RFP 55 - MEG Policy

Draft

16 Pages

Abstract

This document contains use cases/requirements for the Mobile Expert Group’s Policy track.

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].

0.3 Revision History

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

Revision	Date	Comments
Initial	Jan 22 2004	Initial Draft. Mark Hansen, Motorola, mark.hansen@motorola.com
0.1	Jan 27 2004	Nokia requitements added Introduction, Application Domain, Problem description added Gabor Paller, Nokia, gabor.paller@nokia.com
0.2	Feb 4, 2004	Two basic use cases added Comments from the Jan. 30 phone conference addressed Gabor Paller, Nokia, gabor.paller@nokia.com
0.3	March 1, 2004	Operator- and device characteristic-related use cases/requirements added Terminology update and review comments integrated. Gabor Paller, Nokia, gabor.paller@nokia.com
0.4	March 5, 2004	Comments from the March 5. call integrated Gabor Paller, Nokia, gabor.paller@nokia.com
0.5	March 29, 2004	Comments from the March 26. call integrated Gabor Paller, Nokia, gabor.paller@nokia.com

Revision	Date	Comments
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) Policy Work stream. The document describes use cases and requirements related to MEG's Application Model, Device Management and Deployment work streams.

2 Application Domain

The following terminology is used in this document:

Action – Operation protected by the policy. The action is accomplished by a subject on a resource.

Administrator – user of the device management server launching remote management operations

Application – one or more bundle realizing a complex functionality

Application environment – An OSGi framework, a MEG-specific extension of the OSGi framework or a MIDP environment

Bundle – Basic element of the OSGi application model

Condition – The policy rule referring to a certain subject, action and resource is applied only if the condition part is evaluated to true. The condition part is optional.

Key performance indicator, KPI – Application-specific monitoring variable that the application publishes through the management system in order to allow its status to be examined.

Management system – subsystem which is responsible of carrying out management actions coming from local or remote management actors.

OMA DM – Open Mobile Alliance Device Management framework

Policy – Set of rules controlling permissions in the system

Privilege - A right to a definable action that can be granted to subjects

Resource – target of the subject’s actions. A policy rule states whether a certain subject is allowed to do a certain action on a certain resource

Rule – rule expresses the following statement: subject can do action on resource with conditions

Signer – Entity that creates digital signatures. The signer has a private-public key pair and the public key is available when the signature is verified.

Software component – application or bundle

Subject – Subject of the policy rule, a subject is allowed to do certain actions and is under the control of the policy rules

Unit of Delivery - A collection of OSGi entities used by the management system to deliver an application to the device, but not necessarily known to the OSGi framework.

Unit of Deployment - An OSGi artifact associated with the minimal, separately deployable entity, which is currently associated with an OSGi bundle.

Unit of Execution - an OSGi artifact associated with its own execution context

User – End user of the device. Depending on the device policy, end user may also have access to management functionality over a local API.

Security concerns are always important in case of management systems. This is related to the power of the operations available on the management interface. It is important therefore that the rules, which actor can launch what management operation are described in a clear, flexible and manageable way. The collection of these rules (or permissions) is called policy.

We have multiple actors in the system envisioned by the OSGi MEG activity. Management operations can be launched remotely, from management servers (where different management servers may have different policy associated to them) or locally by applications or end users. We also expect the policy rules to be very different in different usage scenarios depending on the ownership of the device, the mobile operator’s business model, the subscription plan, the corporate security policy, etc.

3 Problem Description

OSGi MEG envisions a system where the operation of the system can be described flexibly. The policy affects the system in the following ways:

- Policy controls the management system. When an administrator or an application having management rights tries to launch a management operation (either locally or remotely) the policy system is consulted and the management operation is accepted/rejected based on the policy decision.
- Policy controls the running applications. When an application wants to execute a privileged operation, the policy system is consulted and the operation is executed/rejected based on the policy decision.

OSGi itself has a policy system. The goal of the work stream is to identify requirements that the existing OSGi policy system does not satisfy.

The scope of this document is restricted to the requirements against the rules that the policy system is able to describe. Enforcement and management of these rules (the policy) is out of the scope of the work stream's activity.

4 Use Cases

4.1 Policy controls the management system

Use Case	Policy controls management action
Actor(s)	Management actor, management system, policy subsystem
Preconditions	The management actor connected to the management system successfully
Description	The management actor sends a management operation to the management system. The management system contacts the policy subsystem. The policy subsystem checks the circumstances of the management operation (initiating actor, target resource, other conditions, etc.) against the policy store and accept/reject policy decision is made. Based on the decision, the management operation is carried out or is rejected.
Exceptions	• The policy store cannot be accessed or the policy subsystem is not working properly. In this case the management operation is always rejected and appropriate status code is returned to the initiator of the management operation.

Post conditions	• The management operation is carried out or rejected • Status is available

4.2 Policy controls the runtime behavior of applications

Use Case	Policy controls runtime behaviour
Actor(s)	UE, trusted UDP, policy subsystem
Preconditions	UE has been started successfully.
Description	UE is running and is executing a sensitive operation that is protected by policy. The trusted UDP that the application called makes sure that the policy subsystem is contacted and policy is checked. Based on the policy decision, the sensitive operation is executed or rejected. The calling application is able to determine if the operation was executed or rejected.
Exceptions	• The policy store cannot be accessed or the policy subsystem is not working properly. In this case the execution of the trusted operation is always rejected and appropriate status code is returned to the calling UE.
Post conditions	• The sensitive operation is carried out or rejected • Status is available

4.3 Delegation

Use Case	Delegation of rights
Actor(s)	Management actor, management subsystem, policy subsystem
Preconditions	• The management actor connected to the management system successfully • The management actor owns the right that it wants to delegate and it also has a right to delegate it to the other management actor.
Description	The phone is used by an employee of company ACME as business tool. The operator owns the device and retains privileges to the most sensitive actions to itself. The operator delegates privileges to the corporation ACME to install corporate applications and to give these applications sufficient privileges. So we are having two server side management parties and two associated management agents on the device. The first management agent has absolute "root"-like privileges. The first management agent delegated part of its privileges to the second management agent. The exact process flow is the following: the management actor owns a right and would like to grant this right or an exact subset of this right to another management actor. In order to do this, the management actor executes a delegation management operation. The delegation operation is controlled by the policy. The initiating management actor must have right to delegate the particular right to the other management actor. During the delegation operation the policy subsystem is contacted first to check whether the initiating management actor owns all the necessary rights to execute the operation
Exceptions	• The policy store cannot be accessed or the policy subsystem is not working properly. In this case the delegation operation is always rejected and appropriate status code is returned to the initiating management actor.

All Page Within This Box

Post conditions	- The policy database is updated appropriately.

4.4 Policy tied to operator- or device characteristic

Use Case	Policy tied to operator- or device characteristic
Actor(s)	Administrator, User
Preconditions	Administrator has set up policy for the device. Some (or all) the policy rules are tied to some characteristic of the smart card identification module (like IMSI in the SIM card).
Description	The User removes the smart card identification module from the device or changes its subscription by some other mean in case the wireless network doesn’t use smart card identification module. As a consequence, policy rules tied to the characteristic of subscription (like IMSI on the smart card) don't apply anymore. The applications controlled by these policy rules will not be accessible.
Exceptions	None
Post conditions	User cannot access the applications that were protected by the policy settings tied to the characteristic on the smart card.

5 Requirements

Note that MUST, SHOULD or MAY words are used in policy requirements so that they depend on the implementation of the feature. For example if MUST is used in the KPI-related section, it means that the requirement is mandatory to support if the KPI feature is implemented and it doesn’t mean that the KPI feature itself is mandatory.

5.1 Granularity of Privileges

REQ-POL-01-01. The policy framework MUST support privileges at UDP level.

REQ-POL-01-02. The policy framework MUST support privileges at the service level. Standard OSGi service permissions are used.

REQ-POL-01-03. The policy framework MUST support privileges to specific functions (i.e. APIs)

REQ-POL-01-04. The policy framework MAY support privileges to specific functions coupled with arguments of strings to wildcards.

5.2 Subject Designation

REQ-POL-02-01. It MUST be possible to use management server as subject.

REQ-POL-02-02. End user MAY be supported as policy subject.

REQ-POL-02-03. An individual UDP MUST be supported as policy subject.

REQ-POL-02-04. UDL MAY be supported as policy subject.

REQ-POL-02-05. An UDP signer's identity MUST be supported as a policy subject.

REQ-POL-02-06. UE MAY be supported as policy subject.

5.3 Access Privileges

REQ-POL-03-01. The policy framework MUST support granting access privileges according to source.

REQ-POL-03-03. The policy framework MUST support granting access privileges according to an identity associated with the subject.

REQ-POL-03-04. The policy framework MAY support subject granting of privileges they possess to other subjects (delegation).

REQ-POL-03-05. The policy framework MUST support granting access privileges based upon user approval.

REQ-POL-03-06. The policy framework MUST support dynamic updating of a policy by privileged applications and services.

5.4 Privileges

REQ-POL-04-01. A policy rule MUST be available to allow the launch of UEs immediately.

REQ-POL-04-02. A policy rule MUST be available to allow the launch of UEs at a preset time.

REQ-POL-04-03. A policy rule MUST be available to allow the launch of UEs when driven by an event.

REQ-POL-04-04. A policy rule MUST be available that are associated with UE and UDP lifecycle operations.

REQ-POL-04-05. A policy rule MUST be available to allow UEs and services to publish events.

REQ-POL-04-06: A policy rule MUST be available to allow UEs and services to receive events without consuming them.

REQ-POL-04-07. A policy rule MUST be available for controlling access to UEs that act as handlers for content, which must be granular to the specific MIME types handled.

REQ-POL-04-08. A policy rule MUST be available to allow UEs and services to update policies.

5.5 Programmatic Interface

REQ-POL-05-01. The policy framework MUST support programmatic checking of privileges.

REQ-POL-05-02. The policy framework MUST have a means of querying assigned permissions associated with a given location.

REQ-POL-05-03. The policy framework MUST have a means of querying default permissions associated with a given location.

REQ-POL-05-04. The policy framework MUST have a means of setting permissions for a specific location.

REQ-POL-05-05. The policy framework MUST have a means of setting default permissions for a specific location.

REQ-POL-05-06. The policy framework MUST allow the policy to be updated dynamically.

REQ-POL-05-07. The policy framework MUST allow the policy to be updated incrementally through the addition of an individual policy entry.

REQ-POL-05-08. The policy framework MUST allow the policy to be updated incrementally through the deletion of an individual policy entry.

5.6 Policy requirements for install and update action

REQ-POL-06-01. The subject of the install/update action MUST be management server, UE, UDP or end user.

REQ-POL-06-02 The subject of the install/update action MAY be UDL.

REQ-POL-06-03. The resource of the install/update action MUST be the name of the UE or UDP

REQ-POL-06-04. The resource of the install/update action MAY be the name of the UDL

REQ-POL-06-05. It MUST be possible to restrict the cost incurred by the install/update action by policy. *For example it is possible to state that expensive wireless network cannot be used for the install action.*

REQ-POL-06-06. It MUST be possible to use the signer or the codebase of the UDP as policy condition. *For example it is possible to state that anybody can install any UDP that is signed by company X. This is not the same statement as "any UDP signed by company X can launch an install action"*

REQ-POL-06-07. It MAY be possible to use the signer of the UDL as policy condition.

REQ-POL-06-08. It MUST be possible to describe that user must be prompted for confirmation as policy condition. If the policy rule matches, the user will be prompted for confirmation and the action is executed only if the user accepted the operation.

REQ-POL-06-09. It MAY be possible to describe, what native platform rights are granted for the application. The application may contain native components. Native components may declare what platform rights they require. The required rights of the native component are compared with the policy and if the embedded native component requires more right than allowed by the policy, installation is refused. *This feature is meaningful only if the native platform has some kind of policy mechanism of its own.*

All Page Within This Box

5.7 Policy requirements for uninstall action

REQ-POL-07-01. The subject of the uninstall action MUST be management server, UDP, UE or end user.

REQ-POL-07-02. The subject of the uninstall action MAY be UDL.

REQ-POL-07-03. The resource of the uninstall action MUST be the name of UE or UDP

REQ-POL-07-04. The resource of the uninstall action MAY be the name of UDL

REQ-POL-07-05. It MUST be possible to describe that user must be prompted for confirmation as policy condition. If the policy rule matches, the user will be prompted for confirmation and the action is executed only if the user accepted the operation.

5.8 Policy requirements for inventory query action

REQ-POL-08-01. The subject of the inventory query action MUST be management server, UDP, UE or end user.

REQ-POL-08-02. The subject of the inventory query action MAY be UDL.

REQ-POL-08-03. The resource of the inventory query action MUST be the name of UE or UDP whose inventory information is queried.

REQ-POL-08-04. The resource of the inventory query action MAY be UDL.

REQ-POL-08-05. It MUST be possible to define wildcards in the resource section so that the all items in the inventory or more items in the inventory can be used as resource.

5.9 Policy requirements for policy management

REQ-POL-09-01. It MUST be possible to describe rights for full policy overwrite operation

REQ-POL-09-02. The subject of the policy overwrite action MUST be management server or end user.

REQ-POL-09-03. The resource of the full policy overwrite operation is implied, it refers to the whole policy store.

REQ-POL-09-04. It MAY be possible to describe rights for policy delegation operation. *For example the end user can delegate an installation right if the end user owns the installation right and also has right to delegate that right.*

REQ-POL-09-05. The subject of the delegation action MUST be management server, UDP, UE or end user.

REQ-POL-09-06. The subject of the delegation action MAY be UDL.

REQ-POL-09-07. The resource of the delegation action MUST be the combination of the subject to delegate the right to, the action for which the right is delegated and the resource on which the right is delegated. *For example it is possible to delegate the installation right to the end user on a certain application.*

REQ-POL-09-08. It MUST be possible to describe rights for the policy query

REQ-POL-09-09. The subject of the policy query MUST be management server, UDP, UE or end user.

REQ-POL-09-10. The subject of the policy query MAY be UDL.

REQ-POL-09-11. The resource of the policy query action MUST be the combination of the subject, action and resource. Permission to query policy rules is granted to all the rules where the subject, action and resource matches. *For example it is possible to declare that a certain application can query all the policy rules where the subject is "dms1".*

REQ-POL-09-12. It MUST be possible to restrict the visibility of policy rules based on the subject, action and resource information for the policy query rules. For example it is possible to declare that end user can query all the policy rules where the subject is end user, independently of the action and resource parts.

REQ-POL-09-13. The policy management MUST be done in such way that different parts of policy-related architectural elements (like policy store in the OMA DM component, policy store in the OSGi framework, etc.) represent a consistent policy rule set. *For example if right was delegated to "dms1" management server to install "bundle1", this rule change has to be represented consistently in the system, the OMA DM, the OSGi permission system and other policy stores (if exist) are changed consistently.*

5.10 Policy requirements for configuration management

REQ-POL-10-01. It MUST be possible to have management server, UDP, UE or end user as subject of configuration management policy rule.

REQ-POL-10-02. It MAY be possible to have UDL as subject of configuration management policy rule.

REQ-POL-10-03. It MUST be possible to have a configuration set belonging to a software component as resource of configuration management policy rule. *For example the managed service facility in OSGi allows to define permissions for the configuration parameter set of the managed service.*

REQ-POL-10-04. It MAY be possible to have a certain parameter in the configuration set belonging to a software component as resource of configuration policy rule. *For example it MAY be possible to describe rights for one particular configuration parameter in the configuration set and not for the whole set.*

REQ-POL-10-05. It MAY be possible to have configuration parameter of the application environment (JVM, OSGi framework, etc.) as resource of configuration management policy rule.

REQ-POL-10-06. It MAY be possible to declare that the policy rule refers to multiple resources. *For example it MAY be possible to declare that the subject has access to the configuration sets of all the bundles whose name matches a certain pattern.*

REQ-POL-10-07. It MUST be possible to describe rights for the access (configuration parameter read, update, create) of the configuration set.

REQ-POL-10-08. It MAY be possible to describe rights for the configuration read action.

REQ-POL-10-09 It MAY be possible to describe rights for the configuration update action. *This means that the configuration parameter existed before, the subject cannot create it but it can change its value.*

REQ-POL-10-10. It MAY be possible to describe rights for configuration parameter create action. *This means that the application can create the configuration parameter or update its value if it already exists.*

REQ-POL-10-11. It MUST be possible to describe that user must be prompted for confirmation as policy condition. If the policy rule matches, the user will be prompted for confirmation and the action is executed only if the user accepted the operation.

5.11 Policy requirements for KPI management

REQ-POL-11-01. It MUST be possible to specify permissions for KPI publishing action.

REQ-POL-11-02. The subject of the KPI publishing action MUST be UDP or UE..

REQ-POL-11-03. The subject of the KPI publishing action MAY be UDL.

REQ-POL-11-04. The resource of the KPI publishing action is the name of the KPI to be published. *For example it is possible to specify that UDP called "bundle1" is allowed to publish KPI called "maxproctime".*

REQ-POL-11-05. It MUST be possible to use wildcards when specifying the subject or the resource of the KPI publishing action. *For example it is possible to state that "bundle1" can publish KPI with any name.*

REQ-POL-11-06. It MUST be possible to specify permissions for KPI query action

REQ-POL-11-07. The subject of the KPI query action MUST be management server, UDP or UE or end user

REQ-POL-11-08. The subject of the KPI query action MAY be UDL.

REQ-POL-11-09. The resource of the KPI query action MUST be a combination of UDP, UE (and optionally UDL) name and the KPI name.

REQ-POL-11-10. It MAY BE possible to specify permission for the periodical KPI update action.

REQ-POL-11-11. The subject of the periodical KPI update action MAY BE an UDP, UE or UDL

REQ-POL-11-12. It MAY BE possible to describe the maximum frequency of the periodical KPI update action as a policy condition. *For example it is possible to specify that the application can send notification events at most once in every hour.*

REQ-POL-11-13. It MAY BE possible to describe the addressee of the notification event as a policy condition. *For example it is possible to declare that event though end user is one of the owners of this application, the application's notifications are not sent to the end user.*

5.12 Policy requirements for log access

REQ-POL-12-01. It MUST be possible to specify permissions for the log read access

REQ-POL-12-02. The subject of the log read access action MUST be management server, UDP, UE or end user.

REQ-POL-12-03. The subject of the log read access action MAY be UDL.

REQ-POL-12-03. One component in the resource part of the log read access action MUST be the UDP that sent the log entry to the log service.

REQ-POL-12-04. One component in the resource part of the log read access action MAY be the priority of the log event to read. *For example it may be possible to declare that the subject can have access to critical log events but not to details or informative events.*

REQ-POL-12-05. It MUST be possible to specify permissions for the log write access

REQ-POL-12-06. The subject of the log write access action MUST be an UDP.

All Page Within This Box

REQ-POL-12-07. The subject of the log write access action MAY be an UDL.

REQ-POL-12-08. It MAY be possible to declare condition on the log write action that controls the priority of the events that the application or bundle is allowed to write. *For example a low-priority application is not allowed to flood the log with low-priority events.*

5.13 Policy requirements for software component or application environment execution state management action

REQ-POL-13-01. Subject of the execution state management action MUST be management server, UDP, UE or end user.

REQ-POL-13-02. Subject of the execution state management action MAY be UDL.

REQ-POL-13-03. Resource of the execution state management action MUST be one of the following: UE, UDP, JVM, or application environment

REQ-POL-13-04. It MUST be possible to describe rights for the execution state change action

REQ-POL-13-05. "start" execution state change action MUST be possible for UEs and UDPs.

REQ-POL-13-06. "start" execution state change action MAY be possible for JVM and application framework.

REQ-POL-13-07. "stop" execution state change action MUST be possible for UEs and UDPs

REQ-POL-13-08. "stop" execution state change action MAY be possible for JVM and application framework

REQ-POL-13-09. "kill" execution state change action MAY be possible for UEs or JVM . *"kill" action means that if a misbehaving application doesn't react to "stop" action, it is terminated forcefully.*

REQ-POL-13-10. It MUST be possible to describe that user must be prompted for confirmation as policy condition. If the policy rule matches, the user will be prompted for confirmation and the action is executed only if the user accepted the operation.

REQ-POL-13-11. It MUST be possible to describe rights for execution state query action

REQ-POL-13-12. It MUST be possible to extend the policy rules with other commands than the “start”, “stop” and “kill”. *If there are other lifecycle stages in the system, the policy must be support those as well.*

5.14 Policy requirements for integrity check

REQ-POL-14-01. The subject of the integrity check action MUST be management server, UDP, UEor end user.

REQ-POL-14-02. The subject of the integrity check action MAY be UDL.

REQ-POL-14-03. The resource of the integrity check action MUST be UDP or UE.

REQ-POL-14-04. The resource of the integrity check action MAY be UDL.

5.15 Initial policy and policy behavior during reset

REQ-POL-15-01. There MUST always be a valid policy in the device. *Even if the policy is empty or in uninitialized state, it can still be interpreted as e.g. no rights for anybody.*

REQ-POL-15-02. There MUST be an initial policy in the device.

REQ-POL-15-03. It MUST be possible to restore the initial policy so that the device can be reset to a known state. *If the policy gets corrupted or mismanaged, there is a way to restore the initial policy by e.g. “cold reset” or “reformatting the device”.*

REQ-POL-15-04. If a device's policy is restored back to an initial state, then it MUST be possible to restore a device's installed software components back to some initial state as well.

REQ-POL-15-05. There MUST be a way to overwrite initial policy. Overwriting the initial policy MAY need special tools/privileges. *For example operator has a way to make sure that when the device is “cold reset”, the operator’s initial policy is restored. Overwriting the initial policy is not available for end users normally.*

5.16 Operator- and device characteristic-specific requirements

REQ-POL-16-01. It MUST be possible to use an operator-specific subscriber identifier (like IMSI) as policy condition.

REQ-POL-16-02. It SHOULD be possible to use an operator identification code as policy condition. *For example it is possible to state that certain policy rule is applicable only if the smart card identification module in the device belongs to certain operator.*

REQ-POL-16-03. It MAY be possible to use a device identification code (like IMEI) as policy condition. *For example it is possible to state that certain policy rule is applicable only if the device is the one identified by the IMEI.*

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 Acronyms and Abbreviations

API – Application Programming Interface

DMS – Device Management Server

All Page Within This Box

DRM – Digital Rights Management

GUI – Graphical User Interface

JVM – Java Virtual Machine

KPI – Key Performance Indicator

MEG – Mobile Expert Group

OM – Operational Management

OSGi – Open Services Gateway Interface

OTA – Over The Air

UDL – Unit of Delivery

UDP – Unit of Deployment

UE – Unit of Execution

URL – Uniform Resource Locator

6.3 End of Document