Isode

# XMPP Application Profile for use with XML Guard

12th July 2022

## 1 Overview

This white paper specifies an Application Profile for use of XMPP with an XML Guard. It defines:

- Schema for the Application Profile
- Normalization Requirements
- Rules which can be used to constrain the base profile

This sets out a product-independent specification of using XMPP with an XML Guard.

Application Profiles are summarized in the Isode white paper "XML Guard Application Profiles" . They define a product-independent approach to specify functionality across an XML Guard.

This profile has been developed to support XMPP usage as a (human) user service. Other profiles could be developed, for example to support Internet of Things type functionality through a guard.

The Schema, specified as an XML Schema Definition (XSD) specified an "outer bound" for what is allowed through the guard. For this profile the schema is chosen such that a modern XMPP Client such as Isode Swift or NATO JCHAT which is communicating across a guard for 1:1 messaging, group chat, and military services such as Forms Display and Publishing will work without loss of function.

The associated rules then constrain this schema, by blocking elements of the schema. This enables a basic service, which at minimum would be 1:1 messages or group chat only. The choice of rules leads to a trade-off between the service provide and constraints on what is allowed to flow across the guard. This is going to be driven by cross domain deployment requirements.

## 2 Schema Compliance

This profile is based on schemas from a number of standards. Unless noted otherwise, there is an associated rule for turning off use of the standard.

| Standard | Reason for Inclusion |
|---|---|
| RFC 6120 "Extensible Messaging and Presence Protocol (XMPP): Core" | This and the following RFC define the core XMPP protocols. The schema allows all of this protocol. Aspects of this can be constrained by rules. |

| Standard | Reason for Inclusion |
|---|---|
| RFC 6121 “Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence” | See above |
| XEP-0004: Data Forms | Forms are used for many management functions such as configuring a MUC room. XMPP clients make use of this. |
| XEP-0012: Last Activity | This protocol allows a client to discover when a peer was last active using IQ. |
| XEP-0030: Service Discovery | This is used to locate XMPP services and find information about them, for example to determine peer client capability. |
| XEP-0033: Extended Stanza Addressing | This enables an XMPP message to address multiple recipients. |
| XEP-0045: Multi-User Chat | MUC is the standard group chat protocol. |
| XEP-0047: Inband bytestreams | This is used for file transfer, by breaking up a file into multiple pieces. |
| XEP-0050: Ad-Hoc Commands | This is widely used by XMPP clients to control things. Use across a guard is allowed, but would be unusual. |
| XEP-0054: vCard Profile | Needed for exchange of Avatars |
| XEP 0055: Jabber Search | Useful to find information, for example to search for people. |
| XEP-0060: Publish-Subscribe | This is a general information sharing mechanism. It is anticipated that a guard following this profile will either block Publish-Subscribe entirely or only allow it for Forms Display and Publishing (XEP-00346). Future versions of this profile may include additional services operating over Publish-Subscribe. This schema also covers Personal Event Publishing (XEP-0163). |
| XEP-0071: XHTML-IM | This allows HTML alternate message renderings to be used. This will generally not be allowed across a guard. |

| Standard | Reason for Inclusion |
|---|---|
| XEP-0080: User Location | Specifies geographical location of user |
| XEP-0085: Chat State Notifications | Chat State Notifications provide additional status information, such as “user is typing”. |
| XEP 0092: Software Version. | Can be useful for debug |
| XEP 0115: Entity Capabilities | Optimizes service discovery. Widely used. |
| XEP-0122: Data Forms Validation | Extends forms capability |
| XEP-0128: Service Discovery Extensions | This extends service discovery and is used for core service discovery functions. |
| XEP-0141: Data Forms Layout | Extends forms capability |
| XEP-0153: vCard-Based Avatars | Used for exchanging Avatars. |
| XEP-0166: Jingle | Jingle is a generic peer negotiation mechanism. In this profile it is anticipated that it will only be used in conjunction with file transfer negotiation. |
| XEP-0172: User Nickname. | Allows users to share suggested nicknames |
| XEP-0184: Message Delivery Receipts. | Confirms message delivery to user |
| XEP-0199: XMPP Ping | Can be useful for detecting timeouts |
| XEP-0203: Delayed Delivery | This is used to indicate delays in message handling. |
| XEP-0231: Bits of Binary | Used to encode small binary elements |
| XEP-0234: Jingle File Transfer | Uses Jingle to negotiate file transfer. |
| XEP-0258: Security Labels in XMPP | This is a framework for associating a basic security label with a message, usually using ESS format security labels. |
| XEP-0261: Jingle In-Band Bytestreams Transport Method | An extended in band mechanism that uses XEP-0047 |
| XEP-0289: Federated MUC for Constrained Environments. | Allows MUC rooms to be federated across a guard. |

| Standard | Reason for Inclusion |
|---|---|
| XEP-0297: Stanza Forwarding | Allows stanzas to be forwarded |
| XEP 0319: Last User Interaction in Presence | Shows when user was last active, by communicating this information in presence |
| XEP-0346: Forms Display and Publishing | To access and submit forms across a guard |
| XEP-0350: Data Forms Geolocation Element | Geolocation data within forms |
| STANAG 4774 "CONFIDENTIALITY METADATA LABEL SYNTAX" | NATO Label Format |
| STANAG 4778 "METADATA BINDING MECHANISM" | Label Binding Mechanism |
| NATO SRD 4778.2 Chapter 4 “Extensible Message And Presence Protocol Binding Profile” | Specifies use of STANAG 4774 and STANAG 4778 in XMPP<br>This specification allows use of STANAG 4774 and STANAG 4778 with message stanzas and iq stanzas. |

Some of the base schemas allow generic extensibility, which allows inclusion of arbitrary data. This Application Profile constrains this so that only explicitly valid protocol is allowed. The schema required by this profile is intended to explicitly limit what is transferred.

XEP-0198 (Stream Management) is explicitly excluded, because the model of guard operation is the transfer of independent messages. There is no concept of a stream across the guard. Where reliable transfer of content between the two XMPP entities communicating through the XML guard is needed, XML guard reliability mechanisms are used. Where these mechanisms are unavailable or not used, reliable transfer of content is not assured.

As the cross domain service functions as a replacement for a standards server to server link, XEPs that apply only server to server do not make sense in this application profile. In particular XEP-0220 (Server Dialback) and XEP-0288 (Bidirectional Server-to-Server Connections) are not relevant.

XEP-0077 (In-Band Registration) is not supported, as it is inappropriate for use cross domain.

XML Normalization requires that XML namespaces are absolute, not relative. Most XMPP protocol follows this, but some (in particular vCard) does not. This profile requires that all namespaces are absolute. This means that the sending system needs to map all relative namespaces to absolute ones by pre-pending “http://isode.com/xmpp/relative/” and the receiving system needs to reverse this mapping.

A formal specification of this Application Profile will include these schemas as an appendix.

# 3 Normalization

This profile requires the following normalization of XMPP messages:

- Prohibition of XML Comments and XML Processing Instructions, which are not allowed in XMPP.
- Use of Canonical XML. Following Canonical XML Version 1.1 of May 2008.
- Unicode Normalization following UNICODE NORMALIZATION FORMS 13.0.0 using Normalization Form C (NFC) "Canonical Decomposition, followed by Canonical Composition"
- JIDs must be normalized following the rules if RFC 7622 "Extensible Messaging and Presence Protocol (XMPP): Address Format".

# 4 Rules

This version of the Application Profile defines the following associated rules, that may be enabled to further constrain the base schema. These rules are set out to broadly correspond to the schema order, but grouping related functions together.

| Rule | Notes |
|---|---|
| Prohibit 'chat' messages | This prevents 1:1 chat, by blocking messages of type chat from being transferred. It is anticipated that at a minimum either 1:1 or group chat will be allowed.<br>This rule will block both 1:1 chat directly between users and MUC Private Messages. If independent control of these types is needed, it is recommended to use domain controls, as a generic rule is expected to be unreliable. |
| Prohibit Normal messages | This blocks messages of type normal (individual recipient). It is anticipated that this will usually be set to the same value as Prohibit 'chat'. |
| Prohibit Error | This blocks messages of type error. It is anticipated that this rule will not usually be selected. |
| Prohibit GroupChat | This prevents group chat by blocking all stanzas of type groupchat in the core, which will block all groupchat, including MUC, FMUC and MIX. |
| Prohibit presence stanzas | Prevent sending of any presence information by restricting core protocol.<br>Note that XEP-0045 MUC requires presence support to work. |
| Prohibit presences with status elements | Allow presence, but do not allow presence status string |
| Maximum Presence Status Length | Limit size of presence status string. Where multiple presence status values are present, each presence status element must be less than this limit. |

| Rule | Notes |
|---|---|
| Prohibit presences with multiple status elements | Require that presence stanzas have a single presence status element or none. Note that multiple presence status elements are legal, where each has a different language. |
| No Subject | Block stanzas with subject set. Note that MUC makes use of Subject. |
| Prohibit Multiple Subject | Require that messages have a single subject element or no subject. Note that multiple subject elements are legal, where each has a different language. |
| Maximum Subject Length | Limit length of subject. Where multiple subject elements are present, each subject must be less than this limit. |
| Prohibit IQ Request | Prevents IQ queries from being sent in direction of guard. Model is that request/response requirements may vary by direction. Preventing IQ may be important to control access across boundary, but will reduce XMPP functionality available. |
| Prohibit IQ Response | Matching control for response |
| Maximum body length | Limit the size of a message body. Where multiple body parts are present, each body part must be less than this limit. |
| Prohibit messages with multiple body elements | Require that messages have a single <body/> element or none. Note that multiple body parts are legal, where each body part has a different language. |
| Prohibit 'headline' messages | This blocks messages of type headline. |
| Prohibit Dirty Words | Prohibit the message body element from containing any of the specified words. |
| Authorized Recipients | Prohibit the stanza unless all of the recipients are whitelisted. |
| Authorized Senders | Prohibit the stanza unless the sender is whitelisted. |
| Authorized Recipient Domains | Prohibit the stanza unless all of the recipients belong to a whitelisted domain. |
| Authorized Sender Domains | Prohibit the stanza unless the sender belongs to a whitelisted domain. |

| Rule | Notes |
|---|---|
| Prohibit Data Forms | Block XEP-0004, XEP-0122 and XEP-0141 (Data Forms and Data Forms Extensions). Note that this blocks forms in all places, which will prevent MUC from working. |
| Prohibit Last Activity | Block XEP-0012 (Last Activity) |
| Prohibity Service Discovery | Block XEP-0030, and XEP-0128 (Service Discovery and Service Discovery Extensions). This rule also blocks XEP-0115, which provides service discovery information. |
| Prohibit Multicast | Block XEP-0033 (Extended Stanza Addressing) |
| Prohibit Multi-User Chat | This prevents MUC communication by blocking XEP-0045 |
| Prohibit Ad Hoc Commands | Block XEP-0050 (Ad Hoc Commands) |
| Prohibit vCard | Block XEP-0054 (vCard Profiles) and XEP-0153 (vCard-Based Avatars) |
| Prohibit Search | Block XEP-0055 (Jabber Search) |
| Prohibit PubSub | Prevent use of any PubSub (XEP-0060). It is anticipated that either this rule or the next one will be selected and that general PubSub will not usually be allowed. |
| Prohibit PubSub except Form Discovery and Publishing | Allow XEP-0346 over PubSub, but not general PubSub |
| Prohibit HTML | Block HTML and XEP-0071 encoding |
| Prohibit User Location | Block XEP-0080 (User Location) |
| Prohibit CSN | Prevent Chat State Notifications (XEP-0085). May be desirable to avoid sharing these over domain boundary. |
| Prohibit Software Version Discovery | Block XEP-0092 (Software Version) |
| Prohibit Entity Capabilities | Block XEP-0115 (Entity Capabilities) |

| Rule | Notes |
|---|---|
| Prohibit File Transfer negotiation | Block XEP-0166 (Jingle) XEP-0234 (Jingle File Transfer). No other protocols for negotiating file transfer are allowed in the base schema. No other users of Jingle are allowed in this profile, so both protocols are blocked by this rule. This rule prevents file transfers being negotiated, and this will be used with the following rule which prevents the actual transfer. |
| Prohibit Inline File Transfer | Block XEP-261 (Jingle In-Band Bytestreams Transport Method) and XEP-0047 (Inband bytestreams) and XEP-0231 (Bits Of Binary). |
| Prohibit User Nickname | Block XEP-0172 (User Nickname) |
| Prohibit Message Delivery Receipts | Block XEP-0184 (Message Delivery Receipts) |
| Prohibit XMPP Pings | Block XEP-0199 (XMPP Ping) |
| Prohibit Delayed Delivery | Block XEP-0203 (Delayed Delivery) |
| Prohibit labelled (XEP-0258) messages | Messages must not have XEP-0258 labels |
| Prohibit unlabelled (XEP-0258) messages | All messages must have XEP-0258 labels |
| Authorized XEP-0258 Security Labels | Restricts XEP-0258 Security Label in the message payload to selected values |
| Prohibit Federated Multi-User Chat | Block XEP-0289 (Federated MUC for Constrained Environments). This blocks FMUC, while still allowing MUC. |
| Prohibit Multi-User Chat except Federated MUC | This requires that MUC is only allowed with FMUC. This will prevent use of MUC across the boundary, but allow FMUC rooms to be federated. This will force users to join an FMUC room on their side of the boundary and limit cross-boundary traffic to FMUC. |
| Prohibit Stanza Forwarding | Block XEP-0297 (Stanza Forwarding) |

| Rule | Notes |
|---|---|
| Prohibit Last User Interaction in Presence | Block XEP 0319 (Last User Interaction in Presence) |
| Prohibit Geolocation in forms | Block forms with XEP-0350 (Data Forms Geolocation Element) |
| Prohibit labelled "STANAG 4774" stanzas | Prohibits presence of a STANAG 4774 label on message or PubSub IQ stanzas (i.e., bound as per SRD 4778.2 Edition A Version 1). In this rule and the following rule the term “STANAG 4774 Label” is used to mean “A NATO Confidentiality Label as specified in STANAG 4774 carried in XMPP following Chapter 4 of SRD. Message stanzas and IQ stanzas must not include STANAG 4774 Labels. |
| Prohibit unlabelled "STANAG 4774" stanzas | Enforces presence of a STANAG 4774 label if the stanza is a message or a PubSub IQ stanza with an 'item' descendent. |
| Prohibit unless all contained “STANAG 4774 Labels” match | Require that any “STANAG 4474 Label” represented as a full XMPP Binding Object following the SRD is an exact match to one of a list of configured label binding objects. Note that this will not block a message without a label, so this rule will typically be used in conjunction with the 'Prohibit unlabelled "STANAG 4774" stanzas' rule. |
| Prohibit "STANAG 4774" Label not bound to whole message or IQ item | Require that if any "STANAG 4774 Label" is present, it must be bound to the entire data-object. In the case of a PubSub IQ stanza the entire data-object is considered to be the first child-element of the item element (cf. SRD 4778.2 Edition A Version 1) |
| Authorized "STANAG 4774" Labels security policies | Require that the security policy of any “STANAG 4774 Label” matches one of a list of specified object identifiers. This enforces that a label belongs to a specific policy (e.g., AMOCO) but does not place any other constraints on the label. This might be used where a policy is required, but all labels are valid. |
| Authorized "STANAG 4774" Labels security classifications | Require that the security classification of any “STANAG 4774 Label” matches one of a specified list of enumerated values, which can correspond to SECRET etc.<br>This rule will typically be used in conjunction with enforcing a single security policy. |