RFP 56 - MEG Security Use Cases and Requirements

Draft

15 Pages

Abstract

The adoption of the OSGi platform for mobile devices, driven by MEG, poses new challenges in security area. This document provides leading use cases and requirements in this area.

0 Document Information

0.1 Table of Contents

All Page Within This Box

0.2 Terminology and Document Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY" and "OPTIONAL" in this document are to be interpreted as described in [1].

`Source code is shown in this typeface.`

0.3 Revision History

The last named individual in this history is currently responsible for this document.

Revision	Date	Comments
Initial	March 12 2004	Initial version for discussion inside the work stream Piotr Cofta, Nokia, piotr.cofta@nokia.com
0.1	March 18 2004	Use cases edited, requirements ready to be discussed Piotr Cofta, Nokia, piotr.cofta@nokia.com
0.2	March 23 2004	'mail' use case added; extensive changes to requirements Piotr Cofta, Nokia, piotr.cofta@nokia.com
0.3	March 25 2004	Final cleaning, release Piotr Cofta, Nokia, piotr.cofta@nokia.com
0.9	23 Apr. 2004	BJ Hargrave, hargrave@us.ibm.com Formatted for external review.

1 Introduction

This document is the result of the activity in the OSGi Mobile Expert Group (MEG) Security Work stream. The document describes use cases and requirements related to various aspects of security within the scope of MEG.

2 Application Domain

The purpose of MEG is to bring OSGi solutions to the world of mobile devices. The nature of the mobile domain differs in several places from what has been usually considered to be the scope of OSGi. This unique nature creates significant new challenges regarding the security. Following is the list of most important differences from the security perspective.

- Small form factor. The mobile device is usually designed to be hand-held, with limited memory, processing capabilities and battery life.
- Personal usage. The mobile device is carried, used and operated by the single person in a variety of environments.
- Smart cards. SIM cards are ubiquitous in GSM-compliant devices while higher-end devices allows for memory cards.
- MIDP. There is the existing solution for Java applications with its own security intrinsic.

The security work stream focuses on defining security-related features that can be used by other work streams to support their respective use cases. As such, the security work stream addresses the disperse variety of security-related use cases and requirements. Some of those requirements are specific to the security itself while several others can be addressed within other work streams.

3 Problem Description

It is the desire for OSGi MEG to deliver the solution that is both functional and secure. Even though OSGi provided solid foundation for security, the mobile domain creates new challenges that should be addressed.

Referring to the taxonomy of differences from the previous chapters, some problems are listed below.

- Small form factor. Limited computational capability and restricted memory size prevent security solutions that are resource-hungry. Specifically solutions that do not scale up well are likely to be problematic. Further, resource-consuming cryptographic operations should be designed in the optimal way.

- Personal usage. The different, personal, usage pattern of the device may allow for the simple user model. At the same time the usability of security is of enormous importance.

- Smart cards. SIM and storage cards add another dimension to the dynamics of the environment of the application. Cards can be removed, modified or changed during the life of an application, resulting in changes in the application's status.

- MIDP. Security solutions provided by MEG to support MIDlets must be backward compatible with MIDP2.0.

It is evident that without addressing those issues MEG cannot reliably provide the solution for the mobile application domain.

4 Use Cases

Following is the list of security-related use cases. Most of those use cases contribute also to other work streams' domains. However, it is the security aspect of such use cases that is of the primary concern of the security work stream.

4.1 Device theft

Mobile devices are lightweight and attractive enough to fell prey to thieves or they can be simply left over by mistake. In either case the mobile device can be inspected and the content of its memories can be revealed.

Private users can be concerned with the loss of pictures, ringing tones or a list of contacts. Convenience and privacy are main concerns here while the possibility of illegitimately obtaining telecommunication services is the main financial issue. Enterprises however are likely to store important information into the device so that the disclosure of such information may cause damage to the business or it may facilitate other, more violent forms of attacks. Specifically, credentials (private cryptographic keys, passwords, access codes), if stored in the mobile

terminal, may enable access to the corporate infrastructure. Further, applications (that can be considered another form of data) may require similar protection.

Existing methods to protect data in the mobile device is designed to protect the private user. SIM can be blocked preventing the abuse of the account, but there are no methods to protect e.g. the phone book or the short message inbox.

4.1.1 Theft of locked device

Actors	User, thief
Preconditions	The device is operational. The device is turned off, or the user locked the device (if such mechanism exists)
Scenario	The device is stolen from its user. The thief powers-up the device in order to access data. The device requests certain access code (password). The thief cannot correctly guess the password and is locked-out from the device.
Post-conditions	Device may be non-operational but data is not leaked to the thief.

4.1.2 Theft of operational device

Actors	User, thief
Preconditions	The device is operational. If necessary, the user is logged in.
Scenario	The thief steals the device. The device times-out while being stolen and requires re-authentication. The thief cannot correctly guess the password and is locked-out from the device.
Post-conditions	Device may be non-operational but data is not leaked to the thief.

4.1.3 Theft of the component of the device

Actors	User, thief
Preconditions	The device is operational. If necessary, the user is logged in.
Scenario	The user leaves the device unattended. The device is intercepted by the thief who removes the memory card from the device. The user does not notice the theft (until much later). The thief is able to access information stored on the card. The information, if sensitive, is encrypted by the application that is using available tools and services.
Post-conditions	Data is possibly lost, but no data is compromised.

4.2 Users and applications

Mobile devices are generally designed for the personal use, similarly to desktop computers years ago. Consequently, there is no notion of multiple users in the whole device architecture. For example, SIM-based authentication (PIN) in GSM networks provides the guarantee that only the valid user can activate the device. Lesser known features of SIM authentication allow the user to access additional functions by presenting another credential (PIN2).

Use cases presented below explore whether such user authentication and authorisation is sufficient for the MEG application domain.

4.2.1 User authentication to the device

Actors	User, administrator
Preconditions	The device is configured. Method to authenticate the user is established and provisioned by the administrator.
Scenario	The user attempts to use the device, e.g. to run the application that is responsible for order tracking. The device asks the user for the credential (e.g. the code). The user supplies the proper code. The device provides the required functionality.
Post-conditions	The user gets access to the desired functionality.

4.2.2 Access with no authentication

Actors	User, administrator
Preconditions	The device is configured. Method to authenticate the user is established and provisioned by the administrator.
Scenario	The user attempts to use the device for certain simple function, e.g. to check the current date/time. The use of such function is allowed for everybody. The user can simply pick the device and use the required function. No authentication is needed.
Post-conditions	The user gets limited access to the device.

4.2.3 Use of function that requires more rights

Actors	User
Preconditions	The device is configured. Method to authenticate the user is established and provisioned by the administrator. The person has already authenticated to the device as a regular user.
Scenario	The person attempts to execute function that requires special rights (e.g. the device management function). The person is asked by the device whether he has credential to log-in as more powerful user, e.g. to provide the proper password/code. The device guides the user through the process. The person provides the password and becomes the powerful user.
Post-conditions	The function is executed.

4.3 Signature

The mobile device is perfectly suited to store sensitive personal information, such as private cryptographic keys. There are established methods to use such keys for the purpose of digital signing of documents. Such signature in several jurisdictions is legally binding. Another usage is to remotely authenticate the user or the device. Both cases are sensitive from the security perspective. Further, the device can be used to verify sensitive information delivered to it.

4.3.1 Signing the document

Actors	User
Preconditions	The device is operational and is provisioned with private keys (e.g. in SWIM). The application has the document (e.g. text) that should be digitally signed.
Scenario	The document is displayed for the user.. The user verifies the content of the document and is able to verify the origin of the request. To sign, the user provides a PIN. Cryptographic operations are performed to generate the digital signature.
Post-conditions	The digital signature of the document is available.

4.3.2 Authentication to a remote device or server

Actors	User
Preconditions	The device is operational and is provisioned with private keys (e.g. in SWIM). The application received the challenge, possibly in binary format, from another device or from the server.
Scenario	The user is asked to provide PIN. The user verifies the origin of the request and provides the PIN. Cryptographic operations are performed to generate the digital signature that produces the response.
Post-conditions	The response is available to the application.

4.3.3 PIN/password interception

Actors	User
Preconditions	The user is asked to provide PIN
Scenario	The verification of the origin of the request reveals that such request has been issued by the application that is not entitled to do it. The user rejects the request and contacts the corporate security.
Post-conditions	The security of the device is not compromised.

4.3.4 Signature verification

Actors	User, sender
Preconditions	The sender has sent the mail to the device. The mail is signed with the private key of the sender. The device is in the possession of the matching public key.
Scenario	The mail application receives the message. The mail application verifies positively the authenticity of the message by checking the signature against the known public key, using available functions. The mail application informs the user about the outcome of the verification.
Post-conditions	The user is reassured about the authenticity of the message.

All Page Within This Box

4.4 Application control

OSGi makes extensive use of the Java concept of permission-based sandbox where different applications are granted different sets of permissions that allow them to perform functions they are otherwise not entitled to. MEG is likely to make use of the same mechanism.

This set of use cases explores whether the notion of permissions is sufficient for MEG and what are the cases that need special attention.

4.4.1 Trusted applications

Actors	Application issuers, administrator
Preconditions	The device is provisioned by the administrator so that applications may be granted different permissions depending on the application issuer.
Scenario	Two applications are installed into the device, coming from two different application issuers: one that is trusted and another one that is not trusted. Both applications request certain function that has the permission-controlled access (e.g. access to the particular file).
Post-conditions	One application is granted the access while another is denied it.

4.4.2 SIM-based certificates

Actors	Administrator, operators
Preconditions	An administrator has provisioned the device so that permissions of the particular code are tied to the signature that is verified by the certificate stored on SIM. The certificate is provided by the operator. The application that uses the code is operational. The code has the necessary permissions.
Scenario	The application is paused and the device is unpowered. SIM is replaced and the new SIM (that possibly comes from another operator) does not have the required certificate. The device is powered and the application is restarted.
Post-conditions	The code does not have permissions.

4.4.3 Awareness of the current user

Actors	Administrator, user
Preconditions	The device has an application. The device has been provisioned by the administrator so that it can authenticate the user. The user has already been authenticated.
Scenario	The application is aware that certain sensitive function can be executed only if the user is properly authenticated. The application verifies whether the user is authenticated. As the user has presented proper credentials, the application proceeds with the function.
Post-conditions	The function is performed.

4.4.4 MIDP2.0 compatibility

Actors	User, developer, manufacturer, operator, trusted third party, untrusted party.

Preconditions	The MIDlet that is MIDP2.0 compliant is deployed to the device by the operator, manufacturer, trusted third party or untrusted party. The device provides MIDP2.0 support.
Scenario	The MIDlet uses several features that have permission-based access under MIDP2.0. The behaviour of the MIDlet within the MEG environment is indistinguishable from the behaviour in MIDP2.0 environment for both the user and the developer.
Post-conditions	The MIDlet performs as expected.

4.4.5 Hostile application

Actors	Two applications
Preconditions	Two MEG-compliant applications are installed on the device. The first application performs its functions correctly. The second application is the hostile one.
Scenario	The second application (either incidentally or intentionally) attempts to access files that are normally used by the first application. The hostile application issues the file open request. Such request is verified whether the application has rights to access the file. As such rights are not granted, the access is denied.
Post-conditions	No harm to the first application.

4.5 Server compatibility

The application itself requires access to security features provided by the mobile device. Such access may take on different forms, whether algorithms are openly exposed in the form of crypto-API or they are embedded in the implementation of more complex services, again available to applications through certain APIs.

The non-exhaustive list of such services is as follows:

- Access to secure communication protocols (e.g. SSL, TLS, IPv6, VPN),
- Integration with a Secure Element (e.g. smart card) e.g. to support protocols or to provide secure storage,
- Use of hardware-supported security (crypto-processors, secure storage etc),
- Cryptographic libraries that allow applications to combine existing algorithms into desired schemes,
- Support for data formats used in security (e.g. XML-based signatures),
- Key storage on the platform.

Note that currently the application already has access to several security-related features and the number of such features is growing all the time. Enterprises, however, may have needs that are different from the consumer market. MEG should verify how to best satisfy those specific needs.

Even though MEG is focused on the mobile device, yet there is a counterpart of the device - the infrastructure. Enterprises have been investing in the infrastructure for a long time. The current trend of standardising solutions around web services and XML applies mostly to new deployments. Several businesses are unwilling or unable to pursue this path, setting for gradual upgrade instead. Therefore the existing infrastructure, including all the security standards represents the legacy that the mobile device should adapt to.

This set of use cases briefly explores situations where the infrastructure uses the security protocol that is incompatible with any standard one or where the actual bearer does not have any security protocol.

4.5.1 Legacy protocol

Actors	Device, server
Preconditions	The company is already using the security protocol to protect access to its infrastructure. The protocol includes server authentication and bulk symmetric encryption. The bearer is HTTP, but the format of the protocol differs from HTTPS. The application attempts to communicate with the server.
Scenario	The application uses the selection of cryptographic algorithms to handle the desired protocol.
Post-conditions	The application can communicate with the server.

4.5.2 Specific bearer

Actors	Applications (application issuers) on two devices
Preconditions	The application on one device attempts to securely communicate with another application at another device over SMS. Both applications share the common secret that can be used to encrypt/decrypt the message.
Scenario	The first application generates the message. As there is no secure protocol over SMS, the application uses symmetric key algorithms (e.g. DES) to encrypt the message. The encrypted message is sent to another application that is able to decrypt the message.
Post-conditions	The applications can communicate with each other.

4.6 Data lifecycle

The useful lifetime of the mobile device on the consumer market is relatively short and it may be so for the enterprise market as well. Therefore the upgrade of the mobile device will happen quite often. The discontinuity in security protection introduced by device upgrade should be addressed by MEG.

Making data backup is the routine process for desktop applications and fixed networks and such practice will definitely expand to cover mobile devices and wireless networks. The backup represents another discontinuity in the data lifetime that should be addressed by MEG.

As the device reaches the end of its useful life it is frequently passed down the chain, to less demanding tasks or otherwise it is moved out from its user. Having the relatively low market value, such device may be treated as scrap and may end up in an arbitrary place, out of control. This may easily lead to data scavenging where valuable data is extracted from the end-of-life device.

4.6.1 Device upgrade

Actors	User, serviceman
Preconditions	The old device is about to be upgraded. The new device is already provisioned with all the relevant applications, but application data resident in the old device must be moved to the new one.

Scenario	The old device is left in the service point. The user receives the new device and drives to the meeting. On the way, the new device is provisioned with data removed from the old one while data is removed from the old device. The secure communication between both devices is provided.
Post-conditions	The new device is fully operational with correct data. The old device does not have application data.

4.6.2 Backup/restore

Actors	User
Preconditions	The user runs the regular backup of data stored in the device. The backup device is the multimedia card that is plugged into the device. The backup is encrypted for security reasons. The device has been broken and the user has received the replacement.
Scenario	The user loads the multimedia card into the new device and performs data restore. Even though the card is loaded into a different device, the restore operation succeeds.
Post-conditions	The replacement device is operational with correct application data.

4.6.3 End of life

Actors	Serviceman
Preconditions	The device has reached end of its life. Application data has been already moved to the new device and applications have been removed.
Scenario	The serviceman activates the function that cleans all the data storages that do not belong to any application, e.g. data cache.
Post-conditions	The device does not contain any data.

4.6.4 SIM access

Actors	Applications (device, SIM), user
Preconditions	The application is installed on the device with proper permissions. SIM that is fitted into the device contains card application that can be used by the device application to store and process sensitive information.
Scenario	The application is accessing SIM. Such action is protected by permissions. As the application has the needed permissions, the access is granted. If SIM requires PIN, such PIN can be securely provided by the user.
Post-conditions	The application successfully executes

5 Requirements

Following is the list of technical requirements for the security work stream. Requirements are grouped by use cases, but such grouping is not expected to be definitive as one requirement may satisfy more then one use case.

5.1 User

REQ-SEC-01-01. MEG MUST provide support for the concept of the user authentication/authorisation for the personal use of the device.

REQ-SEC-01-02. MEG MUST provide the lock-out mechanism where the user is locked out from the device after the certain period of inactivity or at the user's request. Such lock-out is equivalent to changing the user to the anonymous one.

REQ-SEC-01-03. The application is responsible to verify user's rights before proceeding. MEG MUST provide services for applications to decide whether to proceed depending on the user authentication.

REQ-SEC-01-04. MEG MUST be able to use the notion of the user in several contexts without frequently asking the user for additional authentication (single log-in).

REQ-SEC-01-05. MEG MUST provide methods for the management agent to provision and manage user-related information on the device.

REQ-SEC-01-06. MEG SHOULD provide a simple method that allow the user to gain access to sensitive functions of applications that require another log-in.

REQ-SEC-01-07. The device MUST be configurable so that certain functions can be accessible to unauthenticated (anonymous) user.

5.2 Signature

REQ-SEC-02-01. MEG MUST provide access to digital signature for the purpose of document signing and remote authentication if such functionality is supported by the device (private key storage).

REQ-SEC-02-02. MEG SHOULD provide means to support trusted dialogue to prevent PIN/password interception. The user SHOULD be able to distinguish between trusted dialogue and regular interaction.

REQ-SEC-02-03. MEG SHOULD provide functions for public-key based signature verification.

5.3 Permissions

REQ-SEC-03-01. MEG MUST provide mechanism where different applications (or software components) are granted different set of rights (permissions).

REQ-SEC-03-02. MEG SHOULD use mechanisms where applications or software components can be granted different rights depending on at least its origin (location) and the identity of the issuer (signature) of such components.

REQ-SEC-03-03. MEG SHOULD provide the mechanism where the change in policy or in conditions propagate to actual permissions (e.g. SIM change).

REQ-SEC-03-04. MEG MUST provide security model compatible with MIDP2.0 for supported MIDlets.

5.4 Data

REQ-SEC-04-01. MEG SHOULD provide means for applications to securely keep selected confidential information in the device.

REQ-SEC-04-02. MEG SHOULD provide support for secure device upgrade.

REQ-SEC-04-03. MEG SHOULD provide support for secure backup and restore.

REQ-SEC-04-04. MEG SHOULD provide support for secure disposal of the device.

REQ-SEC-04-05. MEG SHOULD provide means for applications so that data stored in the removable storage is protected (e.g. encrypted) while it is usable at least on the original mobile device.

REQ-SEC-04-06. MEG MUST provide access to SIM/smart cards if they are supported by the device

5.5 Compatibility

REQ-SEC-05-01. MEG MUST provide access to the wide selection of standard security building blocks.

REQ-SEC-05-02. MEG SHOULD provide methods to integrate support for security features available on the platform (e.g. crypto co-processor, TCG chip etc).

REQ-SEC-05-03. MEG SHOULD integrate smart cards (e.g. SIM) into its own security model whenever appropriate.

5.6 Performance

REQ-SEC-07-01. Security solutions MUST be lightweight in terms of performance and usability.

REQ-SEC-07-02. MEG SHOULD encourage to re-use storages, identities, certificate systems, implementations and concepts that are already present on the mobile device, assuming that they fit the purpose of MEG

REQ-SEC-07-03. MEG SHOULD withstand certain attacks from other MEG applications.

6 Document Support

6.1 References

[1]. Bradner, S., Key words for use in RFCs to Indicate Requirement Levels, RFC2119, March 1997.

[2]. Software Requirements & Specifications. Michael Jackson. ISBN 0-201-87712-0

6.2 Author's Address

Name	Piotr Cofta
Company	Nokia
Address	Itamerenkatu 11-13, 00180 Helsinki, Finland
Voice	+358 50 4820702
e-mail	piotr.cofta@nokia.com

6.3 Acronyms and Abbreviations

GSM	Global System for Mobile communication
MEG	The functionality defined by MEG on top of, or in association with OSGi, whether in a form of a separate framework, additional bundles or otherwise
MIDP	Mobile Information Device Profile. If not qualified, MIDP refers to MIDP2.0 as specified by JSR118.
PIN	Personal Identification Number, the code used to gain access to various functions
SIM	Subscriber Identity Module

6.4 End of Document

All Page Within This Box