Functional requirements in remote Management System

Table of contes

1. General requirements:

- the system allows simultaneous management of devices of many organizations, without mutual access to phones of various organizations (multi-tenancy)
- the system is available as a service, available on contractors dedicated to contracting equipment, hosted in the European Union
- access to the fully web-based system console, also in Polish, English, German
- minimum support for Internet Explorer and Mozilla Firefox browsers
- access to the system for many users, divided into access rights to individual functionalities based on definable roles
- the ability to install the system fully in the company infrastructure
- fail-over system (High Availability)
- full system and application support on mobile phones in Polish, English
- API available for integration with external services / systems via WebService
- support for operating systems (minimum) Android, Windows Mobile, iPhone, Windows Phone, Samsung KNOX
- support for Samsung SAFE extended APIs for Android platforms
- integration with Active Directory, LDAP, MS Exchange and RIM BES servers
- support for the Samsung KNOX solution
- A view of the device list console that is user-definable, along with the visualization of alerts for individual devices
- the system offers all functionalities from one central administration console
- all system functions can be remotely performed on devices from the administration console
- all actions carried out on phones (including application installation,
- configuration, data backup) can be performed on
- single device, on all devices simultaneously or on
- specific group (or multiple groups) of devices - from the console level
- the administrative system
- the ability to access documents stored on company servers from tablets with iOS
- system availability in both the model installed in the internal environment and as a hosted solution
- Integration with SNMP systems
- Integration with the Blackberry Enteprise Server
- Integration with LDAP / AD
- Integration with the Cisco ISE solution, Extreme NAC
- The solution manufacturer must have ISO certificates - at least ISO 9001 and ISO 27001
- The solution manufacturer must have a classified information protection division and a system for processing classified information
- Licensing: the system allows full management of the number of devices specified in the license, it is possible to add unlimited devices at the same time
- Licensing: the number of system users must be unlimited by a license
- The solution must have a built-in VPN client for the Android platform, also operating in the KNOX container, which will allow the use of two factor authentication when establishing a connection, using the second device (eg NFC card, hardware token)
- support for Yubico hardware tokens

2. Requirements for remote configuration:

- support for remote configuration and enrolment without user intervention (including Google Zero Touch, KNOX Mobile Enrollment, KNOX Configure, Apple DEP)
- remote configuration using the OMA DM protocol
- remote configuration using the OMA CP protocol
- remote configuration using the SCEP protocol
- network access configurations, including :
    - internet access points
    - settings of WiFi access points (also based on EAP-TLS)
    - VoIP / SIP settings
    - configuration of e-mail on mobile phones
- the ability to install and configure third-party applications
- the ability to configure the client's internal applications through dedicated integration with the ordering database systems
- the system must provide a Web Service API allowing verification of the correct configuration of the application on the ordering mobile devices
- generating automated and available on-demand reports regarding the activation of the contractor's mobile applications
- grouping configuration for operating systems
- combining the configuration and installation of applications into scripts performed on devices, including the logic embedded in the scripts (the ability to define the interdependencies between individual elements of the script)

3. Application installation requirements:

- installation in silent mode (without user involvement) on devices: any device with Android system version 6 or higher (using Android Work Profile and Device Owner) and iOS (in Supervised mode); additionally (without WP and DO mode on Samsung Android, Huawei Android, Zebra Android, LG Android, Lenovo Android
- preview of installed applications
- creating a whitelist (allowed) application from the Google Play Store
- the ability to silently remove unwanted applications
- remote configuration of the e-mail client
- remote application installation on mobile devices
- the ability to set up an internal store with "corporate appstore" applications
- the ability to configure third-party applications
- Whitelist and blacklist mechanism of allowed and banned applications using the application signature (application signatures)
- the ability to define formats of configuration files - xml or other, allowing to download data from the system and transfer them to mobile applications on the device

4. Security configuration requirements:

- policy configurations for passwords on mobile devices, including:
- defining the requirement to enter the password when starting the device
- defining the complexity of the password (requirement of digits, special characters)
- defining the time of inactivity, followed by automatic blocking forcing the password to be entered

- defining the maximum number of attempts to enter the password followed by the deletion of data from the device
- remote data removal from the device in the event of its loss
- the option of blocking a factory reset on a mobile device tethering (hot-spot)
- remote blocking of the device
- displaying a message to the "finder" in the case of blocking the device, remote device restart
- remote control over the screen and keyboard of the device
- cyclical generation of a backup copy of data
- the ability to block some of the functions of the phone (eg Camera, web browser, bluetooth connectivity)
- blocking the user's ability to install the application
- defining a black list of applications that can not be used by phone users
- blocking the ability of users to edit the settings of the phone
- cooperation with an antivirus solution to detect malware on mobile devices
- integration with Windows CA to fully manage the lifecycle of certificates on mobile devices
- CA server built into the solution to fully manage the lifecycle of certificates on mobile devices without the need for external integration
- the ability to configure and install s / mime certificates on devices
- integration with the Samsung Enterprise FOTA solution to control the firmware version on mobile devices
- management of Bluetooth profiles for Samsung devices
- the ability to remotely change the PIN code of the SIM card in such a way that the user does not know the PIN code (so that when inserted into a device other than the managed one, the SIM card is unusable)

5. Requirements for the separation of company and user data:

- support for Samsung KNOX version 2.0
- support for the Android Enteprise solution
- support for dual APN functionality that allows the use of separate Internet access points for company data (container) and private data
- the possibility of using multiple KNOX licenses within one organization
- the ability to remotely lock and unlock the company data container
- the ability to remotely delete a company data container

6. Requirements for geolocation functionalities:

- location of phones based on GPS data
- location of telephones using the operator base station ID (BTS)
- polling for location on demand
- polling for a location in a continuous mode, with the possibility of defining intervals depending on:
- changing locations for a specific distance
- configurable time interval
- changing the ID of the base station in which the mobile phone is located
- data visualization on the map
- the ability to export the history of location data to a file

7. Requirements for remote support for mobile phones:

- functionality of remote access to the screen and phone keypad, at least for Android, Symbian, Windows Mobile and RIM BlackBerry platforms
- the ability to configure the image quality sent to the server during a remote access session, in order to adjust the amount of data transferred to the network conditions in which the mobile device is located
- the ability to view the device in live mode
- the ability to manage files on a mobile device

8. Additional requirements:

- availability of the Self-Care portal for end users
- the possibility of installing the PKCS12 certificate by the user's portal in order to configure the mail encryption (SMIME) in the KNOX container and the native iOS container
- API availability to integrate third-party solutions with the MDM system
- the ability to operate in a fully enclosed environment (without access to the Internet, in particular to Google, Amazon etc. service providers)
- the availability of procedures for auditing the source code of the solution (in order to verify the security of the solution)
- integration with a comprehensive solution for data backup and data collaboration
- solution enabling verification of the status and degree of policy compliance by a given mobile device by third-party solutions