- LMR devices (note MDM decisions for LMR will be impacted by the choice of LMR network and device, and for more information about LMR device management see *Appendix 4.3 Services Guidelines Digital Land Mobile Radio*):
  - Remote stun and disable;
  - Remote configuration and firmware updates;
  - Remote Over the Air Re-keying (OTAR);
  - Remote Over the Air Programming (OTAP);

Some of these functions may also need to be undertaken and controlled directly by agency personnel in the field to ensure changes are made in a secure and timely manner.

4.3 Mobile Application Management Service

The MAM service will manage and provide access to the latest pre-approved and standardised applications for Emergency Services. This includes current applications as well as future applications enabled by the PSN communications capability. The service will present a list of certified applications to mobile devices allowing agencies to safely select from a white list of applications. Application management needs to cover PSN approved applications on agency supplied devices as well as staff, contractors, and third-party (helicopter crews) supplied devices.

The MAM service will need to containerise applications applicable to agency users' login to ensure applications are only visible and available to the appropriate agency staff.

4.3.1 MAM Features

An end-to-end MAM service provides the ability to: control the provisioning, updating and removal of mobile applications, monitor application performance and usage, and remotely wipe data from managed applications. Key features of the MAM service may include, but are not limited to:

- Application delivery (App Store);
- Application updating;
- Application performance monitoring;
- User authentication;
- Crash log reporting;
- User and group access control;
- Application version management;
- Application configuration;
- Push services;
- Reporting and tracking;
- Usage analytics;
- Event management; and
- Application wrapping.

5. Risks, Issues, Dependencies and Assumptions

5.1 Device and Application Certification

For both MDM and MAM, processes and systems will need to be created to review devices and applications to ensure that they will work within the PSN communications capability and can and will be managed by MDM and MAM services. This needs to include devices and applications procured by the PSN Lead Entity, by individual agencies and provided by staff in a BYOD context.

5.2 Application Sourcing

Application sourcing is outside the scope of the procurement activity. Applications will be acquired individually by agencies once the Cellular Services are established. An exception to this will the Mission Critical Push-to-Talk (MCPTT) application.

Appendix One. MDM and MAM Current State

Police currently use Airwatch MDM, provided by Vodafone as part of the Police mobility programme, as both MDM and MAM for cellular devices. Police use the Tait System Management Centre (SMC) for P25 LMR network management, along with device management in conjunction with the Police Service Desk and ICT. This does not include remote programming or keyfill, which is undertaken in the field with designated users and keyfill devices.

Fire and Emergency are investigating Sierra Wireless AirLink Management and Reporting services. Fire and Emergency LMR configuration and ID allocation is managed by in-house resources from technical and operational data teams. Fire and Emergency LMR device configuration and ID allocation on the Police analogue network is managed by in-house technical resources from technical and operational data teams.

St John utilises a combination of both the Sierra Wireless Airlink Management for Communications Hubs in vehicles, and Sophos MDM for the management of cellular devices such as Samsung tablets for Mobile Data Terminals (MDT & e-PRF) and cell phones.

St John and WFA both use the Tait software package ‘Enable Fleet’ for programming and management of Tait 9000 series LMR devices. The software package is maintained by St John and WFA technical resources, and device programming is done manually either by St John or WFA technical resources, along with authorised service agents. All other St John and WFA LMR devices are managed by in-house technical resources.

For WFA, the MDM operation of cellular MDT & e-PRF tablets is undertaken by St John.