International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 22

(01/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1144 – Supplement on enhancements and new features in eXtensible Access Control Markup Language (XACML 3.0)

ITU-T X-series Recommendations – Supplement 22

ITU-T

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Supplement 22 to ITU-T X-series Recommendations

ITU-T X.1144 – Supplement on enhancements and new features in eXtensible Access Control Markup Language (XACML 3.0)

Summary

Supplement 22 to ITU-T X-series Recommendations summarizes the enhancements and new features of Recommendation ITU-T X.1144 (XACML 3.0) in comparison to Recommendation ITU-T X.1142 (XACML 2.0).

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 22	2014-01-24	17	11.1002/1000/12156

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 22 to ITU-T X-series Recommendations

ITU-T X.1144 – Supplement on enhancements and new features in eXtensible Access Control Markup Language (XACML 3.0)

1 Scope

Supplement 22 to ITU-T X-series Recommendations summarizes the enhancements and new features of XACML 3.0 compared to XACML 2.0 in the XACML core specification.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AC	Access Control
IPC	Intellectual Property Control
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
URI	Uniform Resource Identifier
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language
XPath	XML Path language

5 Conventions

None.

6 Enhancements and new features of XACML 3.0 compared to XACML 2.0

The following changes occur in the XACML core specification *OASIS eXtensible Access Control Markup Language (XACML) Version 3.0* which became an OASIS Standard on 22 January 2013.

- Advice element: This new feature is similar to obligations with the exception that policy enforcement points (PEPs) do not have to comply with the statement. PEPs can consider or discard the statement.

- Custom categories: In extensible access control markup language (XACML 3.0), users are given the option to create their own custom categories. However, in XACML 2.0, attributes have been organized into subject, resource, environment or action.
- Content element: In a XACML 2.0 request, there can only be extensible markup language (XML) content inside the resource category as part of the ResourceContent element. The ResourceContent element is generalized into a Content element that can be found in any category.
- Improvement in XACML request and response: As custom categories can be defined, many types of attribute categories can be found in the XACML 3.0 request. An XACML 2.0 request can contain only subject, resource, environment or action categories.
- Improvements in XML path language (XPath): New XPath data type has been introduced with XACML 3.0. In XACML 2.0, XPath has been defined as a string where it cannot be defined in the context that the namespace prefix is going to resolve. In addition, XPath-based multiple decision schemes have been introduced.
- New attribute functions and datatypes: XACML 3.0 brings in new datatypes and new functions that can be used for the attributes and attribute matching. In particular, XACML 3.0 utilizes XPath to manipulate attributes. Obligations in rules: XACML 3.0 provides that rules can contain obligations. There are several improvements with Obligations in XACML 3.0 when compared to XACML 2.0. One is the Obligation Expression. This would add dynamic expressions in to the obligation statements. In XACML 2.0, the obligation element needs to be defined with the user e-mail statically. However, the user would not be the same for each XACML request. Therefore, it is not possible to configure the e-mail statically in the Obligation element. The Obligation element can only say to PEP: "Please send e-mail to user" (leaving the possibility for PEP to figure out the value of the user's e-mail).

  However, in XACML 3.0, the e-mail of each user can be retrieved using the policy information point (PIP) in a dynamic manner as XACML 3.0 can define an expression element inside the ObligationExpression. Therefore, the Obligation element can say to PEP: "Please send e-mail to user@foo.com address".

  In XACML 2.0, Obligations can only be added to policies and policy sets. With XACML 3.0, rules can also contain Obligations.
- Policy combination algorithms: In XACML, policies are combined together to produce a single decision. Each policy can reach different decisions. These decisions must be combined to return a single result. XACML 3.0 enhances XACML 2.0's existing combination algorithms.
- Scope of XPath expressions: In XACML 2.0, XPath expressions apply to the root of the XACML request. In XACML 3.0, XPath expressions apply to the root of the Content element.
- Target element: XACML 3.0 removes the disjunctive (*or*) and conjunctive (*and*) function of the category elements and introduces the *AnyOf* and *AllOf* elements. The target element still bears the conjunctive function though. Note that XACML 2.0 had already introduced and defined the any-of and all-of functions but did not have the equivalent schema elements. XACML 3.0 specification explains the behaviour of the Target element and its children in XACML 3.0.
- Variables in the Obligation and Advice element: The administrator value can be determined at runtime, for instance through the policy information point (PIP). This enables richer scenarios such that in case of On deny, that tell the PEP to send an e-mail to the requestor's line manager. XACML 2.0 cannot cater for such an obligation, since at design-time it does not know who the requestor is and therefore does not know who their line manager is.

The following changes occur in the Profiles indicated below. They have not reached the OASIS Standard stage yet.

- Enhanced profiles:
  - The hierarchical resource profile presented in XACML 2.0 has been reviewed and enhanced in XACML 3.0 to allow a new scheme to encode hierarchy as uniform resource identifier (URI).
  - Multiple decision profile: Multiple resource request (XACML 2.0) was renamed as multiple decision profile and enhanced with new variants. The profile allows a typical policy enforcement point (PEP) requestor to ask several questions in one XACML request. It enhances performance as it reduces communication overhead between the PEP and the policy decision point (PDP).
  - SAML profile: The authorization decision query was enhanced to enable per-decision policies to be provided by the PEP. When used in conjunction with the delegation profile, a decision request may contain policies or policy sets which will be treated by the PDP as if they appeared in the top level policy set of the policies currently in effect at the PDP. These policies will be used only for that request and discarded after the response is sent. When a multiple decision request is made, these policies will be in effect for all the decisions in the request.
- New profiles:
  - Delegation profile: This is a new profile in XACML 3.0 that allows policies to be defined on who can write policies about what topic. The ability to delegate administrative rights in XACML has started with XACML 3.0. The delegation profile enables global administrators to delegate constrained administrative rights to local administrators. For instance, a global administrator can define access control (AC) policies for an entire set of resources within an organization. The administrator can also delegate the right to an administrator to manage a set of resources. An administrator's rights to define access control rules are constrained by the delegation policy that the global administrator has defined. The delegation profile is most useful in federation scenarios, cloud-based scenarios and in environments where the domains to be secured are so vast that they require local knowledge to define relevant policies.
  - XACML 3.0 provides additional profiles. In particular, a new profile for export compliance has been produced to help author policies that can cater for export compliance scenarios. Similarly, a new profile for intellectual property control (IPC) has been introduced.

Bibliography

[b-ITU-T X.1142] Recommendation ITU-T X.1142 (2006), *eXtensible Access Control Markup Language (XACML 2.0)*.

[b-ITU-T X.1144] Recommendation ITU-T X.1144 (2013), *eXtensible Access Control Markup Language (XACML 3.0)*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014