Implementation Guidelines for OMA Presence SIMPLE v1.1

Candidate Version – 27 Jun 2008

Open Mobile Alliance

OMA-WP-PRS_1_1_Implementation_Guidelines-20080627-C

Contents

Tables

1. Scope

The goal of this document is to provide guidelines to designers for the implementation of the Presence SIMPLE Version 1.1 enabler [PRS_ERELD]. The intention is not to replace or extend the Presence SIMPLE Version 1.1 specifications but rather to describe good practices or valuable design choices in order to help interoperability and migration between different implementations.

This document does not contain any new requirements in addition to [PRS_ERELD].

The guidelines consist of a number of recommendations on how to solve design issues in certain situations or real life examples for particular Presence SIMPLE Version 1.1 features.

2. References

[PDE_DDS] "Presence SIMPLE Data Specification", Version 1.0, Open Mobile Alliance™, OMA-DDS-Presence_Data_Ext-V1_0, URL: http://www.openmobilealliance.org/

[PRS_AC] "Presence Application characteristics", Version 1.1, Open Mobile Alliance™, OMA-SUP-AC_ap0002_presence-V1_1, URL: http://www.openmobilealliance.org/

[PRS_AD] "Presence SIMPLE Architecure", Version 1.1, Open Mobile Alliance™, OMA-AD-Presence_SIMPLE-V1_1, URL: http://www.openmobilealliance.org/

[PRS_DDS] "Presence SIMPLE Data Specification", Version 1.0, Open Mobile Alliance™, OMA-DDS-Presence_SIMPLE-V1_0, URL: http://www.openmobilealliance.org/

[PRS_ERELD] "Enabler Release Definition for OMA Presence SIMPLE", Version 1.1, Open Mobile Alliance™, OMA-ERELD-Presence_SIMPLE-V1_1, URL: http://www.openmobilealliance.org/

[PRS_MO] "OMA Management Object for Presence SIMPLE ", Version 1.1, Open Mobile Alliance™, OMA-TS-Presence_SIMPLE_MO-V1_1, URL: http://www.openmobilealliance.org/

[PRS_RD] "Presence Requirements", Version 1.1, Open Mobile Alliance™, OMA-RD-Presence_SIMPLE-V1_1, URL: http://www.openmobilealliance.org/

[PRS_RLS_XDM] "Resource List Server (RLS) XDM Specification", Version 1.1, Open Mobile Alliance™, OMA-TS-Presence_SIMPLE_RLS_XDM-V1_1, URL: http://www.openmobilealliance.org/

[PRS_SPEC] "Presence SIMPLE Specification", Version 1.1, Open Mobile Alliance™, OMA-TS-Presence_SIMPLE-V1_1, URL: http://www.openmobilealliance.org/

[PRS_XDM] "Presence XDM Specification", Version 1.1, Open Mobile Alliance™, OMA-TS-Presence_SIMPLE_XDM-V1_1, URL: http://www.openmobilealliance.org/

[RFC3863] IETF RFC 3863 "Presence Information Data Format (PIDF)", H. Sugano et al., Aug 2004, URL: http://www.ietf.org/rfc/rfc3863.txt

[RFC3903] IETF RFC 3903 "An Event State Publication Extension to the Session Initiation Protocol (SIP) ", A. Niemi, Oct 2004, URL: http://www.ietf.org/rfc/rfc3903.txt

[RFC3966] IETF RFC 3966 "The tel URI for Telephone Numbers", H. Schulzrinne, Dec 2004, URL: http://www.ietf.org/rfc/rfc3966.txt

[RFC3986] IETF RFC 3986 "Uniform Resource Identifier", T. Berners-Lee, R. Fielding, L. Masinter, Jan 2005, URL: http://www.ietf.org/rfc/rfc3986.txt

[RFC4479] IETF RFC 4479 "A Data Model for Presence ", J. Rosenberg, Jul 2006, URL: http://www.ietf.org/rfc/rfc4479.txt

[RFC4480] IETF RFC 4480 "RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)", H. Schulzrinne et al., Jul 2006, URL: http://www.ietf.org/rfc/rfc4480.txt

[RFC4660] IETF RFC 4660 "Functional Description of Event Notification Filtering", H.Khartabil et al, Sep 2006, URL: http://www.ietf.org/rfc/rfc4660.txt

[RFC4661] IETF RFC 4661 "An Extensible Markup Language (XML) Based Format for Event Notification Filtering", H.Khartabil et al, Sep 2006, URL: http://www.ietf.org/rfc/rfc4661.txt

[RFC5025] IETF RFC 5025 "Presence Authorization Rules", J. Rosenberg, Dec 2007, URL: http://www.ietf.org/rfc/rfc5025.txt

[XDM_Core] "XML Document Management (XDM) Specification", Version 1.1, Open Mobile Alliance™, OMA-TS-XDM_Core-V1_1, URL: http://www.openmobilealliance.org/

[XDM_IG] "Implementation Guidelines for OMA XDM v1.1 ", Open Mobile Alliance™, OMA-WP-XDM_1_1_Implementation_Guidelines, URL: http://www.openmobilealliance.org/

[XDM_SHARED] "Shared XDM Specification", Version 1.1, Open Mobile Alliance™, OMA-TS-XDM_Shared-V1_1, URL: http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

This is an informative document not intended to provide testable requirements for implementations.

The key word "RECOMMENDED" in this document is used to express the specific implementation guideline(s), and is typically accompanied by the detailed justification and example (if applicable) for the guideline.

3.2 Definitions

Presence Authorization Rule	See [PRS_SPEC].
Presence Information	See [PRS_SPEC].
Presence Information Element	See [PRS_SPEC].
Presence List	See [PRS_SPEC].
Presence Server	See [PRS_SPEC].
Presence Source	See [PRS_SPEC].
Presence Subscription	See [PRS_SPEC].
Presentity	See [PRS_SPEC].
Resource List Server	See [PRS_SPEC].
URI List	See [XDM_SHARED].
SIP URI	A communication resource as defined by [RFC3261].
tel URI	A globally unique identifier used to describe a resource identified by a telephone number as defined by [RFC3966].
Watcher	See [PRS_SPEC].
Watcher Information	See [PRS_SPEC].
Watcher Information Subscriber	See [PRS_SPEC].

3.3 Abbreviations

ERELD	Enabler Release Definition
IETF	Internet Engineering Task Force
IG	Implementation Guidelines
IP	Internet Protocol
OMA	Open Mobile Alliance
PIDF	Presence Information Data Format
PoC	Push-to-talk over Cellular
PRS	Presence SIMPLE
PS	Presence Server
RFC	Request For Comments

RLS	Resource List Server
SIMPLE	SIP Instant Message and Presence Leveraging Extensions
SIP	Session Initiation Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XCAP	XML Configuration Access Protocol
XDM	XML Document Management
XDMC	XDM Client
XDMS	XDM Server
XML	eXtensible Markup Language
XPath	XML Path Language
XUI	XCAP User Identifier

4. Introduction

The Presence SIMPLE Version 1.1 service enabler specified by [PRS_ERELD] allows for significant design flexibility, which in some cases may lead to difficulties in interoperability, migration, or user experience between different implementations. This document gives implementation guidance by providing recommendations and examples.

5. Implementation Guidelines

5.1 Presence Information Elements

The [PRS_DDS] "*Presence Information Elements Definitions*" does not define a limit for the length/size of contents of Presence Information Elements.

It is RECOMMENDED that a Watcher:

- support at least the following length/size for the Presence Information Elements listed below:
    - 100 kilobytes for the size of an icon referenced from a <status-icon> element;
    - 100 characters for the value of a <note> element;
    - 20 characters for the value of a <class> element;
    - 100 characters for the value of the <description> child element under a <service-description> element;
    - 20 characters for the value of the <other> child element under an <activities>, <place-type> or <mood> element;
    - 2 characters for the value of the <country> child element under a <civicAddress> element;
    - 50 characters for the value of the <A1>, <A2>, <A3>, <A4>, <A5>, <A6>, <LMK>, <LOC> and <NAM> child elements under a <civicAddress> element;
    - 20 characters for the value of the <PRD>, <POD>, <STS> and <PC> child elements under a <civicLocation> element;
    - 10 characters for the value of the <HNO> and <HNS> child elements under a <civicLocation> element; and
    - 5 characters for the value of the <FLR> child element under a <civicLocation> element.

It is therefore also RECOMMENDED that a Presence Source:

- not exceed the above length/size when publishing the above-listed Presence Information Elements.

The reasons for the recommendations include:

- effective use of resources (e.g. device memory and access network bandwidth);
- avoid misuse of the elements as much as possible;
- simplified migration between devices; and
- improved interoperability between Presence Source, PS, and Watcher, as the length/size of the value of a Presence Information Element is predictable.

5.2 Publication

5.2.1 Publication Content

PIDF is an extensible data format allowing the Presence Source to publish arbitrary Presence Information.

It is RECOMMENDED that a Presence Source:

- limit the publication of Presence Information to the elements specified in [PRS_DDS].

The reasons for the recommendation include:

- effective use of resources (e.g. device processing and access network bandwidth);

- improved interoperability between Presence Source and PS, by decreasing the possibility of conflicts in PS's composition of the published Presence Information; and
- improved interoperability between Presence Source and Watcher, by decreasing the possibility of the Watcher receiving Presence Information that the user interface of the Watcher device is not prepared to render.

5.2.2 Storage of the SIP-Etag Value

A device hosting the Presence Source may be powered off without cancelling active publication event state in the PS.

It is RECOMMENDED that a Presence Source:

- store the value of the "SIP-ETag" header field in persistent storage space and use the stored value in conditional publications for the lifetime of the publication as defined in [RFC3903].

The reasons for the recommendation include:

- increased accuracy of Presence Information delivered to Watchers, by enabling the Presence Source to manipulate the previous publication event state after the device is powered on again, rather than creating a new publication event state in the PS where the (potentially incorrect) previous publication event state may continue being delivered to Watchers until it expires.

5.2.3 Usage of the <note> Element

The [PRS_DDS] allows multiple <note> elements to be included in various Presence Information Elements within a presence document (e.g. <place-type>, <mood>, <tuple>, <device>): [RFC3863] defines the <note> element for the <presence> and <tuple> element, [RFC4479] defines the <note> element for the <person> and <device> element, and [RFC4480] defines the <note> element for RPID.

It is RECOMMENDED that a Presence Source:

- publish only one <note> element [RFC4479], when publishing the "person" component;
- not include the "xml:lang" attribute in the <note> element; and
- not publish any <note> element, when publishing the "service" or "device" component.

It is therefore also RECOMMENDED that the device hosting the Watcher:

- be able to render at least the <note> element which is the direct child element of the <person> element on its user interface.

The reasons for the recommendations include:

- improved interoperability between Presence Source and Watcher, since it is likely infeasible for the device hosting the Watcher to render all possible <note> elements on the user interface;
- the usage of the "xml:lang" attribute has limited value in rendering the <note> element on the user interface;
- the free text description for a "service" component can be delivered using the <service-description> element, and the free text description for a "device" component does not have much meaning; and
- effective use of resources (e.g. access network bandwidth).

5.3 Event Notification Filtering

5.3.1 General

A Watcher/Watcher Information Subscriber can make use of the event notification filtering mechanism as described in [RFC4660] for performance optimization. A Watcher/Watcher Information Subscriber can control the contents received in a SIP NOTIFY request, by including a filter document (i.e. an XML document [RFC4660] [RFC4661]) as payload in the corresponding SIP SUBSCRIBE request [PRS_SPEC].

It is RECOMMENDED that a Watcher/Watcher Information Subscriber:

- use event notification filtering whenever possible. Further details about when the Watcher/Watcher Information Subscriber are to use event notification filtering are described in sections 5.3.2 and 5.3.3, respectively.

The reasons for the recommendation include:

- effective use of resources (e.g. access network bandwidth) by limiting message sizes and number of messages between the Watcher/Watcher Information Subscriber and the PS.

It is RECOMMENDED that when constructing a filter document, the Watcher/Watcher Information Subscriber:

- use only the <what> and <include> elements within a <filter> element;
- not use the “type” attribute describing the value of the <include> or <exclude> element when the type of the value is ‘xpath’; and
- not use the “enabled” and “remove” attributes within a <filter> element.

The reasons for the recommendations include:

- improved performance and interoperability by limiting filter complexity;
- the default value ‘xpath’ is used when the optional “type” attribute is missing; and
- effective use of resources (e.g. access network bandwidth) by limiting message sizes.

It is RECOMMENDED that the Watcher/Watcher Information Subscriber:

- always follow the syntax described in chapter 5 of [RFC4661] when creating XPath expressions in the filter, so that the XPath expression always starts with “//”.

The reasons for the recommendation include:

- improved interoperability by highlighting the correct syntax, since the examples provided in [RFC4661] are not aligned with the syntax description in chapter 5 of the RFC.

5.3.2 Filtering Presence Information

It is RECOMMENDED that a Watcher:

- use event notification filtering when the Watcher requires specific Presence Information - e.g. only the:
    - Presence Information about selected service(s) in the “service” component,
    - Presence Information within a specific component (e.g. the “person” or “device” component),
    - Presence Information of interest, or
    - Presence Information supported by the Watcher.

The reasons for the recommendation include:

- effective use of resources (e.g. access network bandwidth), since message sizes and number of messages between the Watcher and the PS are reduced by transferring only information that is understood and needed by the Watcher.

It is RECOMMENDED that when constructing a filter document, the Watcher:

- not use the <include> element that contains the XPath expression pointing to the <status> element, when using the filter for specific Presence Information from the "service" component; and
- not use the <include> element that contains the XPath expression pointing to the <deviceID> element, when using the filter for specific Presence Information from the "device" component.

The reasons for the recommendations include:

- effective use of resources (e.g. access network bandwidth) by limiting the size of the filter document, since:
    - the <status> element is always included in the resulting filtered Presence Information document as it is the mandatory child element of the <tuple> element; and
    - the <deviceID> element is always included in the resulting filtered Presence Information document as it is the mandatory child element of the <device> element.

It is RECOMMENDED that when constructing a filter document, the Watcher:

- use the <include> elements containing the XPath expressions pointing to the <service-description>, <contact> and <timestamp> elements respectively, when using the filter for specific Presence Information from the "service" component; and
- use the <include> element containing the XPath expression pointing to the <timestamp> element, when using the filter for specific Presence Information from the "person" component.

The reasons for the recommendations include:

- improved interoperability since a Watcher's Presence Information processing requires:
    - the <service-description>, <contact> and <timestamp> elements in case two or more "service" components are conflicting with each other; and
    - the <timestamp> element in case two or more "person" components are conflicting with each other.

Appendix B.1 shows a few examples of filter documents to provide guidance how to specify a filter based on three common use cases.

5.3.2.1 Usage of the Filter Document for Presence Subscription

A filter document for the Presence Subscription may contain one or more <filter> elements. Each <filter> element is used to specify the content of an individual filter. A <filter> element may have a "uri" attribute identifying the resource to which the filter applies, or a "domain" attribute identifying the domain of the resources to which the filter applies. Supplying a "uri" or "domain" attribute in a <filter> element makes sense only for the RLS subscriptions targeted to multiple resources, but not for the Presence Subscriptions targeted to an individual resource.

It is RECOMMENDED that, when constructing a filter document for a Presence Subscription for an individual resource, the Watcher:

- not use 'uri specific filters' (i.e. the <filter> element including a "uri" attribute value) or 'domain specific filters' (i.e. the <filter> element including a "domain" attribute value); and
- use no more than one 'generic filter' (i.e. the <filter> element without a "uri" attribute or "domain" attribute).

The reasons for the recommendations include:

- ‘uri specific filters’ and ‘domain specific filters’ are meaningful only for RLS subscriptions; and
- improved interoperability between Watcher and PS, since more than one filter for a Presence Subscription for an individual resource would generate confusion regarding which filters to apply.

It is RECOMMENDED that, when constructing a filter document for an RLS subscription, the Watcher:

- use no more than one ‘generic filter’, if the filter is intended to apply to all Presentities in the Presence List; or
- use multiple filters as follows:
    - zero or more ‘uri specific filters’, each of which is intended for a Presentity in the Presence List,
    - zero or more ‘domain specific filters’, each of which is intended for a group of Presentities in the Presence List with the same domain, or
    - zero or one ‘generic filter’ for all other Presentities in the Presence List.

The reasons for the recommendations include:

- improved interoperability between Watcher and RLS by ensuring consistent interpretation of filters included in the RLS subscription, in order for the RLS to propagate the filters in the backend subscriptions.

5.3.3 Filtering Watcher Information

It is RECOMMENDED that a Watcher Information Subscriber:

- use event notification filtering when specific Watcher Information (e.g. Watcher Information defined by one or more specific namespaces) or Watcher Information about specific kinds of Watchers (e.g. only the Watchers with status “pending” or “waiting” for reactive authorization) is required.

The reasons for the recommendation include:

- effective use of resources (e.g. access network bandwidth), since message sizes and number of messages are reduced by transferring only information that is understood and needed by the Watcher.

It is RECOMMENDED that when constructing a filter document, the Watcher Information Subscriber:

- use no more than one ‘generic filter’ (i.e. a <filter> element without any attribute); and
- not use any ‘uri specific filters’ (i.e. a <filter> element with the “uri” attribute) or ‘domain specific filters’ (i.e. a <filter> element with the “domain” attribute).

The reasons for the recommendations include:

- ‘uri specific filters’ and ‘domain specific filters’ are meaningful only for RLS subscriptions, but a Watcher Information subscription is always targeted for a single Presentity; and
- improved interoperability between a Watcher Information Subscriber and the PS, as a filter document can be very complex

In Appendix B.2 are given examples of filter documents provided as guidance on how to specify a filter based on two common use cases.

5.4 Encodings

The guidelines about encodings defined in [XDM_IG] “*Encodings*” are also applicable for OMA Presence SIMPLE 1.1.

5.5 Provisioning

5.5.1 Service-URI-Template for Presence Lists

As described in [PRS_RLS_XDM] "*Validation Constraints*", the Service URI for Presence Lists (i.e. the value of the "uri" attribute of a <service> element in a Presence List document) proposed by an XDMC when creating a Presence List in the RLS XDMS must conform to the syntax of the Service-URI-Template parameter described in [PRS_AC] and [PRS_MO].

It is RECOMMENDED that:

- the Service-URI-Template for Presence Lists have the following structure:

  <xui>;pres-list=<id>

  where the <xui> and <id> substitution tags are described in [XDM_Core] "*Provisioned XDMC Parameters*".

The reasons for the recommendation include:

- effective use of resources (e.g. access network bandwidth), since the recommended Service-URI-Template makes it easier for the XDMC to generate a globally unique Service URI that is accepted by the RLS XDMS; and
- simplification for the SIP/IP Core network to recognize the Service URI as a Presence List (e.g. to optimize routing of Presence List subscriptions).

An example of a Service URI conforming to the recommended Service-URI-Template is as follows:

sip:joe@example.com;pres-list=list-a

where the XUI used to generate the Service URI is a SIP URI, as required by [PRS_RLS_XDM] "*Validation constraints*".

5.5.2 Length of Provisioning Parameters

The [PRS_AC] and [PRS_MO] define a set of character formatted provisioning parameters without limiting the length of those parameters.

It is RECOMMENDED that:

- the string of any character-formatted provisioning parameter, defined in [PRS_MO] and [PRS_AC], not exceed 100 characters.

The reasons for the recommendation include:

- use of longer provisioning strings than a device can handle may cause malfunctions;
- effective use of resources (e.g. access network bandwidth); and
- maximum length of 100 characters is deemed sufficient.

5.6 Presence Authorization Rules

5.6.1 Rules Template

The Presence Authorization Rules document defined in [PRS_XDM] offers a lot of flexibility for client implementions since a <rule> element can be composed of many different combinations of the <conditions>, <actions> and <transformations> child elements, allowing clients to use different ways of expressing the same Presence Authorization Rules. This can make migration between and parallel use of different clients complex.

This section defines a set of template rules with predefined values of the "id" attribute of the <rule> element where the combinations of the <rule> child elements are restricted. The template rules are described in Table 1and Table 2 below.

It is RECOMMENDED that an XDMC:

- use the value of the "id" attribute of the <rule> element as defined in column 1 of Table 2 when implementing a rule according to the table; and
- not use a value of the "id" attribute starting with 'wp_prs', when it has a need to specify other types of rules than defined in Table 2.

The reasons for the recommendations include:

- simplified client implementation, since a client can recognize a rule as defined by this document by checking only the "id" attribute of a <rule> element.

It is RECOMMENDED that an XDMC:

- always include a rule where a Presentity is granted access to all of its Presence Information, i.e. a 'wp_prs_allow_own' rule;
- not include more than one rule that contains the <other-identity> condition; and
- not include more than one rule that contains the <anonymous-request> condition.

The reasons for the recommendations include:

- a Presentity is expected to be able to see all of his/her own Presence Information, and a Watcher in an Application Server acting on the behalf of the Presentity is expected to always have access to the Presentity's Presence Information;
- improved performance when evaluating default rules; and
- improved performance when evaluating rules for anonymous requests.

It is RECOMMENDED that an XDMC:

- not include a rule containing the <anonymous-request> condition having the "allow" or "confirm" value for the <sub-handling> action.

The reasons for the recommendation include:

- user privacy when a black-listed user subscribes anonymously, since rules containing the <anonymous-request> condition have the highest precedence when evaluating a rule set according to [XDM_Core] "*Combining Permissions*".

It is RECOMMENDED that an XDMC:

- implement a Presence Authorization Rules document per the template rules described in Table 2.

The reasons for the recommendation include:

- improved interoperability between XDMCs by ensuring that all XDMCs have the same way of implementing a certain type of rule;
- improved interoperability between XDMC and Presence XDMS and between Presence XDMS and PS, by reducing rule complexity; and
- improved performance in processing Presence Authorization Rules by reducing rule complexity.

The template rules described in Table 1 and Table 2 support two main alternatives of implementing a Presence Authorization Rules document:

- "white-list": By default, Watchers are not allowed to access any Presence Information. A Presence Authorization Rules document implemented using the "white-list" method can have all template rules except 'wp_prs_allow_unlisted' rule (the absence of which can be used to detect that a Presence Authorization Rules document is based on the "white-list" method).
- "black-list": By default, Watchers are allowed to access all Presence Information. A Presence Authorization Rules document implemented using the "black-list" method always contains the 'wp_prs_allow_unlisted' rule (which can be used to detect that a Presence Authorization Rules document is based on the "black-list" method), but never the 'wp_prs_unlisted' rule. All other template rules can be used.

NOTE: If it is desired to allow access to some (but not all) Presence Information by default (e.g. neither "white-list" nor "black-list" method), then the Presence Authorization Rules document includes the <other-identity> condition in a rule that does not use a value of the "id" attribute starting with 'wp_prs'.

Table 1 and Table 2 contain descriptions of the different template rules.

Rule	Short Description
wp_prs_unlisted	This rule is used to block all users that are not found in any other rule or to trigger reactive authorization for such users. This rule is the default rule for the “white-list” method.
wp_prs_allow_unlisted	This rule is used to allow access to all Presence Information to users that are not found in any other rule. This rule is the default rule for the “black-list” method.
wp_prs_grantedcontacts	This rule is used to allow access to all Presence Information to all users in the “oma_grantedcontacts” URI List stored in the Shared XDMS. Note: If a user is included both in this rule and in the “wp_prs_one_<id>” or “wp_prs_allow_one_<id>” rule, this rule is ignored as defined in [XDM_Core].
wp_prs_blockedcontacts	This rule is used to block access to all Presence Information from all users in the “oma_blockedcontacts” URI List in the Shared XDMS. Note: If a user is included both in this rule and in the “wp_prs_one_<id> or “wp_prs_allow_one_<id>” rule, this rule is ignored as defined in [XDM_Core]. If the user is included both in this rule and in the “wp_prs_grantedcontacts” or “wp_prs_allow_onelist_<id>, this rule will not be applied for this user as defined in [XDM_Core].
wp_prs_block_anonymous	This rule is used to block anonymous user access to all Presence Information.
wp_prs_allow_own	This rule is used to allow the Presentity access to its own Presence Information.
wp_prs_allow_one_<id>	This rule is used to allow a certain user access to all or to a limited set of Presence Information.
wp_prs_allow_onelist_<id>	This rule is used to allow a certain list of users in the Shared XDMS access to all or a limited set of Presence Information. Note: If a user is included both in this rule and the “wp_prs_grantedcontacts” rule, the user will have access to all Presence Information as defined in [XDM_Core]. If a user is included both in this rule and in the “wp_prs_one_<id> or “wp_prs_allow_one” rule, this rule is ignored as defined in [XDM_Core].
wp_prs_one_<id>	This rule is used to block a certain user for Presence Information or to trigger reactive authorisation for this user. Note: If a user is included both in a “wp_prs_allow_one_<id> rule and this rule, the “wp_prs_one_<id> is ignored for this user as defined in [XDM_Core].
wp_prs_onelist_<id>	This rule is used to block a certain list of users in the Shared XDMS for presence information or to trigger reactive authorisation for this list of users. Note: If a user is included both in this rule and in “wp_prs_blockedcontacts” and/or “wp_prs_granted contacts” rules, the Presence Server will apply only one of the rules as defined in [XDM_Core]. If a user is included both in this rule and in the “wp_prs_one_<id> or “wp_prs_allow_one_<id>” rule, this rule is ignored as defined in [XDM_Core].

Table 1 Short description of Predefined Authorization Template Rules

"id" attribute value of a <rule> element	valid <sub-handling> child element value(s)	valid <transformations> child element(s)	valid <conditions> child element(s)
wp_prs_unlisted	"confirm", "block", or "polite-block"	None.	<other-identity>
wp_prs_allow_unlisted	"allow"	Provide access to all Presence Information (see Appendix B.3).	<other-identity>
wp_prs_grantedcontacts	"allow"	Provide access to all Presence Information (see Appendix B.3).	<external-list> containing a reference to the URI List "oma_grantedcontacts".
wp_prs_blockedcontacts	"block" or "polite-block"	None.	<external-list> containing a reference to the URI List "oma_blockedcontacts".
wp_prs_block_anonymous	"block" or "polite-block"	None.	<anonymous_request>
wp_prs_allow_own	"allow"	Provide access to all Presence Information (see Appendix B.3).	One <one> child element of <identity>, containing the Presentity's URI.
wp_prs_allow_one_<id> where <id> is a value set by the XDMC to make the rule unique within the document.	"allow"	Any.	One <one> child element of <identity>, containing a SIP or a tel URI.
wp_prs_allow_onelist_<id> where <id> is a value set by the XDMC to make the rule "id" attribute unique within the document.	"allow"	Any.	One <entry> child element of <external-list>, containing a reference to a URI List.
wp_prs_one_<id> where <id> is a value set by the XDMC to make the rule "id" attribute unique within the document.	"confirm", "block", or "polite-block"	None.	One <one> child element of <identity>, containing a SIP or a tel URI.
wp_prs_onelist_<id> where <id> is a value set by the XDMC to make the rule "id" attribute unique within the document.	"confirm", "block", or "polite-block"	None.	One <entry> child element of <external-list>, containing a reference to a URI List.

Table 2 Element description of Predefined Authorization Template Rules

Appendix B.3 shows examples of these template rules.

5.6.2 Usage of the <transformations> Element

The <transformations> child element in a Presence Authorization Rules document [PRS_XDM], i.e. the Presence Content Rules, details the visibility that a Watcher is granted to particular Presence Information items in order to protect the privacy of a Presentity.

A coarse grained privacy filter grants visibility to selected <person>, <device> and <tuple> data component elements based on identifying information for these elements [RFC5025]. This can be achieved by the <provide-persons>, <provide-devices>, and <provide-services> child elements of the <transformations> element.

A fine grained privacy filter grants visibility of the selected Presence Attributes in a particular data component. This can be achieved by, e.g. the <provide-willingness>, <provide-activities>, <provide-all-attributes> elements.

The visibility that results from a set of matching rules depends on the combined result of both the coarse grained and fine grained privacy filters supplied in the <transformations> element of the matching rules. Determining the resulting visibility is a complex issue as the semantics of the privacy filter items within the <transformations> element has to be considered.

It is RECOMMENDED that an XDMC:

- include both a coarse grained privacy filter and a fine grained privacy filter in each <transformations> element; and
- include, as the fine grained privacy filter in a <transformations> element, either the <provide-all-attributes> element, or a set of fine grained privacy filters each one valued “true”; i.e. the fine grained privacy filters valued “false” are not included in the rules.

The reasons for the recommendations include:

- the necessity for both a coarse grained and a fine grained privacy filters in order to have a semantically correct privacy filter;
- unambiguous results when <transformations> elements from multiple matching rules are combined;
- smooth device migration by using a predictable structure for the Presence Authorization Rules document; and
- improved interoperability by reducing the complexity of the Presence Authorization Rules document.

5.6.3 Usage of URIs

It is RECOMMENDED that, when managing a rule, the XDMC:

- use a SIP URI in the condition part of the rule, if the SIP URI is known; and
- use the global format of a tel URI as specified in [RFC3966] “*URI Syntax*” in the condition part of the rule, if only a tel URI is known.

The reasons for the recommendations include:

- improved user experience, since the identity obtained in the Presence Subscription request would be a SIP URI or a tel URI of global format, and therefore a tel URI of local format would be hard to match with the identity obtained in the Presence Subscription request;
- improved efficiency of tel URI equivalence testing as defined in [RFC3966] “*URI Comparisons*” and [RFC3986] ”*Normalization and Comparison*”; and
- improved interoperability across domains.

5.7 Usage of Presence Lists

The Presence Lists allow Watchers to subscribe to Presence Information of a pre-defined list of Presentities using a single subscription. A Watcher needs to pre-define a Presence List in the RLS XDMS with its Service URI and the list of those interested Presentities.

It is RECOMMENDED that a Watcher:

- use a Presence List subscription whenever appropriate.

The reasons for the recommendation include:

- effective use of resources (e.g. access network bandwidth) by limiting the number of messages between the Watcher and the PS.

5.7.1 Generating Service URIs for Presence Lists

An XDMC creates a Service URI for Presence Lists according to the Service URI template in section 5.5.1.

When creating a Service URI for a Presence List, it is RECOMMENDED that the XDMC:

- use, as the value of the <id> of a Service URI for a Presence List, the value of the “name” attribute of the referenced URI List from the same Presence List, if the corresponding <service> element in the Presence List contains a <resource-list> element that points to a URI List stored in a Shared XDMS.

The reasons for the recommendation include:

- improved performance and interoperability, as an arbitrarily derived value of <id> by an XDMC may not be accepted by the RLS XDMS, requiring an additional transaction for agreeing upon the value between the XDMC and the RLS XDMS.

5.8 Lists used in Presence Service

Lists are used for different purposes in the presence service. Lists that can be used in the presence service are outlined below:

- Presence List: A list of users whose Presence Information a Watcher can request with a single Presence Subscription [PRS_RLS_XDM]. A Presence List is defined within an RLS-services document stored in the RLS XDMS. A Watcher can maintain multiple Presence Lists (identified by the value of the “uri” attribute of the corresponding <service> element) in a single RLS-services document.

- Grant List: A list of users whom a Presentity allows to subscribe for his/her Presence Information. The users are listed in a Presence Authorization Rules document stored in the Presence XDMS [PRS_XDM], as the child elements under the <conditions> element, whose corresponding <sub-handling> element has the value “allow”.

- (Polite) Block List: A list of users whom a Presentity (polite) blocks from subscribing for his/her Presence Information. The users are listed in a Presence Authorization Rules document stored in the Presence XDMS [PRS_XDM], as the child elements under the <conditions> element, whose corresponding <sub-handling> element has either the value “block” or “polite-block”.

It is RECOMMENDED that an XDMC creating a Presence List in the RLS XDMS:

- use the <resource-list> element to refer to a URI List stored in the Shared XDMS; and

- not use a <list> element in the Presence List document.

The reasons for the recommendations include:

- smooth device migration and simplified implementation if all XDMC are using the same method to reference a URI List in the Shared XDMS; and
- efficient re-use of URI Lists stored in the Shared XDMS, instead of duplicating the list in each application-specific XDMS. For example, a URI List in the Shared XDMS can be used both for a Presence List in the RLS XDMS and a Grant List in the Presence XDMS.

It is RECOMMENDED that an XDMC creating a Grant List or (Polite) Block List:

- use the <external-list> element (as child element of the <conditions> element of the Presence Authorization Rules document) to refer to the URI List stored in the Shared XDMS; and
- not use the <identity> element as a child element of the <conditions> element.

The reasons for the recommendations include:

- smooth device migration and simplified implementation if all XDMC are using the same method to create a Presence Authorization Rule for a list of users; and
- efficient re-use of URI Lists stored in the Shared XDMS, instead of duplicating the list in each application-specific XDMS. For example, a URI List in the Shared XDMS can be used both for a Presence List in RLS XDMS and a Grant List in the Presence XDMS.

Appendix A. Change History (Informative)

Document Identifier	Date	Sections	Description
OMA-WP-PRS_Implementation_Guidelines-20070615-D	15 Jun 2007	All	Initial version of WP (including skeleton and ToC) as permanent doc
	10 Sep 2007	1, 4, 5.8	Incorporated CRs: OMA-PAG-2007-0526 OMA-PAG-2007-0552
	30 Oct 2007	All	Incorporated CRs: OMA-PAG-2007-0565R03 OMA-PAG-2007-0687R01 OMA-PAG-2007-0688R01 OMA-PAG-2007-0689 OMA-PAG-2007-0690R01 OMA-PAG-2007-0747R02
	27 Nov 2007	2, 5	Incorporated CRs: OMA-PAG-2007-0678R01 OMA-PAG-2007-0754R02 OMA-PAG-2007-0773R02 OMA-PAG-2007-0784 OMA-PAG-2007-0790R01
	12 Dec 2007	5.2 5.1 5.6, App B.1 3.3, 5.9 5.10, B.2 5.5, App B.3 5.4 All	OMA-PAG-2007-0287R01 OMA-PAG-2007-0847R01 OMA-PAG-2007-0848R01 OMA-PAG-2007-0849R01 OMA-PAG-2007-0850R01 OMA-PAG-2007-858R02 OMA-PAG-2007-0861R01 Editorials
	9 Jan 2008	3.1 4, 5.5, 5.10.1; All	OMA-PAG-2008-007Formatting
	19 feb 2008	All	Included Editorial comments in OMA-CONRR-2008-XDM_PRS_IMPL_V1_0_20080213-D
	4 Mar 2008	2, 5.2, 5.9 5.10, B.2.2 5.1 3.2 5..2 5.3 5..5 5.6 5.8 5.10 5.10 B.1 B.2.1, B.2.2 5.10, B.2.1, B.2.2 B B.2.1 5.9 B.3.1 5.10, B.2.2	OMA-PAG-2008-0069R03 OMA-PAG-2008-0070 OMA-PAG-2008-0074 OMA-PAG-2008-0075R01 OMA-PAG-2008-0076R01 OMA-PAG-2008-0077 OMA-PAG-2008-0078R01 OMA-PAG-2008-0080R01 OMA-PAG-2008-0081 OMA-PAG-2008-0083R02 OMA-PAG-2008-0084R01 OMA-PAG-2008-0085 OMA-PAG-2008-0086R02 OMA-PAG-2008-0087 OMA-PAG-2008-0112 OMA-PAG-2008-0113 OMA-PAG-2008-0120 OMA-PAG-2008-0121R01 OMA-PAG-2008-0133R01
	6 Mar 2008	5.2, 5.7.1	Corrected errors regarding OMA-2008-0069R03 Editorials in 1,4, 5.4, 5.8, 5.10, Corrected escaping in B.2.1, B2.2
	26 Mar 2008	5.1-5.5, 5.7, 5.8, App A 5.5	Editorials OMA-PAG-2008-0079R01

		5.4, 5.5, B.1.1, B.1.2 B.1.3, B.3.1, B.3.2 2, 5.8. 2 5.5, B.1.1, B.1.2, B.1.3 5.1 5.9 5.8.1, B.2.1	OMA-PAG-2008-0106R02 OMA-PAG-2008-0107R01 OMA-PAG-2008-0108 OMA-PAG-2008-0119R01 OMA-PAG-2008-0143 R02 OMA-PAG-2008-0162R01
	28 Apr 2008	2, 4.5, 5.5, 5.8.1, 5.9 5.3.2 5.4, 5.5 5.8.1 5.8.3(n) App B 5.8.1 B.3.2 B.3.1 5.8.1 1 2 3.2 3.3 5.1 5.2, 5.8(n) 2, 5.3.1 5.3.2 2, 5.3.3 5.7 5.4 5.4 1, 5.5 5.5, 5.4.2.1 (n) 5.5 5.8.1 5.8.2 5.9 App B All	Editorials OMA-PAG-2008-0176R02 OMA-PAG-2008-0177R01 OMA-PAG-2008-0181R01 OMA-PAG-2008-190R02 OMA-PAG-2008-0193 (OMA-PAG-2008-0199R01) OMA-PAG-2008-0202 OMA-PAG-2008-0219 OMA-PAG-2008-0221R02 OMA-PAG-2008-0224 OMA-PAG-2008-0225 OMA-PAG-2008-0226R01 OMA-PAG-2008-0227R01 OMA-PAG-2008-0228 OMA-PAG-2008-0229R02 OMA-PAG-2008-230R01 OMA-PAG-2008-231 OMA-PAG-2008-0232R04 OMA-PAG-2008-0233R01 OMA-PAG-2008-0238R02 OMA-PAG-2008-0239R01 OMA-PAG-2008-0240R01 OMA-PAG-2008-0241R01 OMA-PAG-2008-0242R02 OMA-PAG-2008-0243R02 OMA-PAG-2008-0246R01 OMA-PAG-2008-0247R01 OMA-PAG-2008-0249R01 Editorials
	9 May 2008	All App B.3	OMA-PAG-2008-0292R02 OMA-PAG-2008-309R01
	14 May 2008	None	Corrected error of CR Number 0292R02 Editorial: adding –D in file name
	03 Jun 2008	All	Editorial comments from PAG R&A
	09 Jun 2008	App A	Correction in App A - History for 03 Jun 2008. Editorial comments from PAG R&A: Incorporated CR: OMA-PAG-2008-378R01
OMA-WP-PRS_Implementation_Guidelines-20080627-C	27 Jun 2008	N/A	Status changed to Candidate by TP TP ref#: OMA-TP-2008-0242-INP_XDM_PRS_IMPL_1_0_RRP_for_Candidate_Approval

Appendix B. Examples

This Appendix provides examples that clarify the recommendations in this document.

The examples here include the formatting characters (like extra spaces, linefeeds) and the comments to improve readability. However, it is noted that these are not needed in a real XML implementation and should be omitted to limit the document sizes.

B.1 Presence Information Filtering Examples

Examples of filter documents are given based on three use cases. The examples only cover the case of controlling the content of notifications.

B.1.1 Case 1: Watcher wants to be notified only about a specific service

This section provides an example filter document when a Watcher handling a PoC service comprising the OMA PoC-Session service and OMA PoC-Alert service wants to be notified only with the Presence Information Elements related to all versions of that service.

```
<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
  <ns-bindings>
      <ns-binding prefix="pidf" urn="urn:ietf:params:xml:ns:pidf"/>
      <ns-binding prefix="op" urn="urn:oma:xml:prs:pidf:oma-pres"/>
  </ns-bindings>
  <filter id="PoC-session">
      <what>
          <include>
              //pidf:presence/pidf:tuple[op:service-description/op:service-id=
              "org.openmobilealliance:PoC-session"]
          </include>
          <include>
              //pidf:presence/pidf:tuple[op:service-description/op:service-id=
              "org.openmobilealliance:PoC-alert"]
          </include>
      </what>
   </filter>
</filter-set>
```

B.1.2 Case 2: Watcher wants to be notified only about person data

This section provides an example filter document when a Watcher handling information related to social communities wants to be notified only with the Presence Information Elements under the <person> data component.

```
<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
  <ns-bindings>
      <ns-binding prefix="pidf" urn="urn:ietf:params:xml:ns:pidf"/>
      <ns-binding prefix="pdm" urn="urn:ietf:params:xml:ns:pidf:data-model"/>

  </ns-bindings>
  <filter id="person">
      <what>
          <include>//pidf:presence/pdm:person</include>
      </what>
   </filter>
</filter-set>
```

B.1.3 Case 3: Watcher wants to be notified only about specific elements

This section provides an example filter document when a Watcher that wants to receive only specific Presence Information Elements. The example shows all Presence Information Elements listed in [PRS DDS] "*Presence Information Element Definitions*" that explicitly needs to be included in the filter document for being reported in presence notifications.

```
<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
  <ns-bindings>
      <ns-binding prefix="pidf" urn="urn:ietf:params:xml:ns:pidf"/>
      <ns-binding prefix="pdm" urn="urn:ietf:params:xml:ns:pidf:data-model"/>
      <ns-binding prefix="rpid" urn="urn:ietf:params:xml:ns:pidf:rpid"/>
      <ns-binding prefix="op" urn="urn:oma:xml:prs:pidf:oma-pres"/>
  </ns-bindings>
  <filter id="allSupportedElements">
      <what>
          <include> //pidf:presence/pdm:person/op:overriding-willingness  </include>
          <include> //pidf:presence/pdm:person/rpid:activities            </include>
          <include> //pidf:presence/pdm:person/rpid:place-type            </include>
          <include> //pidf:presence/pdm:person/rpid:time-offset           </include>
          <include> //pidf:presence/pdm:person/rpid:mood                  </include>
          <include> //pidf:presence/pdm:person/rpid:status-icon           </include>
          <include> //pidf:presence/pdm:person/rpid:class                 </include>
          <include> //pidf:presence/pdm:person/pdm:note                   </include>
          <include> //pidf:presence/pdm:person/pdm:timestamp              </include>
          <include> //pidf:presence/pidf:tuple/op:registration-state      </include>
          <include> //pidf:presence/pidf:tuple/op:barring-state           </include>
          <include> //pidf:presence/pidf:tuple/op:willingness/op:basic    </include>
          <include> //pidf:presence/pidf:tuple/rpid:status-icon           </include>
          <include> //pidf:presence/pidf:tuple/op:service-description     </include>
          <include> //pidf:presence/pidf:tuple/rpid:class                 </include>
          <include> //pidf:presence/pidf:tuple/pdm:deviceID               </include>
          <include> //pidf:presence/pidf:tuple/pidf:contact               </include>
          <include> //pidf:presence/pidf:tuple/pidf:timestamp             </include>
          <include> //pidf:presence/pdm:device/op:network-availability    </include>
          <include> //pidf:presence/pdm:device/pdm:timestamp              </include>
      </what>
   </filter>
</filter-set>
```

B.2 Watcher Information Filtering Examples

Examples of filter documents for Watcher Information Subscription are given based on two use cases. The examples only cover the case of controlling the content of notifications.

B.2.1 Case 1: Watcher Information Subscriber wants to be notified in case of reactive authorization.

This example shows a Watcher Information Subscriber that wants to be notified about Watchers that have the status "pending" or "waiting", in order to perform reactive authorization of those Watchers.

```
<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
  <ns-bindings>
      <ns-binding prefix="wi" urn=urn:ietf:params:xml:ns:watcherinfo"/>
  </ns-bindings>
  <filter id="pending">
      <what>
          <include>
              //wi:watcherinfo/wi:watcher-list/wi:watcher[@wi:status="pending" or
   @wi:status="waiting"]
          </include>
      </what>
   </filter>
</filter-set>
```

B.2.2 Case 2: Watcher Information Subscriber wants to be notified only with XML elements used in the OMA Presence SIMPLE 1.1 release.

This example shows a Watcher Information Subscriber that wants to be notified only with XML elements from the "urn:ietf:params:xml:ns:watcherinfo" namespace used in OMA Presence SIMPLE V1.1 [PRS_ERELD]. This would improve the efficient use of network resources when a PS is upgraded to a later enabler release that introduces additional XML elements from other namespaces.

```
<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
   <filter id="default_OMA_PRS_V1_1">
      <what>
          <include type="namespace">urn:ietf:params:xml:ns:watcherinfo</include>
      </what>
   </filter>
</filter-set>
```

B.3 Examples of Presence Authorization Rule Documents based on Rules Template

B.3.1 "White-List" Presence Authorization Rule Document

The example contains a Presence Authorization Rules document for the Presentity "sip:joe@example.com" with all template rules that can be used to define a "white-list" Presence Authorization Rule document described in section 5.6.

An implementation can use a subset of the template rules, defined in Table 2, depending on its need.

Bold Italic text is used to indicate the values that can vary in a rule.
The example has been created using namespace prefixes for easy reading.

```
<?xml version="1.0" encoding="UTF-8"?>
<cr:ruleset
   xmlns:ocp="urn:oma:xml:xdm:common-policy"
   xmlns:pr="urn:ietf:params:xml:ns:pres-rules"
   xmlns:cr="urn:ietf:params:xml:ns:common-policy">

<!-- This rule describes that the Presentity has access to her/his own Presence Information -->
  <cr:rule id="wp_prs_allow_own">
    <cr:conditions>
      <cr:identity>
        <cr:one id="sip:joe@example.com"/>
      </cr:identity>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>allow</pr:sub-handling>
    </cr:actions>
    <cr:transformations>
      <pr:provide-services>
        <pr:all-services/>
      </pr:provide-services>
      <pr:provide-persons>
        <pr:all-persons/>
      </pr:provide-persons>
      <pr:provide-devices>
        <pr:all-devices/>
      </pr:provide-devices>
      <pr:provide-all-attributes/>
    </cr:transformations>
  </cr:rule>

<!-- This rule describes how an anonymous Watcher's request shall be handled -->
  <cr:rule id="wp_prs_block_anonymous">
    <cr:conditions>
      <ocp:anonymous-request/>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>block</pr:sub-handling>
    </cr:actions>
  </cr:rule>

<!-- This rule describes that a request from a Watcher not listed in any other rule is to be
   confirmed. -->
 <cr:rule id="wp_prs_unlisted">
    <cr:conditions>
      <ocp:other-identity/>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>confirm</pr:sub-handling>
    </cr:actions>
  </cr:rule>


<!-- This rule describes that a Watcher is granted access to all Presence Information if its user
   URI is included in the "oma_grantedcontacts" URI List in Shared XDMS-->
 <cr:rule id="wp_prs_grantedcontacts">
```

```
    <cr:conditions>
       <ocp:external-list>
              <ocp:entry anc="http://xcap.example.org/resource-lists/users/
       sip:joe@example.org/index/~~/resource-lists/list%5B@name=%22oma_grantedcontacts%22%5D"/>
       </ocp:external-list>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>allow</pr:sub-handling>
    </cr:actions>
    <cr:transformations>
      <pr:provide-services>
        <pr:all-services/>
      </pr:provide-services>
      <pr:provide-persons>
        <pr:all-persons/>
      </pr:provide-persons>
      <pr:provide-devices>
        <pr:all-devices/>
      </pr:provide-devices>
      <pr:provide-all-attributes/>
    </cr:transformations>
  </cr:rule>

<!-- This rule describes that a Watcher is blocked from accessing all Presence Information if its
   user URI is included in the oma_blockedcontacts list. -->
  <cr:rule id="wp_prs_blockedcontacts">
    <cr:conditions>
       <ocp:external-list>
              <ocp:entry anc="http://xcap.example.org/resource-lists/users/
       sip:joe@example.org/index/~~/resource-lists/list%5B@name=%22oma_blockedcontacts%22%5D"/>
       </ocp:external-list>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>block</pr:sub-handling>
    </cr:actions>
 </cr:rule>

<!--This rule describes that a single user is granted access to a certain set of Presence
   Information -->
  <cr:rule id="wp_prs_allow_one_1">
    <cr:conditions>
      <cr:identity>
        <cr:one id="sip:bob@example.com"/>
      </cr:identity>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>allow</pr:sub-handling>
    </cr:actions>
    <cr:transformations>
      <pr:provide-persons>
        <pr:all-persons/>
      </pr:provide-persons>
      <pr:provide-activities>true</pr:provide-activities>
    </cr:transformations>
  </cr:rule>

<!--This rule describes that users on a single list in Shared XDMS is granted access to a certain
   set of Presence Information. -->
  <cr:rule id="wp_prs_allow_onelist_1">
    <cr:conditions>
       <ocp:external-list>
              <ocp:entry anc="http://xcap.example.org/resource-lists/users/
              sip:joe@example.org/index/~~/resource-lists/list%5B@name=%22list-e%22%5D"/>
       </ocp:external-list>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>allow</pr:sub-handling>
    </cr:actions>
    <cr:transformations>
      <pr:provide-persons>
```

```
        <pr:all-persons/>
      </pr:provide-persons>
      <pr:provide-status-icon>true</pr:provide-status-icon>
    </cr:transformations>
  </cr:rule>

<!--This rule describes that a single user is 'polite-block'ed from accessing any Presence
   Information. -->
  <cr:rule id="wp_prs_one_1">
    <cr:conditions>
      <cr:identity>
        <cr:one id="sip:jason@example.com"/>
      </cr:identity>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>polite-block</pr:sub-handling>
    </cr:actions>
    <cr:transformations/>
  </cr:rule>

<!--This rule describes that users on a single list in Shared XDMS is 'polite-block'ed from
   accessing any Presence Information. -->
  <cr:rule id="wp_prs_onelist_1">
    <cr:conditions>
       <ocp:external-list>
              <ocp:entry anc="http://xcap.example.org/resource-lists/users/
                    sip:joe@example.org/index/~~/resource-lists/list%5B@name=%22list-c%22%5D"/>
       </ocp:external-list>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>polite-block</pr:sub-handling>
    </cr:actions>
    <cr:transformations/>
  </cr:rule>

</cr:ruleset>
```

NOTE: The 'list-c' is a part of "oma_blockedcontacts" URI List example in [XDM_IG] "*URI List Index Document*". In the above example, therefore, both 'wp_prs_onelist_1' rule and 'wp_prs_blockedcontacts' rule would be applicable for the 'list-c' and thus be combined upon rule evaluation. When combined, the 'polite-block' action of the <sub-handling> action element in the 'wp_prs_onelist_1' rule would be selected in the composite rule for the 'list-c', over the 'block' action of the <sub-handling> action element in the 'wp_prs_blockedcontacts' rule. This is because the value of 'polite-block' action (=20) is higher than that of 'block' action (=0) according to [RFC5025].

B.3.2 "Black-List" Presence Authorization Rule Document

The example contains a Presence Authorization Rules document for the presentity sip:joe@example.com with all template rules that can be used to define a "black-list" Presence Authorization Rule document described in section 5.6.

An implementation can use a subset of the template rules, defined in Table 2, depending on its need.

Bold Italic text is used to indicate the values that can vary in a rule.
The example has been created using namespace prefixes for easy reading.

```
<?xml version="1.0" encoding="UTF-8"?>
<cr:ruleset
   xmlns:ocp="urn:oma:xml:xdm:common-policy"
   xmlns:pr="urn:ietf:params:xml:ns:pres-rules"
   xmlns:cr="urn:ietf:params:xml:ns:common-policy">

<!-- This rule describes that a Watcher not listed in any other rule is allowed to see all Presence
   Information. The rule is used only when the "black-list" way is used -->
  <cr:rule id="wp_prs_allow_unlisted">
    <cr:conditions>
      <ocp:other-identity/>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>allow</pr:sub-handling>
    </cr:actions>
    <cr:transformations>
      <pr:provide-services>
        <pr:all-services/>
      </pr:provide-services>
      <pr:provide-persons>
        <pr:all-persons/>
      </pr:provide-persons>
      <pr:provide-devices>
        <pr:all-devices/>
      </pr:provide-devices>
      <pr:provide-all-attributes/>
    </cr:transformations>
 </cr:rule>

<!-- This rule describes that the Presentity has access to her/his own Presence Information -->
  <cr:rule id="wp_prs_allow_own">
    <cr:conditions>
      <cr:identity>
        <cr:one id="sip:joe@example.com"/>
      </cr:identity>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>allow</pr:sub-handling>
    </cr:actions>
    <cr:transformations>
      <pr:provide-services>
        <pr:all-services/>
      </pr:provide-services>
      <pr:provide-persons>
        <pr:all-persons/>
      </pr:provide-persons>
      <pr:provide-devices>
        <pr:all-devices/>
      </pr:provide-devices>
      <pr:provide-all-attributes/>
    </cr:transformations>
  </cr:rule>

<!-- This rule describes how an anonymous Watcher's request shall be handled -->
  <cr:rule id="wp_prs_anonymous">
    <cr:conditions>
      <ocp:anonymous-request/>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>block</pr:sub-handling>
```

```
    </cr:actions>
  </cr:rule>

<!-- This rule describes that a Watcher is blocked from accessing all Presence Information if its
   user URI is included in the “oma_blockedcontacts” URI List in Shared XDMS -->
  <cr:rule id="wp_prs_blockedcontacts">
    <cr:conditions>
       <ocp:external-list>
              <ocp:entry anc="http://xcap.example.org/resource-lists/users/
       sip:joe@example.org/index/~~/resource-lists/list%5B@name=%22oma_blockedcontacts%22%5D"/>
       </ocp:external-list>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>block</pr:sub-handling>
    </cr:actions>
 </cr:rule>

<!--This rule describes that a single user is granted access to a limited set of Presence
   Information -->
  <cr:rule id="wp_prs_allow_one_1">
    <cr:conditions>
      <cr:identity>
        <cr:one id="sip:bob@example.com"/>
      </cr:identity>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>allow</pr:sub-handling>
    </cr:actions>
    <cr:transformations>
      <pr:provide-persons>
        <pr:all-persons/>
      </pr:provide-persons>
      <pr:provide-activities>true</pr:provide-activities>
    </cr:transformations>
  </cr:rule>

<!--This rule describes that users on a single list in Shared XDMS is granted access to a limited
   set of Presence Information. -->
  <cr:rule id="wp_prs_allow_onelist_1">
    <cr:conditions>
       <ocp:external-list>
              <ocp:entry anc="http://xcap.example.org/resource-lists/users/
    sip:joe@example.org/index/~~/resource-lists/list%5B@name=%22list-e%22%5D"/>
       </ocp:external-list>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>allow</pr:sub-handling>
    </cr:actions>
    <cr:transformations>
      <pr:provide-persons>
        <pr:all-persons/>
      </pr:provide-persons>
      <pr:provide-status-icon>true</pr:provide-status-icon>
    </cr:transformations>
  </cr:rule>

<!--This rule describes that a single user is ‘polite-block’ed from accessing any Presence
   Information. -->
 <cr:rule id="wp_prs_one_1">
    <cr:conditions>
      <cr:identity>
        <cr:one id="sip:jason@example.com"/>
      </cr:identity>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>polite-block</pr:sub-handling>
    </cr:actions>
    <cr:transformations/>
  </cr:rule>
```

```
<!--This rule describes that users on a single list in Shared XDMS is ‘polite-block’ed from
   accessing any Presence Information. -->
 <cr:rule id="wp_prs_onelist_1">
    <cr:conditions>
       <ocp:external-list>
              <ocp:entry anc="http://xcap.example.org/resource-lists/users/
                     sip:joe@example.org/index/~~/resource-lists/list%5B@name=%22list-c%22%5D"/>
       </ocp:external-list>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>polite-block</pr:sub-handling>
    </cr:actions>
    <cr:transformations/>
  </cr:rule>

</cr:ruleset>
```

NOTE: The 'list-c' is a part of "oma_blockedcontacts" URI List example in [XDM_IG] “*URI List Index Document*”. In the above example, therefore, both ‘wp_prs_onelist_1’ rule and 'wp_prs_blockedcontacts' rule would be applicable for the 'list-c' and thus be combined upon rule evaluation. When combined, the ‘polite-block’ action of the <sub-handling> action element in the 'wp_prs_onelist_1' rule would be selected in the composite rule for the ‘list-c’, over the ‘block’ action of the <sub-handling> action element in the ‘wp_prs_blockedcontacts’ rule. This is because the value of ‘polite-block’ action (=20) is higher than that of ‘block’ action (=0) according to [RFC5025].