TTA Standard

정보통신단체표준(국문표준)
TTAS.IT-X1141_4 제정일: 2007 년 12 월 26 일

SAML 2.0 메타데이터

SAML 2.0 Metadata

TTA 한국정보통신기술협회
Telecommunications Technology Association

정보통신단체표준(국문표준)
TTAS.IT-X1411_4 제정일: 2007 년 12 월 26 일

SAML 2.0 메타데이터

SAML 2.0 Metadata

한국정보통신기술협회
Telecommunications Technology Association

본 문서에 대한 저작권은 TTA 에 있으며, TTA 와 사전 협의 없이 이 문서의 전체 또는 일부를 상업적 목적으로 복제 또는 배포해서는 안 됩니다.

Copyrightⓒ Telecommunications Technology Association 2007. All Rights Reserved.

서 문

1. 표준의 목적

SAML(Security Assertion Markup Language) 2.0은 분산된 환경에서 인증, 인가 및 속성 정보를 교환하기 위한 XML-기반 프레임워크이다. 이름에서 나타나듯이, SAML은 비즈니스 엔티티들이 어떤 주체의 신원, 속성 그리고 권한부여에 대한 주장을 파트너 회사 또는 다른 엔터프라이즈 응용 등과 같은 다른 엔티티들에게 보장할 수 있도록 해 준다. 이 표준은 SAML 메타데이터를 기술한다.

이 표준은 ITU-T X.1141 “Security Assertion Markup Language (SAML 2.0)”을 근거로 한 국내 표준으로 원문의 다음 내용을 포함하고 있다.

CL 1. 범위

CL 2. 참고문헌

CL 3. 용어정의

CL 4. 약어

CL 5. 관례

CL 7. 공통 데이터 타입

CL 9 SAML 메타데이터

부기 A.28 SAML 스키마 메타데이터

2. 주요 내용 요약

이 표준은 SAML 메타데이터 스키마, 전자 서명 처리 및 메타데이터의 게시 및 해결을 기술한다.

3. 표준 적용 산업 분야 및 산업에 미치는 영향

본 표준은 웹 싱글사인온, 속성 정보 기반 인가와 웹 서비스 보호에서 사용될 수 있다. 따라서, 본 표준은 ID 관리 분야와 웹 서비스 정보보호 분야에 직접적으로 적용되며, 정보보호 산업의 핵심 요소로 활용될 수 있다. 또한, ID 연계의 핵심 기술을 제공함으로써, 기업간 협업을 용이하게 함으로써 새로운 서비스를 창출하고 시장을 활성화할 수 있다.

4. 참조 표준(권고)

4.1. 국외 표준(권고)

- ITU-T, X.1141, 'Security Assertion Markup Language (SAML 2.0)', 2006.06.

4.2. 국내 표준

- TTA, TTAS.IF-X1411_1, 'SAML 2.0 주장과 프로토콜', 2006.12.
- TTA, TTAS.IF-X1411_2, 'SAML 2.0 바인딩', 2006.12.
- TTA, TTAS.IF-X1411_3, 'SAML 2.0 프로파일', 2006.12.

5. 참조표준(권고)과의 비교

5.1. 참조 표준(권고)과의 관련성

TTA TTAS.IF-X1411_1은 ITU-T X.1141 clause 8 (SAML assertion and protocols)의 내용을 포함하고 있으며, TTA TTAS.IF-X1411_2는 ITU-T X.1141 clause 10 (Bindings for SAML)의 내용을 포함하고 있으며, TTA TTAS.IF-X1411_3은 ITU-T X.1141 clause 11 (Profiles for SAML)의 내용을 포함하고 있다.

본 표준은 ITU-T X.1141 clause 9 (SAML metadata)의 내용과 Annex A.28 (SAML Schema metadata)을 포함하는 국내표준이다.

5.2. 참조한 표준(권고)과 본 표준의 비교표

상기 국제 권고에 대한 추가사항은 없으며, 장 구성은 다음과 같다.

TTAS.IT-X1141_4	ITU-T X.1141	비고
1.1. 범위	1. 범위	동일(번역)
1.2. 참고문헌	2. 참고문헌	동일(번역)
1.3. 용어정의	3. 용어정의	동일(번역)
1.4. 약어	4. 약어	동일(번역)
1.5. 관례	5. 관례	동일(번역)
1.6. 공통 데이터 타입	7. 공통 데이터 타입	동일(번역)
2~4. SAML 메타데이터	9. SAML 메타데이터	동일(번역)
부기 A. SAML 스키마 메타데이터	부기 A. 28 SAML 스키마 메타데이터	동일(번역)

6. 지적 재산권 관련 사항

본 표준의 '지적 재산권 확약서' 제출 현황은 TTA 웹사이트에서 확인할 수 있다.

※본 표준을 이용하는 자는 이용함에 있어 지적 재산권이 포함되어 있을 수 있으므로, 확인 후 이용한다.

※본 표준과 관련하여 접수된 확약서 이외에도 지적 재산권이 존재할 수 있다.

7. 시험 인증 관련 사항

7.1. 시험 인증 대상 여부

- 해당 사항 없음

7.2. 시험 표준 제정 현황

- 해당 사항 없음

8. 표준의 이력 정보

8.1. 표준의 이력

판 수	제정·개정일	제정·개정 내역
제1판	2007.12.26.	제정 TTAS.IT-X1141_4

8.2. 주요 개정 사항

- 해당 사항 없음

Preface

1. Purpose of Standard

SAML(Security Assertion Markup Language) is an XML-based framework for communicating user authentication, entitlement, and attribute information among disparate Web access management and security products. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. This standard specifies SAML metadata

This standard is a domestic standard based on ITU-T X.1141 “Security Assertion Markup Language (SAML 2.0)” and contains the following contents of the original standard.

CL 1. Scope

CL 2. References

CL 3. Definitions

CL 4. Abbreviations

CL 5. Conventions

CL 7. Common data types

CL 9. SAML metadata

Annex A.28 SAML Schema metadata

2. Summary of Contents

This standard specifies metadata schema, digital signature processing and metadata publication and resolution.

3. Applicable Fields of Industry and its Effect

This standard can be used in as web single-sign on, attribute information based authorization and web service security. Therefore, it is directly applicable to security areas such as ID Management and web service security. It is also applicable to other information security industry as essential component. In addition, it provides essential technology for ID federation, which makes companies' collaboration easy and so creates new service and revitalize IT market.

4. Reference Standards(Recommendations)

4.1. International Standards(Recommendations)

- ITU-T, X.1141, "Security Assertion Markup Language (SAML 2.0)," 2006.06.

4.2. Domestic Standards

- TTA, TTAS.IF-X1411_1, "SAML 2.0 Assertions and Protocols", 2006.12.
- TTA, TTAS.IF-X1411_2, "Bindings for SAML 2.0", 2006.12.
- TTA, TTAS.IF-X1411_3, "Profiles for SAML 2.0", 2006.12.

5. Relationship to Reference Standards(Recommendations)

5.1. Relationship of Reference Standards(Recommendations)

TTA TTAS.IF-X1411_1 contains the contents of ITU-T X.1141 clause 8 (SAML assertion and protocols), TTA TTAS.IF-X1411_2 contains the contents of ITU-T X.1141 clause 10 (Bindings for SAML) and TTA TTAS.IF-X1411_3 contains the contents of ITU-T X.1141 clause 11 (Profiles for SAML).

This standard is a domestic standard which contains the contents of ITU-T X.1141 clause 9 (SAML metadata) and Annex A.28 (SAML Schema metadata).

5.2. Differences between Reference Standard(Recommendation) and this Standard

This standard has no additional contents as to the international recommendations. The differences between the recommendation and this standard are as follows.

TTAS.IT-X1141_4	ITU-T X.1141	Remark
1.1. Scope	1. Scope	equaled(trans)
1.2. References	2. References	equaled(trans)
1.3. Definitions	3. Definitions	equaled(trans)
1.4. Abbreviations	4. Abbreviations	equaled(trans)
1.5. Conventions	5. Conventions	equaled(trans)
1.6. Common data types	7. Common data types	equaled(trans)
2~4. SAML metadata	9. SAML metadata	equaled(trans)
Annex A. SAML Schema metadata	Annex A. 28 SAML Schema metadata	equaled(trans)

6. Statement of Intellectual Property Rights

IPRs related to the present document may have been declared to TTA. The information pertaining to these IPRs, if any, is available on the TTA Website.

No guarantee can be given as to the existence of other IPRs not referenced on the TTA website.

And, please make sure to check before applying the standard.

7. Statement of Testing and Certification

7.1. Object of Testing and Certification

- None

7.2. Standards of Testing and Certification

- None

8. History of Standard

8.1. Change History

Edition	Issue Date	Outline
The 1st edition	2007.12.26.	Established TTAS.IT-X1141_4

8.2. Revisions

- None

목 차

Contents

SAML 2.0 메타데이터

(SAML 2.0 Metadata)

1. SAML 2.0 개요

1.1. 범위(Scope)

SAML 2.0은 시스템 엔티티가 어떤 주체에 대하여 생성한 주장의 문법과 처리 규칙을 정의한다. 이와 같은 주장을 만들거나 또는 의지하기 위해, SAML 시스템 엔티티들은 주장 자체 또는 주장의 주체에 대한 내용을 통신하기 위해 다른 프로토콜을 사용할 수 있다. SAML 2.0은 SAML 보장의 구조, 관련된 프로토콜 집합, 그리고 SAML 시스템을 관리하는데 관련된 처리 규칙들을 정의한다.

SAML 주장과 프로토콜 메시지들은 XML로 인코딩되어 있으며, XML 네임스페이스를 사용한다. 이것들은 일반적으로 HTTP POST 또는 XML로 인코딩된 SOAP 메시지와 같은 전송을 위한 다른 구조에 내장된다. SAML 2.0은 또한 SAML 프로토콜 메시지들을 내장하고 전송하기 위한 프레임워크를 제공하는 SAML 바인딩을 명기한다. 더욱이, SAML 2.0은 SAML 특징들을 사용할 때, 특정 사용 예(use case)를 달성하고 상호운용성을 달성하기 위해, SAML 주장과 프로토콜을 어떻게 사용해야 하는지에 대한 기본 프로파일 집합을 제공한다.

SAML 2.0은 다음을 정의한다.

1. SAML 에 대한 적합성 요구사항
2. SAML 주장과 프로토콜
   - SAML 주장 스키마
   - SAML 프로토콜 스키마
3. SAML 바인딩

4. SAML 프로파일

   - SAML ECP 프로파일 스키마
   - SAML X.500/LDAP 속성 프로파일 스키마
   - SAML DCE PAC 속성 프로파일 스키마
   - SAML XACML 속성 프로파일 스키마

5. SAML 메타데이터

6. SAML 메타데이터 스키마

7. SAML 인증 문맥

1.2. 참고문헌

다음 권고안들과 다른 참조들은 SAML 2.0에서 참조되는 것들이다. SAML 2.0의 발간 시에는 모두 유효한 상태이다. 모든 권고안들과 다른 참조들은 개정될 수 있으며, SAML 2.0에 기반으로 하는 모든 사용자들은 아래 나열된 권고안들과 다른 참조들에 대하여 가장 최신 판을 적용할 수 있다. ITU의 전기통신 표준국(Telecommunications Standardization Bureau)에서 현재 유효한 ITU-T 권고안들의 리스트를 유지한다. ITEF는 최근에 폐지된 것들과 함께 RFC 리스트를 유지한다. W3C, Unicode Consortium과 Liberty Alliance도 가장 최신의 권고안들과 다른 문서들에 대한 리스트를 유지한다.

- ITU-T Recommendation X.660 (2004), Information technology - Open Systems Interconnection - Procedures for the operation of OSI Registration Authorities: General procedure. .
- ITU-T Recommendation X.667 (2004), Information technology - Open Systems Interconnection - Procedures for the operation of OSI Registration Authorities: Generation and Registration of Universally Unique Identifiers (UUIDs) and their Use as ASN.1 Object Identifier Components.

- ITU-T Recommendation X.680 (2002), Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation.
- ITU-T Recommendation X.800 (1991), Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.
- ITU-T Recommendation X.811 (1995), Security Frameworks for Open Systems: Authentication Framework.
- ITU-T Recommendation X.812 (1995), Security Frameworks for Open Systems: Access control framework.
- ITU-T Recommendation X.1142 (2006), Extensible Access Control Markup Language (XACML 2.0).
- IETF RFC 1034:1987, Domain Names - Concepts and Facilities, 1987.
- IETF RFC 1510:1993, The Kerberos Network Authentication Requestor (V5), 1993.
- IETF RFC 1750:1994, Randomness Recommendations for Security, 1994.
- IETF RFC 1951:1996, DEFLATE Compressed Data Format Specification Version 1.3, 1996.
- IETF RFC 1991:1996, PGP Message Exchange Formats, 1996.
- IETF RFC 2045:1996, Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message, 1996.
- IETF RFC 2119:1997, Key words for use in RFCs to Indicate Requirement Levels, 1997.
- IETF RFC 2246:1999, The TLS Protocol Version 1.0, 1999.
- IETF RFC 2253:1997, Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished, 1997.
- IETF RFC 2396:1998, Uniform Resource Identifiers (URI): Generic Syntax, 1998.
- IETF RFC 2535:1999, Domain Name System Security Extensions, 1999.
- IETF RFC 2616 :1999, Hypertext Transfer Protocol - HTTP/1.1, 1999.

- IETF RFC 2617:1999, HTTP Authentication: Basic and Digest Access Authentication, 1999.
- IETF RFC 2798:2000, Definition of the inetOrgPerson LDAP Object Class, 2000.
- IETF RFC 2828:2000, Internet Security Glossary, 2000.
- IETF RFC 2914:2000, Congestion Control Principles, 2000.
- IETF RFC 2915:2000, The Naming Authority Pointer (NAPTR) DNS Resource Record, 2000.
- IETF RFC 2945:2000, The SRP Authentication and Key Exchange System, 2000.
- IETF RFC 2965:2000, HTTP State Management Mechanism, 2000.
- IETF RFC 3061:2001, A URN Namespace of Object Identifiers, 2001.
- IETF RFC 3075:2001, XML-Signature Syntax and Processing, 2001.
- IETF RFC 3513:2003, Internet Protocol Version 6 (IPv6) Addressing Architecture, 2003.
- IETF RFC 3023:2001, XML Media Types, 2001.
- IETF RFC 3377:2002, Lightweight Directory Access Protocol (v3): Technical Specification, 2002.
- IETF RFC 3403:2002, Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database, 2002.
- IETF RFC 3546:2003, Transport Layer Security (TLS) Extensions, 2003.
- IETF RFC 3923:2004, End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP), 2004.
- IETF RFC 4122:2005, A Universally Unique IDentifier (UUID) URN Namespace, 2005.
- Liberty Alliance POAS:2003, R. Aarts, Reverse HTTP Binding for SOAP Specification Version 1.0, Liberty Alliance Project, 2003.
- OASIS WSS:2006, WS-Security Core Specification 1.1, February, 2006.
- UNICODE-C, M. Davis, M. J. Dürst, Dürst. Unicode Normalization Forms. UNICODE Consortium, March 2001.

- W3C Canonicalization:2002, Exclusive XML Canonicalization Version 1.0, W3C Recommendation, Copyright © [2 July 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/xml-exc-c14n/.
- W3C Character Model:2005, Character Model for the World Wide Web 1.0: Fundamentals, W3C Recommendation, Copyright © [15 February 2005] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2005/REC-charmod-20050215/.
- W3C Datatypes:2001, XML Schema Part 2: Data types, W3C Recommendation, Copyright © [2 May 2001] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/.
- W3C Encryption:2002, XML Encryption Syntax and Processing, W3C Recommendation, Copyright © [10 December 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/.
- W3C Web Services Glossary:2004, Web Services Glossary, W3C Note, Copyright © [11 February 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/ws-gloss/.
- W3C HTML:1999, HTML 4.01 Specification, W3C Recommendation, Copyright © [24 December 1999] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/REC-html40/.

- W3C Namespaces:1999, Namespaces in XML, W3C Recommendation, Copyright © [14 January 1999] World Wide Web Consortium (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/REC-xml-names/.
- W3C Primer:2005, SOAP Version 1.2 Part 0: Primer, W3C Recommendation, Copyright © [24 June 2005] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2003/REC-soap12-part0-20030624/.
- W3C Signature:2002, XML Signature Syntax and Processing, W3C Recommendation, Copyright © [12 February 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/xmldsigcore/.
- W3C Signature Schema:2001, XML Signature Schema, W3C Recommendation, Copyright © [1 March 2001] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd.
- W3C String:1998, Requirements for String Identity Matching and String Indexing, W3C Note, Copyright © [10 July 1998] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/WD-charreq.
- W3C SOAP:2000, Simple Object Access Protocol (SOAP) 1.1, W3C Note, Copyright © [08 May 2000] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2000/NOTE-SOAP-20000508.
- W3C XHTML:2002, The Extensible HyperText Markup Language (Second Edition), W3C Recommendation, Copyright © [1 August 2002] World Wide Web Consortium,

(Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/xhtml1/.

- W3C XML 1.0:2004, Extensible Markup Language (XML) 1.0 (Third Edition), W3C Recommendation, Copyright © [4 February 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/REC-xml/.
- W3C XML Schema Part 1:2001, XML Schema Part 1: Structures, W3C Recommendation, Copyright © [2 May 2001] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/.

주의 – SAML 2.0 문서 내에 있는 문서에 대한 참조는 참조되는 문서의 상태를 제공하지는 않는다.

1.3. 용어 정의

SAML 2.0에 대해, 다음과 같은 용어 정의가 적용된다.

1.3.1. 들여온 정의들(Imported definitions)

1.3.1.1. SAML 2.0은 ITU-T Rec. X.667에서 정의된 다음 용어들을 사용한다.

a) UUID

1.3.1.2. SAML 2.0은 ITU-T Rec. X.680에서 정의된 다음 용어들을 사용한다.

a) 객체 식별자(Object identifier);

b) 오픈 타입 표기법(Open type notation).

1.3.1.3. SAML 2.0은 ITU-T Rec. X.811에서 정의된 다음 용어들을 사용한다.

사용자(Principle).

1.3.1.4. SAML 2.0은 ITU-T Rec. X.812에서 정의된 다음 용어들을 사용한다.

a) 접근 제어 정보(Access control information);

b) 사용자(User).

1.3.1.5. SAML 2.0은 W3C 웹 서비스 어휘에서 정의된 다음 용어들을 사용한다.

a) 초기 SOAP 송신자(Initial SOAP sender);

b) 네임스페이스(Namespace);

c) 최종 SOAP 수신자(Ultimate SOAP receiver);

d) XML 스키마(XML schema).

1.3.1.6. SAML 2.0은 IETF RFC 2828에서 정의된 다음 용어들을 사용한다.

a) 접근(Access);

b) 접근 제어(Access control);

c) 프락시(Proxy);

d) 프락시 서버(Proxy server);

e) 푸시(Push);

f) 풀(Pull);

g) 보안 아키텍처(Security architecture);

h) 보안 정책(Security policy);

i) 보안 서비스(Security service).

1.3.1.7. SAML 2.0은 IETF RFC 2396에서 정의된 다음 용어들을 사용한다.

a) Uniform resource identifier (URI);

b) URI 참조(URI reference).

1.3.2. 추가적인 용어 정의(Additional definitions)

1.3.2.1. 접근 권한(Access rights)

주체가 자원에 대하여 가질 수 있는 인가된 상호작용의 타입을 설명. 예로는 읽기, 쓰기, 실행, 추가, 변경 그리고 삭제를 들 수 있다.

1.3.2.2. 계정(Account)

사용자와 비즈니스 서비스 제공자 사이에 정상적인 거래와 서비스를 제공하기 위한 형식적인 비즈니스 협약.

1.3.2.3. 계정 연결(Account linkage)

서로 다른 두 제공자에서 동일한 사용자를 나타내는 계정을 연관시키는 방법. 이를 통해 두 제공자들은 그 사용자에 대한 정보를 통신할 수 있다. 계정 연결은 속성 공유나 또는 Identity 연계(federation)을 통해 설정될 수 있다.

1.3.2.4. 능동적인 역할(Active role)

예를 들어 자원에 접근하는 등, 어떤 연산을 수행할 때, 시스템 엔티티가 가지는 역할.

1.3.2.5. 관리 도메인(Administrative domain)

하나 또는 그 이상의 관리 정책, 인터넷 도메인 이름 등록들, 공공 법률 엔티티들(예를 들어, 개인, 기업 또는 다른 조직), 호스트, 네트워크 디바이스 그리고 상호 연결되는 네트워크의 집합, 그리고 그들 위에서 동작하는 네트워크 서비스와 응용들의 어떠한 조합으로 정의되는 환경 또는 문맥. 관리 도메인은 하나 또는 그 이상의 보안 도메인을 포함하거나 또는 정의할 수 있다. 하나의 관리 도메인은 단일한 사이트 또는 다중 사이트를 포함할 수 있다. 관리 도메인을 정의하는 특징들은 시간이 지남에 따라 진화할 수 있다. 관리 도메인들은 관리 도메인 경계를 넘어 서비스를 제공하거나 또는 소비하는 것에 대하여 협약을 만들 수 있다.

1.3.2.6. 관리자(Administrator)

시스템을 설치하거나 또는 관리하는 사람 또는 시스템을 이용하여 시스템 엔티티, 사용자와/또는 내용을 관리하는 사람. 관리자는 일반적으로 특정 관리 도메인에 가입하게 되고 하나 이상의 관리 도메인에 가입할 수도 있다.

1.3.2.7. 가맹, 가맹 그룹(Affiliation, affiliation Group)

사용자(principal)에 대한 식별자들의 (연계 관점에서) 단일한 네임스페이스를 공유하는 시스템 엔티티 집합.

1.3.2.8. 익명성(Anonymity)

익명 상태. 이것은 이름이나 신원이 알려지거나 노출되지 않도록 하는 조건을 나타냄.

1.3.2.9. 보장하는 기관(Asserting party)

공식적으로, 하나 또는 그 이상의 SAML 기관을 호스트팅하는 관리 도메인. 비공식적으로, SAML 기관의 한 인스턴스.

1.3.2.10. 주장(Assertion)

주체에 대하여 수행되는 인증 행위, 주체에 대한 속성 정보 또는 명기된 자원에 대하여 주체가 행할 수 있는 인가 데이터 등에 대하여 SAML 기관이 생성한 데이터 조각.

1.3.2.11. 속성(Attribute)

객체의 독특한 특성. 실세계 객체에 대하여, 속성들은 종종 크기, 모양, 무게 및 색깔 등과 같은 물리적인 특징들로 명기된다. 사이버스페이스에서 객체는 크기, 인코딩 타입, 네트워크 주소 등등을 설명하는 속성들을 가질 수 있다. 속성들은 종종 “속성 이름”과 “속성 값(들)로 표현된다. 예를 들어, “foo”는 값 ‘bar’를 가지며, “count”는 값 1을, “gizmo”는 ‘frob”과 ‘2”를 값들로 가진다.

1.3.2.12. 속성 주장(Attribute assertion)

주체의 속성들에 대한 정보를 운반하는 주장.

1.3.2.13. 속성기관(Attribute authority)

속성 주장들을 생성하는 시스템 엔티티.

1.3.2.14. 인증(Authentication)

인증은 어떤 사람 또는 어떤 사물이 어느 정도의 신뢰 내에서 그것이 자신이 그렇다고 선언하는 것이 정말로 맞는지 아닌지를 결정하는 과정이다.

1.3.2.15. 인증 주장(Authentication assertion)

주체에 대하여 발생된 성공적인 인증 행위에 대한 정보를 운반하는 주장.

1.3.2.16. 인증 기관(Authentication authority)

인증 주장들을 생성하는 시스템 엔티티.

1.3.2.17. 인가(Authorization)

어떤 주체가 특정 자원에 대하여 명기된 타입의 접근을 수행하는 것이 허가되었는지를, 적용가능한 접근제어 정보를 평가함으로써, 결정하는 과정. 일반적으로, 인가는 인증 문맥 내에 있다. 일단 주체가 인증이 되면, 그것은 다른 타입들의 접근을 수행하는 것에 대하여 인가될 수 있다.

1.3.2.18. 인가 결정(Authorization decision)

인가 행위의 결과. 그 결과는 부정적인 될 수 있다. 즉, 그것은 주체가 자원에 대한 어떠한 접근 권한도 없음을 가리킨다.

1.3.2.19. 인가 결정 주장(Authorization decision assertion)

인가 결정에 대한 정보를 운반하는 주장.

1.3.2.20. 후 채널(Back channel)

후 채널은, 예를 들어 사용자 에이전트인 HTTP 클라이언트와 같은 또 다른 시스템 엔티티를 통하여 메시지를 리다이렉트(redirect) 하지 않고 두 시스템 엔티티들 사이에 직접적인 통신을 가리킨다.

1.3.2.21. 바인딩, 프로토콜 바인딩(Binding, protocol binding)

일반적으로, 어떤 프로토콜 메시지와 메시지 교환 패턴을 구체적인 방식으로 또 다른 프로토콜로 매핑시키는 것에 대한 명세임. 예를 들어, SAML <AuthnRequest> 메시지를 HTTP에 매핑하는 것은 바인딩의 한 예가 된다. 동일한 SAML 메시지를 SOAP으로 매핑하는 것은 또 다른 바인딩이 된다. SAML 문맥에서는, 각각의 바인딩에 “SAML xxx binding”이라는 패턴의 이름이 주어진다.

1.3.2.22. 크리덴셜(Credentials)

주장되는 사용자(principal) 신원을 확인하기 위해 전송되는 데이터.

1.3.2.23. 최종 사용자(End user)

응용 목적으로 자원을 사용하는 자연인(natural person).

1.3.2.24. 엔티티(Entity)

“시스템 엔티티”를 참고한다.

1.3.2.25. 연계하다(Federate)

둘 또는 그 이상의 엔티티들을 함께 연결하거나 또는 바인딩하기.

1.3.2.26. 연계(Federation)

이 용어는 두가지 의미로 사용된다.:

1. 두 엔티티 사이에 관계를 설정하는 행위.
2. 어떠한 개수의 서비스 제공자들과 아이덴터티 제공자들로 구성된 하나의 연합(association).

1.3.2.27. 연계된 아이덴터티(Federated identity)

제공자들 사이에 그 사용자를 참조하기 위해 사용되는 식별자 집합과 속성들에 대하여 협정(agreement)가 있을 때, 사용자(principal)의 아이덴터티는 연계가 되었다고 말해진다.

1.3.2.28. 전 채널(Front channel)

전 채널은 두 개의 HTTP로 통신하는 서버들이 “HTTP redirect” 메시지를 채용하고 이를 통해, 예를 들어 웹 브라우저 또는 다른 어떠한 HTTP 클라이언트인 사용자 에이전트를 경유하여 상호간에 메시지를 전달하는 경우에 효과가 발생되는 통신 채널을 가리킨다.

1.3.2.29. 식별자(Identifier)

시스템 엔티티들 유일하게 가리키도록 시스템 엔티티에 매핑된 데이터 객체. 예를 들어 문자열이 될 수 있음. 시스템 엔티티는 그것을 가리키는 다중 식별자를 가질 수 있다. 하나의 식별자는 본질적으로 엔티티의 “구별되는 속성”이다.

1.3.2.30. 아이덴터티, 신원(Identity)

엔티티의 본질. 어떤 사물의 아이덴터티는 어떤 사물의 특징들로 종종 설명된다. 이 특성들 중에 식별자들이 포함될 수 있다.

1.3.2.31. 아이덴터티 탈연계(Identity defederation)

제공자들이 일정 집합의 식별자와/또는 속성들을 통해 사용자(principal)을 참조하는 것을 그만두기로 동의할 때, 발생하는 동작.

1.3.2.32. 아이덴터티 연계(Identity federation)

사용자(principal)을 위해 연계된 아이덴터티를 생성하는 동작.

1.3.2.33. 아이덴터티 제공자(Identity provider)

사용자(principal)들을 위해 아이덴터티 정보를 생성하고, 유지하며, 관리하고 그리고 웹 브라우저 프로파일과 같이 하나의 연계 내에서 다른 서비스 제공자에게 사용자(principal) 인증을 제공하는 일종의 서비스 제공자.

1.3.2.34. 아이덴터티 제공자 라이트(Identity provider lite)

단지 SAML에서 요구되는 부분만을 사용하여, 사용자(principal)들을 위해 아이덴터티 정보를 생성하고, 유지하며, 관리하고 그리고 웹 브라우저 프로파일과 같이 하나의 연계 내에서 다른 서비스 제공자에게 사용자(principal) 인증을 제공하는 일종의 서비스 제공자.

1.3.2.35. 로그인, 로그온, 사인-온(Login, logon, sign-on)

일종의 처리. 이 처리를 통해 사용자가 인증기관에게 크리덴셜을 제출하고 간단한 세션을 설정하고 그리고 선택적으로 리치(rich) 세션을 설정한다.

1.3.2.36. 로그아웃, 로그오프, 사인-오프(Logout, logoff, sign-off)

일종의 처리. 이 처리를 통해 사용자는 단순 세션 또는 리치(rich) 세션을 종료하기를 원한다는 것을 알린다.

1.3.2.37. 마크업 언어(Markup language)

특수한 목적으로 XML 문서의 구조에 적용되는 일단의 XML 요소들과 XML 속성들. 마크업 언어는 일반적으로 일단의 XML 스키마들과 동반되는 문서로 정의된다.

1.3.2.38. 이름 제한자(Name qualifier)

다른 사용자들(principals)을 나타내기 위해, (연계 관점에서) 하나 이상의 네임 스페이스에서 사용될 수 있는 하나의 식별자가 모호해지지 않도록 해 주는 문자열.

1.3.2.39. 기관, 당사자(Party)

비공식적으로, 주장을 수신하거나 또는 자원을 접근하는 것과 같은 어떤 처리나 통신에 참여하는 하나 또는 그 이상의 사용자들(principals).

1.3.2.40. 영속적인 의사익명(Persistent pseudonym)

다중 세션에 걸쳐있는 확장된 기간 동안에 주어진 의지하는 기관이 사용자를 식별할 수 있도록, 어떤 아이덴터티 제공자에 의해 할당된 프라이버시-보호형 이름 식별자. 아이덴터티 연계를 나타내는데 사용될 수 있다.

1.3.2.41. 정책 결정점(Policy decision point (PDP))

자신을 위해 인가 결정을 내리거나 또는 이와 같은 결정을 요구하는 다른 시스템 엔티티를 위해 인가 결정을 내리는 시스템 엔티티. 예를 들어, SAML PDP는 인가 결정 요청들을 받아들여, 응답으로 인가 결정 주장들을 생성한다. PDP는 인가 결정 기관이다.

1.3.2.42. 정책 집행점(Policy enforcement point (PEP))

인가 결정을 요청하고 뒤이어 집행하는 시스템 엔티티. 예를 들어, SAML PEP는 일가 결정 요청들을 PDP에게 전달하고, 응답으로 수신되는 인가 결정 주장들을 처리한다.

1.3.2.43. 사용자 아이덴터티(Principal identity)

일반적으로 식별자인 어떤 사용자 아이덴터티의 표현.

1.3.2.44. 프로파일(Profile)

여러 목적 중에 하나를 위한 일단의 규칙들. 각각의 집합은 “SAML xxx 프로파일” 또는 “xxx SAML 프로파일” 패턴으로 이름이 주어진다.

1. 어떤 프로토콜 또는 다른 사용 문맥에 주장을 내장시키거나 또는 그것들로부터 추출하는 방법에 대한 규칙들.
2. 특수한 사용 문맥에서 SAML 프로토콜 메시지를 사용하는 것에 대한 규칙들.
3. SAML 로 표현된 속성들을 또 다른 속성 표현 시스템으로 매핑시키는 것에 대한 규칙들. 이와 같은 규칙의 집합은 “속성 프로파일”로 알려진다.

1.3.2.45. 프로토콜 바인딩(Protocol binding)

“바인딩”을 참고한다.

1.3.2.46. 제공자(Provider)

아이덴터티 제공자들과 서비스 제공자들 둘 다를 가리키는 포괄적인 표현.

1.3.2.47. 의지하는 기관(측)(Relying party)

다른 시스템 엔티티가 제공한 정보를 기반으로 행동을 취할 것을 결정하는 시스템 엔티티. 예를 들어, SAML 의지하는 기관은 주체에 대하여 보장하는 기관(SAML 기관)이 제공한 주장들을 의지한다.

1.3.2.48. 요청자(Requester)

또 다른 시스템 엔티티(SAML 기관, 응답자)에게 서비스를 요청하기 위해 SAML 프로토콜을 활용하는 시스템 엔티티. 많은 시스템 엔티티들이 클라이언트와 서버 둘 모두로서 동시에 또는 순차적으로 동작하기 때문에, 이 표시법에서 “클라이언트”라는 용어는 사용되지 안 된다. SAML SOAP 바인딩이 사용중인 경우에는, SAML 요청자는 초기 SOAP 송신자와 구조적으로 분리된다.

1.3.2.49. 자원(Resource)

(예를 들어, 파일 형태나 메모리 형태, 등등으로) 하나의 정보 시스템에 포함되는 데이터, 또한:

1. 시스템이 제공하는 서비스.
2. 시스템 장비의 한 항목(다른 말로, 하드웨어, 펌웨어, 소프트웨어 또는 문서등과 같은 시스템 컴포넌트)

1.3.2.50. 응답자(Responder)

또 다른 시스템 엔티티(요청자)로부터 전달받은 서비스 요청에 대하여 응답하기 위해 SAML 프로토콜을 활용하는 시스템 엔티티(SAML 기관). 많은 시스템 엔티티들이 클라이언트와 서버 둘 모두로서 동시에 또는 순차적으로 동작하기 때문에, 이 표시법에서 “서버”라는 용어는 사용되지 안 된다. SAML SOAP 바인딩이 사용중인 경우에는, SAML 응답자는 최종 SOAP 수신자와 구조적으로 분리된다.

1.3.2.51. 역할, 롤(Role)

사전들은 역할을 “수행자에 의해 동작되는 특성” 또는 “함수 또는 위치)로 정의한다. 시스템 엔티티들은 예를 들어 능동적인 역할들과 수동적인 역할들과 같은 다양한 타입들의 역할들을 순차적으로/또는 동시적으로 수행한다. 관리자의 개념은 종종 역할의 한 예이다.

1.3.2.52. SAML 아티팩트(SAML artifact)

일반적으로 더 크고, 가변-크기의 SAML 프로토콜 메시지를 가리키는 작고, 고정-크기를 가지는 구조화된 데이터 객체. SAML 아티팩트들은 “3xx Redirection” 상태 코드들을 가지는 HTTP 응답 메시지들과 뒤따르는 HTTP GET 메시지들과 같이 URL에 내장되고 HTTP 메시지들을 통해 운반되도록 설계된다. 이런 방식으로, 서비스 제공자는 간접적으로, 사용자 에이전트를 경유하여, 다른 제공자에게 SAML 아티팩트를 전달할 수 있다. 다른 제공자는 artifact를 제공하는 제공자와의 직접적은 상호작용을 통해 SAML 아티팩트를 디레퍼런스(dereference)하여 SAML 프로토콜 메시지를 얻을 수 있다.

1.3.2.53. SAML 기관(SAML authority)

SAML 도메인 모델에서 주장들을 발급하는 추상적인 시스템 엔티티. 속성 기관, 인증 기관, 정책 결정점(PDP)를 또한 참고한다.

1.3.2.54. 보안(Security)

정보의 기밀성을 보장하고, 그것을 처리하는데 사용되는 시스템과 네트워크를 보호하고, 그들에 대한 접근을 제어하는 일단의 보호방법들. 보안은 일반적으로 비밀(secrecy), 기밀성, 무결성, 이용가능성 등의 개념을 포괄한다. 이것은 어떤 시스템이 잠재적으로 상호연관된 공격들을 방어하는 것을 보장하기 위한 것이다.

1.3.2.55. 보안 주장(Security assertion)

보안 아키텍처의 문맥에서 철저히 검사된 주장.

1.3.2.56. 보안 문맥(Security context)

개별적인 SAML 프로토콜 메시지에 대하여, 메시지의 보안 문맥은 만약 있다면 메시지의 보안 헤더 블록들과 수신자에게 메시지를 배달할 때, 사용될 수 있는 다른 보안 메커니즘들의 의미적인 합(semantic union)이다. HTTP, TLS와 IPSEC등과 같은 하부 네트워크 스택 레이어들에서 채택되는 보안 메커니즘들이 후자의 예가 된다.

1.3.2.57. 보안 도메인(Security domain)

일단의 자원들과 그들 자원들을 접근하는 것이 인가된 시스템 엔티티들을 포함하여, 보안 모델과 보안 아키텍처에서 정의된 환경 또는 문맥. 하나 또는 그 이상의 보안 도메인들이 단일 관리 도메인(administrative domain)에 존재할 수 있다. 어떠한 보안 도메인을 정의하는 특징들은 시간이 지남에 따라 일반적으로 진화한다.

1.3.2.58. 보안 정책 표현(Security policy expression)

사용자(principal) 아이덴터티들과 또는 그것의 속성들을 허용가능한 동작들(actions)로 매핑하는 것. 보안 정책 표현은 종종 본질적으로 접근 제어 리스트가 된다.

1.3.2.59. 서비스 제공자(Service provider)

어떤 시스템 엔티티에게 주어진 역할. 이 역할을 통해 그 시스템 엔티티는 사용자들(principals) 또는 다른 시스템 엔티티들에게 서비스들을 제공한다.

1.3.2.60. 서비스 제공자 라이트(Service provider lite)

어떤 시스템 엔티티에게 주어진 역할. 이 역할을 통해 그 시스템 엔티티는 단지 필요한 SAML 프로토콜 부분만을 사용하여, 사용자들(principals) 또는 다른 시스템 엔티티들에게 서비스들을 제공한다.

1.3.2.61. 세션(Session)

상호작용 기간 동안 상호작용에 대한 일부 상태를 유지하는 것을 특징으로 하는, 종종 사용자를 포함하는(Principal), 시스템 엔티티들의 지속적인 상호작용.

1.3.2.62. 세션 기관(Session authority)

세션들과 관련된 상태를 어떤 시스템 엔티티가 유지할 때, 그 기관에게 주어진 역할.

1.3.2.63. 세션 참여자(Session participant)

어떤 기관이 적어도 하나의 세션 기관과 어떤 세션에 참여할 때, 그 기관에게 주어진 역할.

1.3.2.64. 사인-오프(Sign-off)

“로그아웃”을 참고한다.

1.3.2.65. 사인-온(Sign-on)

“로그인”을 참고한다.

1.3.2.66. 사이트(Site)

지리적인 또는 DNS 이름 관점에서 하나의 관리 도메인을 나타내는 비공식적인 용어. 이것은 어떤 관리 도메인의 특정 지리적인 또는 위상적인

(topological) 부분을 나타낼 수도 있고, 또는 하나의 ASP 사이트에서 그렇듯이, 다중 관리 도메인들을 포괄할 수도 있다.

1.3.2.67. 주체(Subject)

어떤 보안 도메인 문맥에서 하나의 사용자(principal). SAML 주장들은 주체에 대한 선언들을 생성한다.

1.3.2.68. 시스템 엔티티, 엔티티(System entity, entity)

컴퓨터/네트워크 시스템의 능동적인 어떤 요소. 예를 들어, 자동화된 처리 또는 처리 집합. 하부 시스템, 분리된 기능 집합을 통합하는 사람 또는 사람들 그룹.

1.3.2.69. 타임-아웃(Time-out)

만약 어떤 사건이 발생하지 않았다면, 그 시각 이후, 어떤 조건이 “참”이 되는 기간. 예를 들어, 세션의 상태가 특정 기간 동안 비활성화되어 있었기 때문에 종료되는 세션은 “타임 아웃” 되었다고 말해진다.

1.3.2.70. 일시적인 의사익명(Transient pseudonym)

다중 세션에 걸쳐있을 필요가 없는 상대적으로 짧은 기간 동안에 주어진 의지하는 기관이 사용자를 식별할 수 있도록, 어떤 아이덴터티 제공자에 의해 할당된 프라이버시-보호형 이름 식별자.

1.3.2.71. XML 요소(XML attribute)

XML 요소의 시작-태그(start-tag)에 포함되어 있고, 이름과 값을 가지는 XML 데이터 구조.

1.3.2.72. XML 요소(XML element)

XML 문서 내에서 다른 이와 같은 구조들 사이에서 구조적으로 배열되며, 시작-태그(start-tag)와 종료-태그(end-tag) 또는 빈 태그(empty tag)로 가리켜지는 XML 데이터 구조.

1.3.2.73. SAML 메타데이터(SAML Metadata)

SAML 시스템 엔티티에 대한 정보를 제공하는 데이터.

1.4. 약어(Abbreviations)

AA	Attribute Authority
ASN.1	Abstract Syntax Notation One
ASP	Application Service Provider
CA	Certification Authority
CMP	Certificate Management Protocol
CRL	Certificate Revocation List
DDDS	Dynamic Delegation Discovery System
DCE	Distributed Computing Environment
DNS	Domain Name System
ECP	Enhanced Client/Proxy
HTTP	HyperText Transfer Protocol

HTTPS	Secure HyperText Transport Protocol
IdP	Identity Provider
IdP Lite	Identity Provider Lite
IP	Internet Protocol
IPSEC	Internet Protocol SECurity
MD5	Message Digest algorithm 5
MIME	Multipurpose Internet Mail Extensions
NAPTR	Naming Authority PoinTeR
OID	Object IDentifier
PAC	Privilege Attribute Certificates
PAOS	Reverse SOAP
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PGP	Pretty Good Privacy
PKI	Public-Key Infrastructure
POP	Proof Of Possession
RA	Registration Authority
RSA	Rivest Shamir Adleman public key algorithm
SHA-1	Secure Hash Algorithm 1
SP	Service Provider
SPKI	Simple Public Key Infrastructure
SP Lite	Service Provider Lite
SSO	Single Sign On
TLS	Transport Layer Security protocol
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time
UUID	Universal Unique IDentifier

XACML eXtensible Access Control Markup Language

XML eXtensible Markup Language

1.5. 관례(Conventions)

SAML 2.0에서 사용되는 키워드인 "해야만 한다(must)", "하지 않아야만 한다(must not)", "요구된다(required)", "일 것이다(shall)", "이지 않을 것이다(shall not)", "해야 한다(should)", "하지 않아야 한다(should not)", "권고된다(recommended)", "일(할) 수 있다(may)", "선택적인(optional)" 은 IETF RFC 2119에서 설명된 것과 같이 해석되어야 한다.

SAML 2.0은 W3C XML 스키마 Part 1, W3C 스키마 Part 2와 그들 표준들의 규범적 텍스트(normative text)를 사용하여 XML 인코딩된 SAML 주장과 프로토콜 메시지들의 문법과 의미를 설명한다. SAML 2.0의 SAML 스키마 문서들과 스키마 리스트 사이에 불일치가 발생할 경우에는, 스키마 문서가 높은 우선순위를 가진다. 어떤 경우에는, SAML 2.0이 스키마 문서에 의해 가리키는 것 이상의 제약을 가하는 경우가 있다는 것에 주의해야 한다.

1.6. 공통 데이터 타입(Common data types)

다음 하부 절들은 SAML 스키마들에서 나타나는 공통된 데이터 타입들을 어떻게 사용하고 해석하는지를 정의한다.

1.6.1. 문자열 값(String Values)

모든 SAML 문자열 값들은 **xs:string** 타입을 가지며, 이 타입은 W3C XML 스키마 데이터타입들 표준에 내장(built in) 되어 있다. SAML 2.0에서 별다른 언급이 없으면, SAML 메시지들에 존재하는 모든 문자열들은 적어도 하나 이상의 공백이 아닌 문자(non-whitespace)로 구성되어야만 한다.

이 SAML 2.0 또는 특정 프로파일들에서 별다른 언급이 없으면, XML 스키마 xs:string 타입을 가지거나 또는 이 문자열 타입으로부터 유도된 타입을 가지는 SAML 문서 내의 모든 요소들은 정확한 이진 비교(exact binary comparison)를 사용하여 비교되어야만 한다. 특히, SAML 구현과 배치(deployment)들은 대소문자를 구분하지 않는 문자열 비교, 공백의 정규화 또는 절단(trimming) 또는 숫자나 화폐와 같이 로케일에 따라 고유한(locale-specific) 변환 등에 의존하지 않아야만 한다. 이 요구는 W3C 문자열의 요구사항을 따르게 하기 위해 의도된 것이다.

만약 어떤 구현이 다른 문자 인코딩(encodings) 방식들을 사용하여 표현된 값들을 비교한다면, 그 구현은 두 값을 유니코드 문자 인코딩인 정규화 폼 C(Normalization Form C)로 변환하고 그것들에 대하여 정확한 이진 비교를 수행한 것과 같은 결과를 반환하는 비교 방법을 사용해야만 한다. 이 요구는 W3C 문자 모델과 특히, 유니코드-정규화 텍스트(Unicode-normalized Text)들에 대한 규칙을 따르게 하기 위해 의도된 것이다.

SAML 문서 형태로 받은 데이터와 외부 소스로부터 받은 데이터를 비교하는 응용(application)은 XML에 대해 규정된 정규화 규칙을 고려해야만 한다. 요소들 내에 포함된 텍스트(text)는 라인의 끝이 라인피드 문자들(ASCII code 10Decimal)을 사용하여 나타내도록 정규화된다. 문자열들 (또는 문자열로부터 유도된 타입들)로 정의된 XML 속성 값들은 W3C XML 1.0, 3.3.3절에서 설명된 것처럼 정규화된다. 모든 공백 문자들은 스페이스(blanks) (ASCII code 32Decimal)로 대체된다.

SAML 2.0은 XML 속성 값들 또는 요소 내용에 대하여 대조(collation) 또는 정렬 순서를 정의하지 않는다. SAML 구현들은 값들에 대하여 특정한 정렬 순서들에 의존하지 않아야만 한다. 왜냐하면 처리에 참여한 호스트(host)들에서 설정된 로케일(locale)에 따라, 그 정렬 순서들이 달라지기 때문이다.

1.6.2. URI 값(URI Values)

모든 SAML URI 참조 값들은 xs:anyURI 타입을 가지며, 이 타입은 W3C XML 스키마 데이터타입들에 내장(built in) 되어 있다.

SAML 2.0에서 다르게 지시되지 않는다면, SAML에서 정의된 속성들 또는 요소들 내에

서 사용되는 모든 URI 참조 값들은 적어도 하나 이상의 공백이 아닌 문자로 구성되어야만 하며, 절대경로를 표현하도록 요구된다.

SAML 2.0은 상태코드, 포맷 타입, 속성과 시스템 엔티티 이름들 등과 같은 식별자들로써 URI 참조를 광범위하게 사용한다. 따라서, 똑 같은 URI가 다른 시각에 다른 정보를 나타내는데 절대로 사용되지 않도록, URI 값들이 유일하고 동시에 일관되도록 (consistent) 하는 것이 필수적이다.

1.6.3. 시간 값(Time Value)

모든 SAML의 시각 값들은 xs:dateTime 타입을 가지며, 이 타입은 W3C XML 스키마 데이터타입들에 내장(built in) 되어 있다. 모든 SAML 시각 값들은 시간대(time zone) 컴포넌트가 없는 UTC 형식(form)으로 표현되어야만 한다.

SAML 시스템 엔티티들은 1000분의 1초보다 더 정교한 시각에 의존하지 않아야 한다. 구현들은 윤초(leap seconds)를 명기하는 시각 값들을 생성하지 않아야만 한다.

1.6.4. ID 와 ID 참조 값(ID and ID Reference Values)

xs:ID 단순 타입은 주장들, 요청 및 응답에 대한 SAML 식별자들(identifiers)을 선언하는데 사용된다. SAML 2.0에서 xs:ID 타입으로 선언된 값들은 xs:ID 타입 자체의 정의에 의해 주어진 특성뿐만 아니라 다음과 같은 특성들을 만족시켜야만 한다.

- 식별자들은 할당하는 어떠한 기관(party)도 자신 또는 다른 기관(party)이 다른 데이터 객체에게 우연히 동일한 식별자를 할당할 수 있는 가능성이 거의 무시할 수 있을 정도라는 것을 보장해야만 한다.
- 어떤 데이터 객체가 자신이 특정한 식별자를 가지고 있다고 선언한 곳에, 그와 같은 선언은 정확히 하나만 있어야만 한다.

SAML 시스템 엔티티가 그것이 생성하는 식별자가 유일하다는 것을 보장하는 메커니즘은 시스템 구현에 의해 결정된다. 랜덤(random) 또는 의사랜덤(pseudorandom) 기술이

채택된 경우에, 임의적으로 선택된 두 개의 식별자가 서로 동일할 확률은 2^{-128} 보다 작거나 같아야만 하고, 2^{-160} 보다 작거나 같아야 한다. 이 요구는 128 비트와 160 비트 사이의 길이를 갖는 임의적으로 선택된 값을 인코딩함으로써 충족될 수 있다. 인코딩은 xs:ID 데이터타입을 정의하는 규칙을 준용해야만 한다. 의사랜덤 발생기는 서로 다른 시스템들 사이에 바람직한 유일성 특성을 보장하기 위해 유일한 값(material)으로 시드(seed)를 설정하여야만 한다.

xs:NCName 단순 타입은 SAML에서 xs:ID 타입의 식별자들을 참조하는데 사용된다. 이렇게 하는 이유는 xs:IDREF가 이런 목적으로 사용될 수 없기 때문이다. SAML에서, SAML 식별자 참조에 의해 참조되는 요소는 식별자 참조가 사용되는 문서와 다른 문서에서 실질적으로 정의될 수 있다. xs:IDREF를 사용하게 되면, 그것의 값이 동일한 XML 문서에 있는 어떤 요소의 ID 속성 값과 매치(match) 되어야 한다는 요구를 위반하게 될 것이다.

2. 메타데이터

SAML 프로파일은 식별자, 바인딩 지원과 종점(endpoint), 인증서와 키 등에 대하여 시스템 엔티티들 사이에 협정이 필요하다. 본 장에서는 SAML 프로파일을 반영하는 역할에 따라 구성된 SAML 시스템 엔티티들에 대한 확장가능한 메타데이터 포맷을 정의한다. 이와 같은 역할에는 SSO 아이덴터티 제공자, SSO 서비스 제공자, 제휴(affiliation), 속성 기관, 속성 요청자 및 정책 결정점의 역할을 포함한다.

SAML 메타데이터는 시스템 엔티티가 지원하는 SAML 프로토콜들과 프로파일의 일반적인 조합들을 표현하는 역할들의 확장가능한 집합으로 구성된다. 각각의 역할은 확장가능한 기본 타입인 RoleDescriptor로부터 유도된 요소에 의해 설명된다. 이 설명자들은 다시 SAML 메타데이터의 주요한 단위인 <EntityDescritor> 컨테이너(container)에 포함된다. 엔티티는 서비스 제공자들의 제휴와 같이 다른 엔티티들의 제휴를 표현할 수도 있으며 <AffiliationDescriptor>이 이 목적으로 제공된다.

이와 같은 설명자들은 다시 <EntitiesDescriptor> 요소를 사용하여 중첩된(nested) 그룹으로 표현될 수 있다.

메타데이터의 신뢰성을 설정하기 위해 다양한 보안 메커니즘들이 지원될 수 있다. 특히 이 표준에서 정의된 대부분의 요소들은 개별적으로 전자서명될 수 있다.

부모 자식의 관계를 갖는 요소들이 캐싱(caching)이나 유효기간 만료 정보와 같은 공통 속성들을 포함할 때, 부모 요소가 자식 요소에 대해 우선 순위를 갖는다.

주의 : 일반적으로, SAML 메타데이터는 시스템 엔티티에 대한 능력이나 선택사항들에 대한 인가문(authoritative statement)으로 취급되지 않는다. 즉, 메타데이터는 정확하게 기술되어야 하지만, 그것을 철저(exhaustive)하게 의지할 필요는 없다. 특정 선택사항이 생략되었다고 해서, 시스템 엔티티가 그것을 지원하거나 또는 지원하지 않는다는 것을 의미하는 것은 아니다. 예를 들어, 어떤 SAML 속성 기관은 <AttributeAuthorityDescriptor>안에 명명되지 않은 속성들을 지원할 수 있다. 생략은 프라이버시나 다른 고려사항을 반영할 수도 있다. 반대로, 어떤 속성을 지원한다는 것을 가리키는 것이 주어진 요청자가 그것을 받을 수 있거나 또는 받을 것이라는 것을 암시하는 것은 아니다.

2.1. 네임스페이스

SAML 메타데이터는 다음 네임스페이스를 사용한다.

```
urn:oasis:names:tc:SAML:2.0:metadata
```

이 표준은 위 네임스페이를 참조하기 위해 네임스페이스 접두사 “md:”를 사용한다.

다음 스키마 조각은 SAML 메타데이터 문서들에서 네임스페이스의 사용을 설명한다.

```
<schema
    targetNamespace="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <import namespace="http://www.w3.org/2000/09/xmldsig#"
        schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd"/>
    <import namespace="http://www.w3.org/2001/04/xmlenc#"
        schemaLocation="http://www.w3.org/TR/2002/REC-xmlenc-core-
20021210/xenc-schema.xsd"/>
    <import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
        schemaLocation="saml-schema-assertion-2.0.xsd"/>
    <import namespace="http://www.w3.org/XML/1998/namespace"
        schemaLocation="http://www.w3.org/2001/xml.xsd"/>
    <annotation>
```

```
        <documentation>
            Document identifier: saml-schema-metadata-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
              V2.0 (March, 2005):
                Schema for SAML metadata, first published in SAML 2.0.
        </documentation>
    </annotation>
...
</schema>
```

2.2. 공통 타입

본 절에서는 메타데이터 요소들과 속성들에서 공통으로 사용되는 여러 가지 메타데이터 타입을 정의한다.

2.2.1. entityIDType 단순 타입

이 단순 타입은 XML 스키마 데이터 타입 **anyURI** 이 최대 1,024 문자 길이를 갖도록 제한한다. **entityIDType**은 SAML 엔티티들에 대한 유일 식별자로써 사용된다. 이 타입의 식별자는 주어진 배치(deployment) 환경에서 상호작용을 하는 모든 엔티티들에서 유일해야만 한다. URI를 사용하고 단일 URI가 다른 엔티티들을 참조해서는 안 된다는 규칙을 준수하면 이 요구사항을 만족시키게 된다.

다음 스키마 조각은 **entityIDType** 단순 타입을 정의한다.

```
<simpleType name="entityIDType">
   <restriction base="anyURI">
       <maxLength value="1024"/>
   </restriction>
</simpleType>
```

2.2.2. EndpointType 복합 타입

복합 타입 **EndpointType**은 프로토콜 메시지가 전달되는 SAML 엔티티의 SAML 프로토콜 바인딩 종점을 설명한다. 다양한 프로토콜 또는 프로파일에 특정한 메타데이터 요소들이 이 타입에 구속(bound)될 수 있다. 이 타입은 다음 속성들로 구성된다.

Binding [Required]

종점에 의해 지원되는 SAML 바인딩을 기술하는 필수적인 속성으로 각각의 바인딩에는 그것을 식별하는 하나의 URI가 할당된다.

Location [Required]

종점의 위치를 기술하는 필수적인 URI 속성으로 이 URI에 허용되는 문법은 프로토콜 바인딩에 의존한다.

ResponseLocation [Optional]

프로토콜 또는 프로파일의 일부로써 응답 메시지가 전달되는 위치를 선택적으로 기술한다. 이 URI에 허용되는 문법은 프로토콜 바인딩에 의존한다.

ResponseLocation 속성은 부하 균형(load balancing) 또는 백업 수단이 아닌, 프로토콜 또는 프로파일과 연관된 요청과 응답 메시지들을 전달받기 위해 요청과 서로 다른 종점들이 기술될 수 있도록 하기 위해 사용된다. 어떤 역할이 단지 한 타입의 메시지만 적용이 가능한 프로토콜 또는 프로파일에 관계된 타입의 요소를 포함한다면, 이 속성은 사용되지 않는다.

주의(informative): PE41(OASIS PE:2006 참조)는 위 문장의 의미를 다음과 같은 문장을 추가함으로써 명확히 하고 있다.

만약 ResponseLocation 속성이 생략된다면, 어떤 프로토콜 또는 프로파일과 연관된 어떠한 응답 메시지도 Location 속성에서 지시된 URI에서 처리된다는 것을 가정할 수 있다.

대부분의 문맥에서, 이 타입의 요소는 스키마에서 비종속 연속(unbounded sequence)에 나타난다. 이것은 일반적으로 다른 프로토콜 바인딩과 함께, 하나의 프로토콜 또는 프로파일이 다중 종점들에서 엔티티에 의해 제공되는 것을 허용한다. 이렇게 함으로써, 메타데이터 소비자(consumer)는 그것의 필요에 따라 적절한 종점을 선택할 수 있다. 또한 다중 종점은 특히 비동기 프로토콜 바인딩의 경우, “클라이언트-측” 부하 균형 또는 장애 극복(failover)을 제공할 수 있다.

이 요소는 또한 비-SAML 네임스페이스에서 정의된 임의의 요소들과 속성들이 사용되는 것을 허용한다.

다음 스키마 조각은 **EndpointType** 복합 타입을 정의한다.

```
<complexType name="EndpointType">
   <sequence>
      <any namespace="##other" processContents="lax" minOccurs="0"
           maxOccurs="unbounded"/>
   </sequence>
   <attribute name="Binding" type="anyURI" use="required"/>
   <attribute name="Location" type="anyURI" use="required"/>
   <attribute name="ResponseLocation" type="anyURI" use="optional"/>
   <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
```

2.2.3. IndexedEndpointType 복합 타입

이 타입은 다른 방식으로 동일한 종점들의 인덱싱을 허용하기 위해 한 쌍의 속성들의 추가하여 **EndpointType**를 확장한다. 이를 통해 동일한 종점들이 프로토콜 메시지들에 의해 참조될 수 있다. 이 타입에서 추가되는 속성들은 다음과 같다.

index [Required]

종점이 프로토콜 메시지에서 참조될 수 있도록, 종점에 유일한 정수 값을 할당하는 필수적인 요소이다. 인덱스 값은 단지 동일한 부모 요소 내에 포함된 유사한 요소들의 모임 내에서만 유일하면 된다(즉, 이들은 전체 인스턴스 상에서 유일할 필요는 없

다).

isDefault [Optional]

인덱스된 집합 사이에서 기본(default) 종점을 지시하기 위해 사용되는 선택적인 부울린(boolean) 속성. 만약 생략되면, 이 값은 “false”로 가정된다.

이 타입에 기반한 유사한 종점들의 어떠한 연속에서도, 기본 종점은 isDefault 속성이 “true”로 설정된 첫 번째 종점이 된다. 만약 그러한 종점이 존재하지 않으면, 기본 종점을 isDefault 속성이 “false”로 설정되지 않은 첫 번째 종점이 된다. 만약 이러한 종점도 존재하지 않으면, 기본 종점은 연속에서 첫 번째 요소가 된다.

주의(informative): PE37(OASIS PE:2006 참조)는 다음 문장을 가지고 위 문단의 의미를 명확히 하고 있다.

공통 요소 이름과 네임스페이스를 공유하는 인덱스된 종점들의 어떠한 연속에서도(즉, 하나의 역할에 포함된 <md:AssertionConsumerService>의 모든 인스턴스), 기본 종점은 isDefault 속성이 “true”로 설정된 첫 번째 종점이다. 만약 그러한 종점들이 존재하지 않으면, isDefault 기본 종점은 속성이 “false”로 설정되지 않은 첫 번째 종점이 된다. 만약 그러한 종점도 존재하지 않으면, 기본 종점은 연속에서 첫 번째 요소가 된다.

다음 스키마 조각은 **IndexedEndpointType** 복합 타입을 정의한다.

```
<complexType name="IndexedEndpointType">
    <complexContent>
        <extension base="md:EndpointType">
            <attribute name="index" type="unsignedShort" use="required"/>
            <attribute name="isDefault" type="boolean" use="optional"/>
        </extension>
    </complexContent>
</complexType>
```

2.2.4. localizedNameType 복합 타입

이 타입은 표준 XML 언어 속성을 가지고 문자열을 값으로 가지는 요소를 확장한다.다음 스키마 조각은 localizedNameType 복합 타입을 정의한다.

```
<complexType name="localizedNameType">
    <simpleContent>
        <extension base="string">
            <attribute ref="xml:lang" use="required"/>
        </extension>
    </simpleContent>
</complexType>
```

2.2.5. localizedURIType 복합 타입

이 타입은 표준 XML 언어 속성을 가지고 URI를 값으로 갖는 요소를 확장한다.

다음 스키마 조각은 localizedURIType 복합 타입을 정의한다.

```
<complexType name="localizedURIType">
    <simpleContent>
        <extension base="anyURI">
            <attribute ref="xml:lang" use="required"/>
        </extension>
    </simpleContent>
</complexType>
```

2.3. 루트 요소들

SAML 메타데이터 인스턴스(instance)는 단일 엔티티나 또는 다중 엔티티들을 설명한다. 전자의 경우, 루트(root) 요소는 <EntityDescriptor>가 되어야만 한다. 후자의 경우 루트 요소는 <EntitiesDescriptor>가 되어야만 한다.

2.3.1. <EntitiesDescriptor> 요소

이 요소는 선택적으로 명명된 SAML 엔티티들의 그룹을 위한 메타데이터를 포함한다. 이 요소의 **EntitiesDescriptorType** 복합 타입은 <EntityDescriptor> 요소들, <EntitiesDescriptor> 요소들 또는 둘 모두의 연속을 포함한다.

ID [Optional]

일반적으로 전자서명을 할 때 참조 포인트로 사용되는 요소를 위한 문서 내에서 유일한 식별자이다.

validUntil [Optional]

이 요소에 포함된 메타데이터와 다른 요소들의 만료 시각을 가리키는 선택적인 요소이다.

cacheDuration [Optional]

이 요소에 포함된 메타데이터와 다른 요소들을 소비자가 캐시해야하는 최대 시각을 가리키는 선택적인 요소이다.

Name [Optional]

어떤 배치 환경에서 SAML 엔티티들의 그룹을 식별하는 문자열 이름이다.

<ds:Signature> [Optional]

ITU-T X.1141 8장에서 설명된 것과 같이, 포함하는 요소와 그것의 내용을 인증하는 XML 전자서명이다.

<Extensions> [Optional]

이것은 메타데이터 게시자와 소비자 사이에 협약된 선택적인 메타데이터 확장을 포함한다. 확장 요소들은 SAML에서 정의되지 않은 네임스페이스에 한정(namespace qualified)되어야만 한다.

<EntitiesDescriptor> 또는 <EntityDescriptor> [One or More]

하나 또는 그 이상의 SAML 엔티티들에 대한 메타데이터나 또는 추가적인 메타데이터의 중첩된 그룹을 포함한다.

메타데이터 인스턴스의 루트 요소로 사용될 때, 이 요소는 validUntil 또는 cacheDuration 둘 중에 하나는 포함해야만 한다. 메타데이터 인스턴스의 루트 요소는 둘 중에 한 속성만 포함하는 것을 권고한다.

다음 스키마 조각은 <EntitiesDescriptor> 요소와 그것의 EntitiesDescriptorType 복합 타입을 정의한다.

```
<element name="EntitiesDescriptor" type="md:EntitiesDescriptorType"/>
<complexType name="EntitiesDescriptorType">
    <sequence>
        <element ref="ds:Signature" minOccurs="0"/>
        <element ref="md:Extensions" minOccurs="0"/>
        <choice minOccurs="1" maxOccurs="unbounded">
            <element ref="md:EntityDescriptor"/>
            <element ref="md:EntitiesDescriptor"/>
        </choice>
    </sequence>
    <attribute name="validUntil" type="dateTime" use="optional"/>
    <attribute name="cacheDuration" type="duration" use="optional"/>
    <attribute name="ID" type="ID" use="optional"/>
    <attribute name="Name" type="string" use="optional"/>
</complexType>
<element name="Extensions" type="md:ExtensionsType"/>
<complexType final="#all" name="ExtensionsType">
    <sequence>
        <any namespace="##other" processContents="lax"
maxOccurs="unbounded"/>
    </sequence>
</complexType>
```

2.3.2. <EntityDescriptor> 요소

이 요소는 단일 SAML 엔티티에 대한 메타데이터를 기술한다. 단일 엔티티는 다중 프로파일을 지원하는 많은 다른 역할을 수행할 수 있다. 이 표준은 확장을 위해 추상적인 <RoleDescriptor> 요소뿐만 아니라 다음과 같은 구체적인 역할을 직접적으로 지원한다.

- SSO 아이덴터티 제공자
- SSO 서비스 제공자
- 인증 기관
- 속성 기관
- 정책 결정점
- 제휴

이 요소의 EntityDescriptorType 복합 타입은 다음과 같은 요소와 속성으로 구성된다.

entityID [Required]

요소의 내용에 의해 설명되는 메타데이터가 어떤 SAML 엔티티인지를 나타내는 유일한 식별자를 기술한다.

ID [Optional]

일반적으로 전자서명을 할 때 참조 포인트로 사용되는 요소를 위한 문서 내에서 유일한 식별자이다.

validUntil [Optional]

이 요소에 포함된 메타데이터와 다른 요소들의 만료 시각을 가리키는 선택적인 요소이다.

cacheDuration [Optional]

이 요소에 포함된 메타데이터와 다른 요소들을 소비자가 캐시해야하는 최대 시각을 가리키는 선택적인 요소이다.

<ds:Signature> [Optional]

ITU-T X.1141 8장에서 설명된 것과 같이, 포함하는 요소와 그것의 내용을 인증하는 XML 전자서명이다.

<Extensions> [Optional]

이것은 메타데이터 게시자와 소비자 사이에 협약된 선택적인 메타데이터 확장을 포함한다. 확장 요소들은 SAML에서 정의되지 않은 네임스페이스로 한정되어야만 한다.

<RoleDescriptor>, <IDPSSODescriptor>, <SPSSODescriptor>, <AuthnAuthorityDescriptor>, <AttributeAuthorityDescriptor>, <PDPDescriptor> [One or More] 또는 <AffiliationDescriptor> [Required]

이 요소의 주요 내용은 하나 또는 그 이상의 역할 설명자 요소들의 연속이나 또는 제휴를 정의하는 특수한 설명자이다.

<Organization> [Optional]

요소에 의해 설명되는 SAML 엔티티에 대해 책임지고 있는 조직을 식별하는 선택적인 요소이다.

<ContactPerson> [Zero or More]

다양한 종류의 담당자(contact personnel)을 식별하는 요소들의 선택적인 연속이다.

<AdditionalMetadataLocation> [Zero or More]

SAML 엔티티에 대한 추가적인 메타데이터가 위치한 네임스페이스에 한정된 위치들의 선택적인 연속이다. 이것은 다른 포맷의 메타데이터나 또는 비-SAML 권고안에 대한 설명을 포함할 수 있다.

SAML에서 정의하지 않은 임의의 네임스페이스에 한정된 속성들이 또한 포함될 수 있다.

메타데이터 인스턴스의 루트 요소로 사용될 때, 이 요소는 validUntil 또는 cacheDuration 둘 중에 하나는 포함해야만 한다. 메타데이터 인스턴스의 루트 요소는 둘

중에 한 속성만 포함하는 것을 권고한다.

만약 동일한 타입의 다중 역할 설명자 요소들이 나타나면, 그들이 서로 걸치는 (overlapping) protocolSupportEnumeration 값들을 공유하지 않을 것이 권고된다. 하나의 protocolSupportEnumeration 값을 공유하는 동일한 타입의 다중 역할 설명자 요소들 사이에서 선택하는 것은 이 표준내에서 정의되지 않는다. 그러나 다른 구별하는 확장 요소들의 사용을 통해 메타데이터 프로파일들에 의해 정의될 수는 있다.

다음 스키마 조각은 <EntityDescriptor> 요소와 EntityDescriptorType 복합 타입을 정의한다.

```
<element name="EntityDescriptor" type="md:EntityDescriptorType"/>
<complexType name="EntityDescriptorType">
    <sequence>
        <element ref="ds:Signature" minOccurs="0"/>
        <element ref="md:Extensions" minOccurs="0"/>
        <choice>
            <choice maxOccurs="unbounded">
                <element ref="md:RoleDescriptor"/>
                <element ref="md:IDPSSODescriptor"/>
                <element ref="md:SPSSODescriptor"/>
                <element ref="md:AuthnAuthorityDescriptor"/>
                <element ref="md:AttributeAuthorityDescriptor"/>
                <element ref="md:PDPDescriptor"/>
            </choice>
            <element ref="md:AffiliationDescriptor"/>
        </choice>
        <element ref="md:Organization" minOccurs="0"/>
        <element ref="md:ContactPerson" minOccurs="0"
maxOccurs="unbounded"/>
        <element ref="md:AdditionalMetadataLocation" minOccurs="0"
                maxOccurs="unbounded"/>
    </sequence>
    <attribute name="entityID" type="md:entityIDType" use="required"/>
    <attribute name="validUntil" type="dateTime" use="optional"/>
```

```
    <attribute name="cacheDuration" type="duration" use="optional"/>
    <attribute name="ID" type="ID" use="optional"/>
    <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
```

2.3.2.1. <Organization> 요소

이 요소는 SAML 엔티티나 역할을 책임지는 조직에 대한 기본 정보를 기술한다. 이 요소의 사용은 항상 선택적이다. 이 요소의 내용은 본질적으로 정보전달적(informative)이고 어떠한 핵심 SAML 요소들 또는 속성들에 직접적으로 매핑되지 않는다. 이 요소의 OrganizationType 복합 타입은 다음 요소들로 구성된다.

<Extensions> [Optional]

이것은 메타데이터 게시자와 소비자 사이에 협약된 선택적인 메타데이터 확장을 포함한다. 확장 요소들은 전역 (네임스페이로 한정되지 않은) 요소들이나 또는 SAML에서 정의된 네임스페이스로 한정된 요소들을 포함해서는 안된다.

<OrganizationName> [One or More]

사람에게 적절하거나 또는 적절하지 않을 수 있는 하나 또는 그 이상의 언어에 한정된(language-qualified) 이름들이다.

<OrganizationDisplayName> [One or More]

사람에게 적절한 하나 또는 그 이상의 언어에 한정된 이름들이다.

<OrganizationURL> [One or More]

추가적인 정보를 위해 사용자가 방문할 수 있는 위치를 기술하는 하나 또는 그 이상의 언어에 한정된 URI들이다. 언어 한정자는 특정 위치에 있는 자료의 내용을 참조한다.

SAML에서 정의하지 않은 임의의 네임스페이스에 한정된 속성들이 또한 포함될 수 있다.

다음 스키마 조각은 <Organization> 요소와 OrganizationType 복합 타입을 정의한다.

```
<element name="Organization" type="md:OrganizationType"/>
<complexType name="OrganizationType">
    <sequence>
        <element ref="md:Extensions" minOccurs="0"/>
        <element ref="md:OrganizationName" maxOccurs="unbounded"/>
        <element ref="md:OrganizationDisplayName" maxOccurs="unbounded"/>
        <element ref="md:OrganizationURL" maxOccurs="unbounded"/>
    </sequence>
    <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
<element name="OrganizationName" type="md:localizedNameType"/>
<element name="OrganizationDisplayName" type="md:localizedNameType"/>
<element name="OrganizationURL" type="md:localizedURIType"/>
```

2.3.2.2. <ContactPerson> 요소

이 요소는 SAML 엔티티나 역할에 대해 어느 정도 책임을 지는 사람에 대한 기본적인 접근 정보를 기술한다. 이 요소의 사용은 항상 선택적이다. 이 요소의 내용은 본질적으로 정보전달적이고 어떠한 핵심 SAML 요소들 또는 속성들에 직접적으로 매핑되지 않는다. 이 요소의 ContactType 복합 타입은 다음 요소들로 구성된다.

contactType [Required]

ContactTypeType 열거(enumeration)를 사용하는 접근 타입을 기술한다. 가능한 값들은 기술적, 지원, 관리, 과금 그리고 다른 사항들이 될 수 있다.

<Extensions> [Optional]

이것은 메타데이터 게시자와 소비자 사이에 협약된 선택적인 메타데이터 확장을 포함한다. 확장 요소들은 SAML에서 정의되지 않은 네임스페이스로 한정되어야만 한다.

<Company> [Optional]

담당자의 회사 이름을 기술하는 선택적인 문자열 요소이다.

<GivenName> [Optional]

담당자의 이름을 기술하는 선택적인 문자열 이름이다.

<SurName> [Optional]

담당자의 성을 기술하는 선택적인 문자열 이름이다.

<EmailAddress> [Zero or More]

담당자의 e-mail 주소들을 나타내는 mailto: URI들을 포함하는 영 또는 그 이상의 요소들이다.

<TelephoneNumber> [Zero or More]

담당자의 전화번호를 기술하는 영 또는 그 이상의 문자열 요소들이다.

SAML에서 정의하지 않은 임의의 네임스페이스에 한정된 속성들이 또한 포함될 수 있다.

다음 스키마 조각은 <ContactPerson> 요소와 ContactType 복합 타입을 정의한다.

```
<element name="ContactPerson" type="md:ContactType"/>
<complexType name="ContactType">
    <sequence>
        <element ref="md:Extensions" minOccurs="0"/>
        <element ref="md:Company" minOccurs="0"/>
        <element ref="md:GivenName" minOccurs="0"/>
        <element ref="md:SurName" minOccurs="0"/>
        <element ref="md:EmailAddress" minOccurs="0"
maxOccurs="unbounded"/>
        <element ref="md:TelephoneNumber" minOccurs="0"
maxOccurs="unbounded"/>
    </sequence>
    <attribute name="contactType" type="md:ContactTypeType" use="required"/>
    <anyAttribute namespace="##other" processContents="lax"/>
```

```
</complexType>
<element name="Company" type="string"/>
<element name="GivenName" type="string"/>
<element name="SurName" type="string"/>
<element name="EmailAddress" type="anyURI"/>
<element name="TelephoneNumber" type="string"/>
<simpleType name="ContactTypeType">
    <restriction base="string">
        <enumeration value="technical"/>
        <enumeration value="support"/>
        <enumeration value="administrative"/>
        <enumeration value="billing"/>
        <enumeration value="other"/>
    </restriction>
</simpleType>
```

2.3.2.3. <AdditionalMetadataLocation> 요소

이 요소는 SAML 엔티티에 대해 추가적인 XML 기반 메타데이터가 어디에 있는지를 기술하는 네임스페이에 한정된 URI를 나타낸다. 이 요소에 대한 복합 타입인 AdditionalMetadataLocationType은 namespace 속성을 가지고 anyURI 타입을 확장한다. 이 필수 속성은 기술된 위치에서 찾게 되는 인스턴스 문서의 루트 요소의 XML 네임스페이를 포함한다.

다음 스키마 조각은 이 요소와 AdditionalMetadataLocationType 복합 타입을 정의한다.

```
<element name="AdditionalMetadataLocation"
        type="md:AdditionalMetadataLocationType"/>
<complexType name="AdditionalMetadataLocationType">
    <simpleContent>
        <extension base="anyURI">
            <attribute name="namespace" type="anyURI" use="required"/>
        </extension>
```

```
    </simpleContent>
</complexType>
```

2.4. 역할 설명자 요소

본 장의 요소들은 메타데이터에서 대부분의 연산적인(operational) 지원 컴포넌트들을 보완한다. 각각의 요소는 SAML 프로파일들을 지원하는 특정한 연산 행동의 집합을 정의한다.

2.4.1. <RoleDescriptor> 요소

이 요소는 서로 다른 역할들 사이에 처리상의 공통적인 특성을 제공할 목적으로 공통적인 설명 정보를 포함하는 추상적인 확장점이다. 새로운 역할들이 이 요소의 타입인 RoleDescriptorType 복합 타입을 확장함으로써 정의될 수 있다. RoleDescriptorType 복합 타입은 다음 요소와 속성을 포함한다.

ID [Optional]

일반적으로 전자서명을 할 때 참조 포인트로 사용되는 요소를 위한 문서 내에서 유일한 식별자이다.

validUntil [Optional]

이 요소에 포함된 메타데이터와 다른 요소들의 만료 시각을 가리키는 선택적인 요소이다.

cacheDuration [Optional]

이 요소에 포함된 메타데이터와 다른 요소들을 소비자가 캐시해야하는 최대 시각을 가리키는 선택적인 요소이다.

protocolSupportEnumeration [Required]

루트 요소에 의해 지원되는 프로토콜 스펙 집합을 식별하는 공백으로 분리된 (whitespace-delimited) URI 집합이다. SAML v2.0 엔티티들에 대해, 이 집합은 SAML 프로토콜 네임스페이스 URI인 “urn:oasis:names:tc:SAML:2.0:protocol”를 포함해야만 한다. 후속(subsequent) SAML 권고에서 동일한 네임스페이스 URI를 공유할 수 있지만, 필요하다면 구별하기 위해 다른 “protocol support” 식별자들을 제공할 수 있다.

errorURL [Optional]

사용자에게 이 역할과 관련된 문제 해결과 추가적인 지원을 제공하는 위치를 기술하는 선택적인 URI 속성이다.

<ds:Signature> [Optional]

포함하는 요소와 그것의 내용을 인증하는 XML 전자서명이다.

<Extensions> [Optional]

이것은 메타데이터 게시자와 소비자 사이에 협약된 선택적인 메타데이터 확장을 포함한다. 확장 요소들은 SAML에서 정의되지 않은 네임스페이스에 한정(namespace qualified)되어야만 한다.

<KeyDescriptor> [Zero or More]

엔티티가 이 역할로 동작할 때, 엔티티가 사용하는 암호 키들에 대한 정보를 제공하는 요소들의 선택적인 연속이다.

<Organization> [Optional]

이 역할과 관련된 조직을 기술하는 선택적인 요소. <EntityDecriptor> 요소 내에 사용된 요소와 동일하다.

<ContactPerson> [Zero or More]

이 역할과 관련된 담당자를 기술하는 요소들의 선택적인 연속이다.

<EntityDescriptor> 요소 내에 사용된 요소와 동일하다.

SAML에서 정의하지 않은 임의의 네임스페이스에 한정된 속성들이 또한 포함될 수 있다.

다음 스키마 조작은 <RoleDecirptor> 요소와 RoleDescriptorType 복합 타입을 정의한다.

```
<element name="RoleDescriptor" type="md:RoleDescriptorType"/>
<complexType name="RoleDescriptorType" abstract="true">
    <sequence>
        <element ref="ds:Signature" minOccurs="0"/>
        <element ref="md:Extensions" minOccurs="0"/>
        <element ref="md:KeyDescriptor" minOccurs="0"
maxOccurs="unbounded"/>
        <element ref="md:Organization" minOccurs="0"/>
        <element ref="md:ContactPerson" minOccurs="0"
maxOccurs="unbounded"/>
    </sequence>
    <attribute name="ID" type="ID" use="optional"/>
    <attribute name="validUntil" type="dateTime" use="optional"/>
    <attribute name="cacheDuration" type="duration" use="optional"/>
    <attribute name="protocolSupportEnumeration" type="md:anyURIListType"
            use="required"/>
    <attribute name="errorURL" type="anyURI" use="optional"/>
    <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
<simpleType name="anyURIListType">
    <list itemType="anyURI"/>
</simpleType>
```

2.4.1.1. Element <KeyDescriptor>

이 요소는 추가적이고 자세한 암호 정보와 함께, 엔티티가 데이터를 서명하거나 또는 암호화된 키를 수신하는데 사용하는 암호 키(들)에 대한 정보를 제공한다. KeyDescriptorType 복합 타입은 다음 요소와 속성으로 구성된다.

use [Optional]

설명되고 있는 키의 목적을 기술하는 선택적인 속성이다. 값들은 KeyTypes 열거로부터 유도되며 “encryption”과 “signing” 값들로 구성된다.

<ds:KeyInfo> [Required]

간접적으로 또는 직접적으로 키를 식별하는 선택적인 요소이다. 이 요소의 사용에 대한 추가적인 정보는 W3C XML 서명을 참조한다.

<EncryptionMethod> [Zero or More]

엔티티가 지원하는 알고리즘과 알고리즘에 특정한 설정들을 식별하는 선택적인 요소이다. 정확한 내용은 지원되는 알고리즘에 따라 달라진다. 이 요소의 xenc:EncryptionMethodType 복합 타입 정의는 W3C 암호화를 참조한다.

다음 스키마 조각은 <KeyDescriptor> 요소와 KeyDescriptorType 복합 타입을 정의한다.

```
<element name="KeyDescriptor" type="md:KeyDescriptorType"/>
<complexType name="KeyDescriptorType">
    <sequence>
        <element ref="ds:KeyInfo"/>
        <element ref="md:EncryptionMethod" minOccurs="0"
maxOccurs="unbounded"/>
    </sequence>
    <attribute name="use" type="md:KeyTypes" use="optional"/>
</complexType>
<simpleType name="KeyTypes">
    <restriction base="string">
```

```
            <enumeration value="encryption"/>
            <enumeration value="signing"/>
        </restriction>
    </simpleType>
    <element name="EncryptionMethod" type="xenc:EncryptionMethodType"/>
```

2.4.2. SSODescriptorType 복합 타입

이 추상 타입은 후속 절에서 설명되는 구체적인(concrete) 타입들인 SPSSODescriptorType과 IDPSSODescriptorType에 대한 공통 기반 타입이다. 이것은 SSO를 지원하는 아이덴터티 제공자와 서비스 제공자 둘 모두에 공통인 프로파일들을 반영하는 요소를 가지고 RoleDescriptorType를 확장한다. 이 타입은 다음 요소들을 포함한다.

<ArtifactResolutionService> [Zero or More]

ITU-T X.1141 8장에서 정의된 아티팩트 해결(artifact resolution) 프로파일을 지원하는 색인된 종점들을 설명하는 IndexedEndpointType 타입의 영 또는 그 이상의 요소들이다. ResponseLocation 속성은 반드시 생략되어야만 한다.

<SingleLogoutService> [Zero or More]

ITU-T X.1141 8장에서 정의된 단일 로그아웃 프로파일들을 지원하는 종점들을 설명하는 EndpointType 타입의 영 또는 그 이상의 요소들이다.

<ManageNameIDService> [Zero or More]

ITU-T X.1141 8장에서 정의된 이름 식별자 관리 프로파일들을 지원하는 종점들을 설명하는 EndpointType 타입의 영 또는 그 이상의 요소들이다.

<NameIDFormat> [Zero or More]

이 역할로 동작하는 시스템 엔티티가 지원하는 이름 식별자 포맷들을 열거하는

anyURI 타입의 영 또는 그 이상의 요소들이다.

다음 스키마 조각은 SSODescriptorType 복합 타입을 정의한다.

```
<complexType name="SSODescriptorType" abstract="true">
   <complexContent>
      <extension base="md:RoleDescriptorType">
         <sequence>
            <element ref="md:ArtifactResolutionService" minOccurs="0"
                     maxOccurs="unbounded"/>
            <element ref="md:SingleLogoutService" minOccurs="0"
                     maxOccurs="unbounded"/>
            <element ref="md:ManageNameIDService" minOccurs="0"
                     maxOccurs="unbounded"/>
            <element ref="md:NameIDFormat" minOccurs="0"
                      maxOccurs="unbounded"/>
         </sequence>
      </extension>
   </complexContent>
</complexType>
<element name="ArtifactResolutionService" type="md:IndexedEndpointType"/>
<element name="SingleLogoutService" type="md:EndpointType"/>
<element name="ManageNameIDService" type="md:EndpointType"/>
<element name="NameIDFormat" type="anyURI"/>
```

2.4.3. <IDPSSODescriptor> 요소

이 요소는 SSO를 지원하는 아이덴터티 제공자에 특정한 프로파일들을 반영하는 내용을 가지고 SSODescriptorType을 확장한다. IDPSSODescriptorType 복합 타입은 다음 요소와 속성을 포함한다.

WantAuthnRequestsSigned [Optional]

아이덴터티 제공자가 수신한 <samlp:AuthnRequest> 메시지들이 서명될 것을 요구하는 것을 지시하는 선택적인 속성이다. 만약 이 속성이 생략되면, 값은 “false”로 가정된다.

<SingleSignOnService> [One or More]

ITU-T X.1141 8장에서 정의된 인증 요청 프로토콜의 프로파일을 지원하는 종점들을 설명하는 **EndpointType** 타입의 하나 또는 그 이상의 요소들이다. 모든 아이덴터티 제공자들은 정의에 따라, 이와 같은 종점을 적어도 하나는 지원한다. ResponseLocation 속성은 생략되어야만 한다.

<NameIDMappingService> [Zero or More]

ITU-T X.1141 8장에서 정의된 이름 식별자 매핑 프로파일을 지원하는 종점들을 설명하는 **EndpointType** 타입의 하나 또는 그 이상의 요소들이다. ResponseLocation 속성은 생략되어야만 한다.

<AssertionIDRequestService> [Zero or More]

ITU-T X.1141 10장에서 정의된 주장 요청 프로토콜 프로파일이나 또는 주장 요청에 대한 특별한 URI 바인딩을 지원하는 종점들을 설명하는 **EndpointType** 타입의 하나 또는 그 이상의 요소들이다.

주의(사실적): PE33(OASIS PE:2006 참조)은 주장 요청 프로토콜을 주장 질의/요청으로 대체할 것을 제안한다.

<AttributeProfile> [Zero or More]

이 아이덴터티 제공자가 지원하는 속성 프로파일들을 열거하는 **anyURI** 타입의 영 또는 그 이상의 요소들이다.

<saml:Attribute> [Zero or More]

이 아이덴터티 제공자가 지원하는 SAML 속성들을 식별하는 영 또는 그 이상의 요소들이다. 특정 값이 선택적으로 포함될 수 있으며, 이것은 단지 속성의 정의에서 허용되는 값들만 지원된다는 것을 가리킨다. 이 문맥에서 어떤 속성을 지원한다는 것은 아이덴터티 제공자가 SSO 동안 주장들을 배달할 때, 그 속성을 주장에 포함할 수 있는 능력을 가지고 있다는 것을 의미한다.

주의(사실적): PE7(OASIS PE:2006 참조)은 위 문단의 끝에 다음과 같은 문장을 추가할 것을 제안한다.

WantAuthnRequestsSigned 속성은 그들이 서명되지 않은 <AuthnRequest> 메시지가 아이덴터티 제공자에게 받아들여질 것을 기대하는 지 또는 그렇지 않은지를 서비스 제공자들에게 지시할 의도를 가진다. 비록 비서명된 요청이 거절될 것이라는 사실이 합리적으로 예상될 지라도, 아이덴터티 제공자가 의무적으로 비서명된 요청을 거절해야 하는 것은 아니며, 또한 서비스 제공자도 그것의 내용을 의무적으로 서명해야 하는 것은 아니다. 어떤 경우에는, 서비스 제공자가 어떠한 아이덴터티 제공자가 최종적으로 그것의 요청을 수신 받아 응답할 지를 알 수조차 없을 수 있다. 따라서, 이와 같은 경우에 이 속성의 사용은 엄격하게 정의될 수 없다. 더욱이, 예상되는 특정 서명 방식은 바인딩에 의존적이라는 사실을 주의해라. ITU-T X.1141 10.5절의 HTTP Redirect 바인딩은 서명이 XML 메시지에 위치되기 보다는 URI-인코드된 값으로 적용될 것을 요구한다. 반면에 다른 바인딩들은 일반적으로 서명이 유용한 방식으로 메시지 내에 위치하는 것을 허용한다.

다음 스키마 조각은 <IDPSSODescriptor> 요소와 IDPSSODescriptorType 복합 타입을 정의한다.

```
<element name="IDPSSODescriptor" type="md:IDPSSODescriptorType"/>
<complexType name="IDPSSODescriptorType">
    <complexContent>
        <extension base="md:SSODescriptorType">
            <sequence>
                <element                                ref="md:SingleSignOnService"
maxOccurs="unbounded"/>
                <element ref="md:NameIDMappingService" minOccurs="0"
                        maxOccurs="unbounded"/>
                <element ref="md:AssertionIDRequestService" minOccurs="0"
                         maxOccurs="unbounded"/>
```

```
                <element ref="md:AttributeProfile" minOccurs="0"
                        maxOccurs="unbounded"/>
                <element ref="saml:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
            </sequence>
            <attribute name="WantAuthnRequestsSigned" type="boolean"
                    use="optional"/>
        </extension>
    </complexContent>
</complexType>
<element name="SingleSignOnService" type="md:EndpointType"/>
<element name="NameIDMappingService" type="md:EndpointType"/>
<element name="AssertionIDRequestService" type="md:EndpointType"/>
<element name="AttributeProfile" type="anyURI"/>
```

2.4.4. <SPSSODescriptor> 요소

이 요소는 서비스 제공자에 특정한 프로파일들을 반영하는 내용을 가지고 SSODescriptorType을 확장한다.

SPSSODescriptorType 복합 타입은 다음의 추가적인 요소와 속성을 포함한다.

AuthnRequestsSigned [Optional]

이 서비스 제공자가 송신한 <samlp:AuthnRequest> 메시지들이 서명될 것인지 여부를 지시하는 선택적인 속성이다. 만약 생략되면, 이 값은 “false”로 가정된다.

주의(사실적): PE7(OASIS PE:2006 참조)은 위 문단의 끝에 다음과 같은 문장을 추가할 것을 제안한다.

"false" 값 (또는 이 속성의 생략)이 서비스 제공자가 결코 자신의 요청을 서명하지 않을 것이나 또는 서명된 요청이 에러로 고려되어야 한다는 것을 암시하지는 않는다. 그렇지만, 이 속성의 값을 “true”로 설정한 메타데이터

의 소유자인 서비스 제공자로부터 서명되지 않은 <samlp:AutnRequest> 메시지를 받은 아이덴터티 제공자는 SAML 에러 응답을 반환해야만 하며, 이 요청을 이행해서는 안된다.

WantAssertionsSigned [Optional]

서비스 제공자가 수신한 <saml:Assertion> 요소들이 서명되어야 한다는 요구를 가리키는 선택적인 속성이다. 만약 생략되면, 이 값은 “false”로 가정된다. 이 요구사항은 특정 프로파일/바인딩 조합의 사용으로부터 유도된 서명에 대한 요구사항 외에 추가적인 것이다.

주의(사실적): PE7(OASIS PE:2006 참조)은 위 문단의 끝에 다음과 같은 문장을 추가할 것을 제안한다.

SAML 바인딩 또는 프로파일 계층(layer)에서 포함하는 전자서명(enclosing signature)가 이 요구사항을 충족시키지는 못한다는 것을 주의한다. 예를 들어 주장들을 포함하는 <samlp:Response>를 서명하는 것이나 또는 TLS 연결이 이와 같은 경우에 해당된다.

<AssertionConsumerService> [One or More]

인증 요청 프로토콜의 프로파일을 지원하는 색인된 종점들을 설명하는 하나 또는 그 이상의 요소들이다. 모든 서비스 제공자들은 정의에 따라, 이와 같은 종점을 적어도 하나는 지원한다.

<AttributeConsumingService> [Zero or More]

서비스 제공자에서 제공하는, SAML 속성들의 사용을 요구하거나 원하는 응용 또는 서비스를 설명하는 영 또는 그 이상의 요소들이다.

많아야 하나의<AttributeConsumingService> 요소만이 isDefault 속성을 “true”로 설정할 수 있다. isDefault 속성이 “true”로 설정된 요소가 하나도 없는 경우도 허용된다.

다음 스키마 조각은 <SPSSODescriptor> 요소와 SPSSODescriptorType 복합 타입을

정의한다.

```
<element name="SPSSODescriptor" type="md:SPSSODescriptorType"/>
<complexType name="SPSSODescriptorType">
    <complexContent>
        <extension base="md:SSODescriptorType">
            <sequence>
                <element ref="md:AssertionConsumerService"
                        maxOccurs="unbounded"/>
                <element ref="md:AttributeConsumingService" minOccurs="0"
                        maxOccurs="unbounded"/>
            </sequence>
            <attribute name="AuthnRequestsSigned" type="boolean"
use="optional"/>
            <attribute name="WantAssertionsSigned" type="boolean"
use="optional"/>
        </extension>
    </complexContent>
</complexType>
<element name="AssertionConsumerService" type="md:IndexedEndpointType"/>
```

2.4.4.1. Element <AttributeConsumingService>

이 요소는 서비스가 요구하거나 원하는 속성에 의해 서비스 제공자가 제공하는 특정서비스를 정의한다. AttributeConsumingServiceType 복합 타입은 다음 요소와 속성을 포함한다.

index [Required]

프로토콜 메시지에 의해 참조될 수 있도록, 요소에 유일한 정수 값을 할당하는 필수적인 속성이다.

isDefault [Optional]

서비스 제공자가 지원하는 기본 서비스를 식별한다. 특정 서비스가 응용에 의해 별도

로 지시되지 않은 경우에 유용하다. 만약 생략되면, 값은 “false”로 가정된다.

<ServiceName> [One or More]

서비스에 대한 하나 또는 그 이상의 언어에 한정된 이름들이다.

<ServiceDescription> [Zero or More]

서비스를 설명하는 영 또는 그 이상의 언어에 한정된 문자열들이다.

<RequestedAttribute> [One or More]

이 서비스가 요구하거나 원하는 속성들을 기술하는 하나 또는 그 이상의 요소들이다.

다음 스키마 조각은 <AttributeRequestingService> 요소와 AttributeRequestingServiceType 복합 타입을 정의한다.

```
<element name="AttributeConsumingService"
type="md:AttributeConsumingServiceType"/>
<complexType name="AttributeConsumingServiceType">
    <sequence>
        <element ref="md:ServiceName" maxOccurs="unbounded"/>
        <element ref="md:ServiceDescription" minOccurs="0"
maxOccurs="unbounded"/>
        <element ref="md:RequestedAttribute" maxOccurs="unbounded"/>
    </sequence>
    <attribute name="index" type="unsignedShort" use="required"/>
    <attribute name="isDefault" type="boolean" use="optional"/>
</complexType>
<element name="ServiceName" type="md:localizedNameType"/>
<element name="ServiceDescription" type="md:localizedNameType"/>
```

2.4.4.2. Element <RequestedAttribute>

이 요소는 선택적으로 특정 값들을 포함하며, 특정 SAML 속성에 대한 서비스 제공자의 관심을 기술한다. RequestedAttributeType 복합 타입은 다음 속성을 가지고

saml:AttributeType을 확장한다.

isRequired [Optional]

(유용하거나 또는 원하는 속성을 단순히 찾는 것과는 달리) 기능을 제대로 동작시키기 위해, 서비스가 대응되는 SAML 속성을 요구하는지 여부를 가리키는 선택적인 XML 속성이다.

만약 특정 <saml:AttributeValue> 요소들이 포함되면, 단지 매칭되는 값들만 서비스와 연관된다.

다음 스키마 조각은 <RequestedAttribute> 요소와 RequestedAttributeType 복합 타입을 정의한다.

```
<element name="RequestedAttribute" type="md:RequestedAttributeType"/>
<complexType name="RequestedAttributeType">
    <complexContent>
        <extension base="saml:AttributeType">
            <attribute name="isRequired" type="boolean" use="optional"/>
        </extension>
    </complexContent>
</complexType>
```

2.4.5. Element <AuthnAuthorityDescriptor>

이 요소는 <samlp:AuthnQuery> 메시지에 응답하는 SAML 기관인 인증 기관에 특정한 프로파일을 반영하는 내용을 가지고 RoleDescriptorType을 확장한다. AuthnAuthorityDescriptorType 복합 타입은 다음의 추가적인 요소를 포함한다.

<AuthnQueryService> [One or More]

ITU-T X.1141 8장에서 정의된 인증 질의 프로토콜의 프로파일을 지원하는 종점들을 설명하는 EndpointType 타입의 하나 또는 그 이상의 요소들이다. 모든 인증 기관들은 정의에 따라, 이와 같은 종점을 적어도 하나는 지원한다.

<AssertionIDRequestService> [Zero or More]

ITU-T X.1141 8장에서 정의된 주장 요청 프로토콜의 프로파일이나 또는 10장에 정의된 주장 요청에 대한 특별한 URI들을 지원하는 종점들을 설명하는 EndpointType 타입의 하나 또는 그 이상의 요소들이다.

<NameIDFormat> [Zero or More]

이 기관에서 지원하는 이름 식별자 포맷들을 열거하는 anyURI 타입의 영 또는 그 이상의 요소들이다. (이 요소에 대해 가능한 값들은 ITU-T X.1141 8.7절을 참조한다.)

다음 스키마 조각은 <AuthnAuthorityDescriptor> 요소와 AuthnAuthorityDescriptorType 복합 타입을 정의한다.

```
<element name="AuthnAuthorityDescriptor"
type="md:AuthnAuthorityDescriptorType"/>
<complexType name="AuthnAuthorityDescriptorType">
    <complexContent>
        <extension base="md:RoleDescriptorType">
            <sequence>
                <element ref="md:AuthnQueryService" maxOccurs="unbounded"/>
                <element ref="md:AssertionIDRequestService" minOccurs="0"
                        maxOccurs="unbounded"/>
                <element ref="md:NameIDFormat" minOccurs="0"
                        maxOccurs="unbounded"/>
            </sequence>
        </extension>
    </complexContent>
</complexType>
<element name="AuthnQueryService" type="md:EndpointType"/>
```

2.4.6. <PDPDescriptor> 요소

이 요소는 <samlp:AuthzDecisionQuery> 메시지에 응답하는 SAML 기관인 정책결정점들에 특정한 프로파일을 반영하는 내용을 가지고 RoleDescriptorType 확장한다.

PDPDescriptorType 복합 타입은 다음의 추가적인 요소를 포함한다.

<AuthzService> [One or More]

ITU-T X.1141 8장에서 정의된 인가 정책 질의 프로토콜의 프로파일을 지원하는 종점들을 설명하는 EndpointType 타입의 하나 또는 그 이상의 요소들이다. 모든 정책결정점은 정의에 따라, 이와 같은 종점을 적어도 하나는 지원한다.

<AssertionIDRequestService> [Zero or More]

ITU-T X.1141 8장에서 정의된 주장 요청 프로토콜의 프로파일이나 또는 10장에 정의된 주장 요청에 대한 특별한 URI들을 지원하는 종점들을 설명하는 EndpointType 타입의 영 또는 그 이상의 요소들이다.

주의(사실적): PE33(OASIS PE:2006 참조)은 주장 요청 프로토콜을 주장 질의/요청으로 대체할 것을 제안한다.

<NameIDFormat> [Zero or More]

이 기관에서 지원하는 이름 식별자 포맷들을 열거하는 anyURI 타입의 영 또는 그 이상의 요소들이다. (이 요소에 대해 가능한 값들은 ITU-T X.1141 8.7절을 참조한다.)

다음 스키마 조각은 <PDPDescriptor> 요소와 PDPDescriptorType 복합 타입을 정의한다.

```
<element name="PDPDescriptor" type="md:PDPDescriptorType"/>
<complexType name="PDPDescriptorType">
    <complexContent>
        <extension base="md:RoleDescriptorType">
            <sequence>
```

```
                <element ref="md:AuthzService" maxOccurs="unbounded"/>
                <element ref="md:AssertionIDRequestService" minOccurs="0"
                        maxOccurs="unbounded"/>
                <element ref="md:NameIDFormat" minOccurs="0"
                        maxOccurs="unbounded"/>
            </sequence>
        </extension>
    </complexContent>
</complexType>
<element name="AuthzService" type="md:EndpointType"/>
```

2.4.7. Element <AttributeAuthorityDescriptor>

이 요소는 <samlp:AttributeQuery> 메시지에 응답하는 SAML 기관인 속성 기관에 특정한 프로파일을 반영하는 내용을 가지고 RoleDescriptorType 확장한다.

AttributeAuthorityDescriptorType 복합 타입은 다음의 추가적인 요소를 포함한다.

<AttributeService> [One or More]

ITU-T X.1141 8장에서 정의된 속성 질의 프로토콜의 프로파일을 지원하는 종점들을 설명하는 EndpointType 타입의 하나 또는 그 이상의 요소들이다. 모든 속성 기관들은 정의에 따라, 이와 같은 종점을 적어도 하나는 지원한다.

<AssertionIDRequestService> [Zero or More]

ITU-T X.1141 8장에서 정의된 주장 요청 프로토콜의 프로파일이나 또는 10장에 정의된 주장 요청에 대한 특별한 URI들을 지원하는 종점들을 설명하는 EndpointType 타입의 영 또는 그 이상의 요소들이다.

주의(사실적): PE33(OASIS PE:2006 참조)은 주장 요청 프로토콜을 주장 질의/요청으로 대체할 것을 제안한다.

<NameIDFormat> [Zero or More]

이 기관에서 지원하는 이름 식별자 포맷들을 열거하는 anyURI 타입의 영 또는 그 이상의 요소들이다. (이 요소에 대해 가능한 값들은 ITU-T X.1141 8.7절을 참조한다.)

<AttributeProfile> [Zero or More]

이 기관에서 지원하는 속성 프로파일들을 열거하는 anyURI 타입의 영 또는 그 이상의 요소들이다. (이 요소에 대해 가능한 값들은 ITU-T X.1141 8.7절을 참조한다.)

<saml:Attribute> [Zero or More]

이 기관이 지원하는 SAML 속성들을 식별하는 영 또는 그 이상의 요소들이다. 특정 값이 선택적으로 포함될 수 있으며, 이것은 단지 속성의 정의에서 허용되는 값들만 지원된다는 것을 가리킨다.

다음 스키마 조각은 <AttributeAuthorityDescriptor> 요소와 AttributeAuthorityDescriptorType 복합 타입을 정의한다.

```
<element name="AttributeAuthorityDescriptor"
        type="md:AttributeAuthorityDescriptorType"/>
<complexType name="AttributeAuthorityDescriptorType">
   <complexContent>
        <extension base="md:RoleDescriptorType">
            <sequence>
                <element ref="md:AttributeService" maxOccurs="unbounded"/>
                <element ref="md:AssertionIDRequestService" minOccurs="0"
                        maxOccurs="unbounded"/>
                <element ref="md:NameIDFormat" minOccurs="0"
                        maxOccurs="unbounded"/>
                <element ref="md:AttributeProfile" minOccurs="0"
                        maxOccurs="unbounded"/>
                <element ref="saml:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
            </sequence>
```

```
        </extension>
    </complexContent>
</complexType>
<element name="AttributeService" type="md:EndpointType"/>
```

2.5. <AffiliationDescriptor> 요소

이 요소는 <EntityDescriptor>가 단일 엔티티가 아닌 SAML 엔티티들의 제휴(일반적으로 서비스 제공자들)를 설명할 때, 사용되는 역할 설명자들의 연속에 대한 대안이다. 이 요소는 제휴 그 자체에 대한 일반적인 정보와 함께 제휴를 구성하는 개별적인 엔티티들에 대한 요약 정보를 제공한다. AffiliationDescriptorType 복합 타입은 다음 요소와 속성을 포함한다.

affiliationOwnerID [Required]

제휴를 책임지는 엔티티의 유일한 식별자를 기술한다. 소유자는 제휴의 멤버인 것으로 가정되지 않는다. 만약 소유자가 멤버라면, 그것의 식별자는 <AffiliateMember> 요소에 또한 나타나야만 한다.

ID [Optional]

일반적으로 전자서명을 할 때 참조 포인트로 사용되는 요소를 위한 문서 내에서 유일한 식별자이다.

validUntil [Optional]

이 요소에 포함된 메타데이터와 다른 요소들의 만료 시각을 가리키는 선택적인 요소이다.

cacheDuration [Optional]

이 요소에 포함된 메타데이터와 다른 요소들을 소비자가 캐시해야하는 최대 시각을 가리키는 선택적인 요소이다.

<ds:Signature> [Optional]

ITU-T X.1141 8장에서 설명된 것과 같이, 포함하는 요소와 그것의 내용을 인증하는 XML 전자서명이다.

<Extensions> [Optional]

이것은 메타데이터 게시자와 소비자 사이에 협약된 선택적인 메타데이터 확장을 포함한다. 확장 요소들은 SAML에서 정의되지 않은 네임스페이스에 한정되어야만 한다.

<AffiliateMember> [One or More]

각각의 멤버의 유일한 식별자를 기술함으로써, 제휴 멤버들을 열거하는 하나 또는 그 이상의 요소들이다(ITU-T X.1141 8.7절을 참조한다.)

<KeyDescriptor> [Zero or More]

제휴가 총괄적으로 사용하는 암호 키들에 대한 정보를 제공하는 요소들의 선택적인 연속이다. 이것은 제휴를 구성하는 엔티티들 각각의 메타데이터에 게시되어 사용되는 키와는 다르다.

SAML에서 정의하지 않은 임의의 네임스페이스에 한정된 속성들이 또한 포함될 수 있다.

다음 스키마 조각은 <AffiliationDescriptor> 요소와 AffiliationDescriptorType 복합 타입을 정의한다.

```
<element name="AffiliationDescriptor" type="md:AffiliationDescriptorType"/>
<complexType name="AffiliationDescriptorType">
    <sequence>
        <element ref="ds:Signature" minOccurs="0"/>
        <element ref="md:Extensions" minOccurs="0"/>
        <element ref="md:AffiliateMember" maxOccurs="unbounded"/>
        <element ref="md:KeyDescriptor" minOccurs="0"
maxOccurs="unbounded"/>
    </sequence>
    <attribute name="affiliationOwnerID" type="md:entityIDType" use="required"/>
```

```
    <attribute name="validUntil" type="dateTime" use="optional"/>
    <attribute name="cacheDuration" type="duration" use="optional"/>
    <attribute name="ID" type="ID" use="optional"/>
    <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
<element name="AffiliateMember" type="md:entityIDType"/>
```

2.6. 예들

다음은 아이덴터티 제공자와 속성 기관으로 동작하는 SAML 시스템 엔티티에 대한 메타데이터 예이다. 서명은 실제 내용 없이 위치만 표시되어 있다.

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    entityID="https://IdentityProvider.com/SAML">
    <ds:Signature>...</ds:Signature>
     <IDPSSODescriptor WantAuthnRequestsSigned="true"
         protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
          <KeyDescriptor use="signing">
               <ds:KeyInfo>
                    <ds:KeyName>IdentityProvider.com SSO Key</ds:KeyName>
               </ds:KeyInfo>
          </KeyDescriptor>
          <ArtifactResolutionService isDefault="true" index="0"
              Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
              Location="https://IdentityProvider.com/SAML/Artifact"/>
          <SingleLogoutService
              Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
              Location="https://IdentityProvider.com/SAML/SLO/SOAP"/>
          <SingleLogoutService
              Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
              Location="https://IdentityProvider.com/SAML/SLO/Browser"
```

```
ResponseLocation="https://IdentityProvider.com/SAML/SLO/Response"/>
        <NameIDFormat>
            urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
        </NameIDFormat>
        <NameIDFormat>
            urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
        </NameIDFormat>
        <NameIDFormat>
            urn:oasis:names:tc:SAML:2.0:nameid-format:transient
        </NameIDFormat>
        <SingleSignOnService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
            Location="https://IdentityProvider.com/SAML/SSO/Browser"/>
        <SingleSignOnService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://IdentityProvider.com/SAML/SSO/Browser"/>
        <saml:Attribute
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
            FriendlyName="eduPersonPrincipalName">
        </saml:Attribute>
        <saml:Attribute
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
            FriendlyName="eduPersonAffiliation">
              <saml:AttributeValue>member</saml:AttributeValue>
              <saml:AttributeValue>student</saml:AttributeValue>
              <saml:AttributeValue>faculty</saml:AttributeValue>
              <saml:AttributeValue>employee</saml:AttributeValue>
              <saml:AttributeValue>staff</saml:AttributeValue>
        </saml:Attribute>
    </IDPSSODescriptor>
    <AttributeAuthorityDescriptor
```

```
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
 <KeyDescriptor use="signing">
      <ds:KeyInfo>
           <ds:KeyName>IdentityProvider.com AA Key</ds:KeyName>
      </ds:KeyInfo>
 </KeyDescriptor>
 <AttributeService
     Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
     Location="https://IdentityProvider.com/SAML/AA/SOAP"/>
 <AssertionIDRequestService
     Binding="urn:oasis:names:tc:SAML:2.0:bindings:URI"
     Location="https://IdentityProvider.com/SAML/AA/URI"/>
 <NameIDFormat>
     urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
 </NameIDFormat>
 <NameIDFormat>
     urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
 </NameIDFormat>
 <NameIDFormat>
     urn:oasis:names:tc:SAML:2.0:nameid-format:transient
 </NameIDFormat>
 <saml:Attribute
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
     Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
     FriendlyName="eduPersonPrincipalName">
 </saml:Attribute>
 <saml:Attribute
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
     Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
     FriendlyName="eduPersonAffiliation">
      <saml:AttributeValue>member</saml:AttributeValue>
      <saml:AttributeValue>student</saml:AttributeValue>
      <saml:AttributeValue>faculty</saml:AttributeValue>
      <saml:AttributeValue>employee</saml:AttributeValue>
```

```
            <saml:AttributeValue>staff</saml:AttributeValue>
        </saml:Attribute>
    </AttributeAuthorityDescriptor>
    <Organization>
        <OrganizationName xml:lang="en">Identity Providers R
US</OrganizationName>
        <OrganizationDisplayName xml:lang="en">
            Identity Providers R US, a Division of Lerxst Corp.
        </OrganizationDisplayName>
        <OrganizationURL
xml:lang="en">https://IdentityProvider.com</OrganizationURL>
    </Organization>
</EntityDescriptor>
```

다음은 서비스 제공자로 동작하는 SAML 시스템 엔티티에 대한 메타데이터 예이다. 서명은 실제 내용 없이 위치만 표시되어 있다. 설명을 위해, 서비스는 사용자가 그들을 유일하게 식별할 것을 요구하지 않고 역할과 유사한(role-like) 속성을 기반으로 인가 접근을 요구한다.

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    entityID="https://ServiceProvider.com/SAML">
    <ds:Signature>...</ds:Signature>
     <SPSSODescriptor AuthnRequestsSigned="true"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
         <KeyDescriptor use="signing">
             <ds:KeyInfo>
                 <ds:KeyName>ServiceProvider.com SSO Key</ds:KeyName>
             </ds:KeyInfo>
         </KeyDescriptor>
         <KeyDescriptor use="encryption">
             <ds:KeyInfo>
```

```
                <ds:KeyName>ServiceProvider.com Encrypt Key</ds:KeyName>
            </ds:KeyInfo>
            <EncryptionMethod
                Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
        </KeyDescriptor>
        <SingleLogoutService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://ServiceProvider.com/SAML/SLO/SOAP"/>
        <SingleLogoutService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
            Location="https://ServiceProvider.com/SAML/SLO/Browser"

    ResponseLocation="https://ServiceProvider.com/SAML/SLO/Response"/>
        <NameIDFormat>
            urn:oasis:names:tc:SAML:2.0:nameid-format:transient
        </NameIDFormat>
        <AssertionConsumerService isDefault="true" index="0"
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
            Location="https://ServiceProvider.com/SAML/SSO/Artifact"/>
        <AssertionConsumerService index="1"
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://ServiceProvider.com/SAML/SSO/POST"/>
        <AttributeConsumingService index="0">
            <ServiceName xml:lang="en">Academic Journals R
US</ServiceName>
            <RequestedAttribute
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
                FriendlyName="eduPersonEntitlement">
                 <saml:AttributeValue>
                    https://ServiceProvider.com/entitlements/123456789
                 </saml:AttributeValue>
            </RequestedAttribute>
        </AttributeConsumingService>
```

```
    </SPSSODescriptor>
    <Organization>
        <OrganizationName xml:lang="en">Academic Journals R
US</OrganizationName>
        <OrganizationDisplayName xml:lang="en">
            Academic Journals R US, a Division of Dirk Corp.
        </OrganizationDisplayName>
        <OrganizationURL
xml:lang="en">https://ServiceProvider.com</OrganizationURL>
    </Organization>
</EntityDescriptor>
```

3. 서명 처리(Signature processing)

메타데이터 인스턴스에 포함되어 있는 다양한 요소들은 <ds:Signature> 요소를 포함함으로써 전자적으로 서명될 수 있다. 이를 통해 다음과 같은 이득을 얻을 수 있다.

■ 메타데이터 무결성

신뢰되는 서명자에 의한 메타데이터의 인증

예를 들어, 의지하는 측이 보안 채널을 통해 중개자 없이 직접적으로 메타데이터 발행 엔티티로부터 직접적인 정보를 얻어, 전자서명이 아닌 다른 방법으로 발행자가 의지하는 측에 인증이 된다면, 전자서명이 항상 요구되는 것은 아니다.

많은 다른 기법들이 두 기관 사이에서 직접적인 인증과 보안 채널 설정을 위해 사용이 가능하다. 이 기법들은 TLS, HMAC, 패스워드-기반 메커니즘을 포함한다. 게다가, 적용 가능한 보안 요구사항들은 통신하는 응용에 의지한다.

또한, 요소들은 자체적으로 서명된 요소를 포함하는 부모 요소들에 대한 서명을 상속할 수 있다.

이와 같은 상황이 아니라면, 적어도 메타데이터 인스턴스의 루트 요소가 서명되는 것이 권고된다.

■ XML 서명 프로파일

W3C XML 서명 규격은 Signature은 융통성과 많은 선택을 가지고 데이터를 서명하는 것에 대한 일반적인 XML 문법을 기술한다. 본 절은 이들 기능들에 대해 세부적으로 제약을 가한다. 이것은 메타데이터 처리기가 일반적인 XML 서명 처리를 완벽하게 할 필요가 없게 한다. 이 용법은 전자서명이 적용되는 요소들에 선택적으로 존재하는 xs:ID-타입형의 속성들을 이용한다. 이들 속성들은 집합적으로 본 절에서 식별자 속성으로 불린다.

(1) 서명 포맷과 알고리즘

XML 서명은 포함하는(enveloping), 포함된(enveloped), 분리된(detached) 세가지 방식으로 서명되는 문서와 서명을 연관시킨다.

SAML 메타데이터는 이 표준안에서 정의된 요소들을 서명할 때, 반드시 포함된 서명을 사용해야만 한다. SAML 처리기는 “http://www.w3.org/2000/09/xmldsig#rsa-sha1”로 식별되는 알고리즘과 부합하는 공개키 연산을 위해 RSA 서명과 검증의 사용을 지원해야 한다.

(2) References

서명된 메타데이터 요소들은 서명된 요소에 대한 식별자 속성에 값을 제공해야만 한다. 이 요소는 서명된 메타데이터 요소를 포함하는 실제 XML 문서의 루트 요소일 수도 또는 아닐 수도 있다.

서명은 서명되는 메타데이터 요소의 식별자 속성 값에 대한 하나의 URI 참조를 포함하는 단일한 <ds:Reference>를 포함해야만 한다. 예를 들어, 만약 식별자 속성 값이 “foo”이면, <ds:Reference> 요소의 URI 속성은 “#foo”이어야만 한다.

따라서, 메타데이터 요소의 속성은 서명된 요소와 그것이 포함하는 모든 자식 요소들의 내용에 적용되어야만 한다.

(3) 정규화 방식(Canonicalization method)

SAML 구현은 <ds:SignedInfo>의 <ds:CanonicalizationMethod> 요소와 <ds:Transform> 알고리즘 모두에서 주석이 있건 없건 간에 배타적인 정규화(exclusive canonicalization)를 사용해야 한다. 배타적인 정규화는 XML 문맥에 포함된 SAML 메타데이터에 대해 생성된 서명들이 XML 문맥에 독립적으로 검증되는 것을 보장해 준다.

(4) 변환(Transforms)

SAML 메타데이터 내에 있는 서명들은 식별자 “http://www.w3.org/2000/09/xmldsig#enveloped-signature”를 가진 포함된 서명 변환이나 또는 식별자 “http://www.w3.org/2001/10/xml-exc-c14n#”나 “http://www.w3.org/2001/10/xml-exc-c14n#WithComments”를 가지는 배타적인 정규화 변환이 아닌 다른 변환을 포함해서는 안된다.

서명의 검증자는 다른 변환 알고리즘을 포함하는 서명을 유효하지 않은 것으로 판단할 수 있다. 만약 검증자가 유효하지 않은 것으로 판단하지 않는다면, 검증자는 서명된 메타데이터의 어떠한 내용도 서명으로부터 배제되지 않는다는 것을 확인해야만 한다. 이것은 어떠한 변환이 수용가능한 지에 대한 대역외(out-of-band) 협의가 이루어지거나, 또는 내용에 대해 수작업으로 변환을 적용하여 그 결과가 동일한 SAML 메타데이터를 구성하는 것으로 재검증함으로써 수행될 수 있다.

(5) 키정보(KeyInfo)

W3C XML 서명은 <ds:KeyInfo> 요소의 사용법을 정의한다. SAML은 <ds:KeyInfo>의 사용을 요구하지 않으며, 그것의 사용에 대한 어떠한 제약도 가하지 않는다. 따라서 <ds:KeyInfo>는 나타나지 않을 수 있다.

4. 메타데이터 게시 및 해결

이 표준안에서는 엔티티가 메타데이터 문서를 게시(publish)하고 소비자가 메타데이터 문서의 위치를 찾기(resolve) 위해 두 가지 메커니즘을 제공한다. 한 가지 방식은 entityID 또는 providerID로 다양하게 참조되는 URI인 엔티티의 유일한 식별자를 직접적으로 역참조(dereferencing)하는 잘 알려진 위치(well-known-location)을 통한 것이다. 다른 방식은 DNS에 메타데이터의 위치를 게시함으로써 간접적으로 메타데이터를 얻어오는 방식이다. 다른 대역외 메커니즘 또한 허용된다. 두 가지 방식을 지원하는 소비자는 잘 알려진 위치 메커니즘을 사용하기 전에 DNS를 통해 해결을 시도해야만 한다.

메타데이터 검색(retrieval)이 문서의 네트워크 전송(transport)을 요구할 때, 전송은 서버 인증과 무결성 보호를 제공하는 메커니즘에 의해 보호되어야 한다. 예를 들어, HTTP-기반 해결(resolution)은 IETF RFC 3546에 의해 개정된 IETF RFC 2246에 정의된 것과 같이 TLS를 통해 보호되어야 한다.

본 장에서는 XML 서명, TLS 서버 인증과 DNS 서명을 포함하여 메타데이터의 정확도와 적법성에 대한 신뢰를 확인하는 것을 돕기 위한 다양한 메커니즘들이 설명된다. 사용되는 메커니즘에 관계없이, 의지하는 측에서는 메타데이터 정보를 의지하기 전에 이것에 대한 신뢰를 설정하는 어떠한 수단을 가지고 있어야 한다.

4.1. 잘 알려진 위치를 통한 게시와 해결

다음 절은 잘 알려진 위치 방식을 통해 메타데이터를 게시하고 해결하는 것을 설명한다.

4.1.1. 게시

엔티티들은 그것의 유일한 식별자를 통해 표시되는 위치에 문서를 위치시킴으로써, 잘 알려진 위치에 그들의 메타데이터 문서들을 게시할 수 있다. 이 때, 엔티티 유일 식별자

는 URN이 아닌 URL 형태를 가져야만 한다. HTTPS URL이 이러한 목적으로 사용되는 것이 강력하게 권고된다. 만약 메타데이터가 그 위치에 직접적으로 위치되지 않는다면 HTTP 1.1 302 리다이렉트와 같은 URL 방식(scheme)에서 지원되는 우회(indirection) 메커니즘이 사용될 수 있다. 만약, 게시 프로토콜이 MIME-기반 내용 타입의 식별을 허용한다면, 메타데이터 인스턴스의 내용 타입은 반드시 “application/samlmetadata+xml”이어야만 한다.

잘 알려진 위치에 제공되는 XML 문서는 유일한 식별자로 대표되는 엔티티에 대한 메타데이터만 설명해야만 한다. 즉, 루트 요소는 위치와 매칭이 되는 entityid를 가진 <EntityDescriptor>이어야만 한다. 만약 다른 엔티티들이 설명될 필요가 있다면, <AdditionalMetadataLocation> 요소가 사용되어야만 한다. 따라서, <EntitiesDescriptor> 요소는 이 메커니즘을 사용하여 게시되는 요소들에서는 사용되어서는 안된다. 왜냐하면, 엔티티들 그룹은 이와 같은 엔티티로 정의되지 않기 때문이다.

4.1.2. 해결

만약 엔티티의 유일한 식별자가 URL이면, 메타데이터 소비자들은 식별자를 역참조함으로써, 방식(scheme)에 특정한 방식을 이용하여, 직접적으로 엔티티의 유일한 식별자를 해결하는 것을 시도할 수 있다.

4.2. DNS 를 통한 게시와 해결

메타데이터 문서들의 접근성을 높이고 엔티티의 유일한 식별자와 메타데이터의 위치 사이에 추가적인 우회를 제공하기 위해, 엔티티들은 IETF RFC 1034에 정의된 것 같이 그들의 대응되는 DNS 영역(zone)에 그들의 메타데이터 문서 위치를 게시할 수 있다. 엔티티의 유일한 식별자인 URI가 이 처리의 입력으로 사용된다. URI는 유연한(flexible) 식별자이기 때문에, 위치 게시 방법들과 해결 처리는 URI의 방식과 전체 도메인(fully-qualified) 이름으로 결정된다. 이에 따라, 메타데이터에 대한 URI 위치는 IETF RFC 2914와 RFC 3403에 정의된 것과 같이 NAPTR RR(Resource Record)의 질의를 통해 유도될

수 있다.

의지하는 측이 게시된 위치의 유효성, 영역의 기관, DNS 응답의 무결성을 확인할 수 있도록, 엔티티는 IETF RFC 2535를 사용하는 서명된 영역 파일들에 resource record를 게시하는 것이 권고된다. 만약 DNS 영역 서명이 존재하면, 의지하는 측은 적절히 서명을 검증해야만 한다.

4.2.1. 게시

이 표준은 IETF RFC 2915와 IETF RFC 3403에서 설명된 NAPTR resource record를 사용한다.

동적 위임 발견 시스템(Dynamic Delegation Discovery System, DDDS)은 종료 조건에 도달할 때까지 응용에 한정된 입력 문자열과 그 문자열을 변환하는 잘 알려진 규칙들의 응용에 기반한 정보 검색을 위한 일반적인 목적을 가지는 시스템이다. 이것은 응용에 특정하게 정의된 데이터베이스에 대한 조사(look-up)나 또는 응용에 의해 정의된 규칙들에 기반한 URL 해결을 요구한다. DDDS는 DDDS 규칙을 적용하는데 필요한 DNS 내의 정보 저장을 위해 특정 타입의 DNS Resource Record인 NAPTR record를 정의한다.

다중 메타데이터 문서가 배포될 필요가 있거나, 별도의 키 내용을 요구하는 다중 신뢰 관리 때문에 다른 메타데이터 문서들이 요구될 때, 또는 서비스 인터페이스가 별도의 메타데이터 선언들을 요구할 때, 엔티티들은 분리된 URL들을 게시할 수 있다. 선택적인 <AdditionalMetadataLocation> 요소의 사용을 통하거나 regexp 기능과 NAPTR resource record 자체에 있는 다중 서비스 정의 필드들을 통해 이것이 달성될 수 있다.

만약, 게시 프로토콜이 MIME-기반 내용 타입의 식별을 허용한다면, 메타데이터 인스턴스의 내용 타입은 반드시 “application/samlmetadata+xml”이어야만 한다.

만약 엔티티의 유일한 식별자가 URN이면, 대응되는 메타데이터 위치의 게시는 IETF RFC 3404에서 기술된 것과 같이 처리된다. 그렇지 않다면, 메타데이터 위치의 해결은 아래에 기술된 것과 같이 처리된다.

다음은 SAML 메타데이터를 위한 응용에 특정한 DDDS 프로파일이다.

(1) 첫 번째 잘 알려진 규칙(First well known rule)

SAML 메타데이터 해결을 처리하는데 첫 번째 잘 알려진 규칙은 엔티티의 유일한 식별자를 분석(parsing)하여 전체 도메인 이름을 추출하는 것이다.

(2) 순서 필드(The order field)

순서 필드는 반환되는 각각의 NAPTR resource record를 처리하는 순서를 가리킨다. 게시자는 이 필드가 가리키는 순서에 따라 해결 응용에서 처리되어야만 하는 다중 NAPTR resource record들을 제공할 수 있다.

(3) 선호 필드(The preference field)

종료 NAPTR resource record에 대해, 게시자는 해결하는 응용에게 선호하는 사용 순서를 표현한다. 해결하는 응용은 예를 들어 resource record가 응용이 지원하지 않는 프로토콜을 반환하는 경우와 같이 서비스 필드가 해결자의 요구사항을 만족시키지 못 하는 경우, 이 순서를 무시할 수 있다.

(4) 플래그 필드(The flag field)

SAML 메타데이터 해결은 두 번씩 “U” 플래그를 사용한다. 이 플래그는 종료자(terminal)이고 “null” 값이다. 이것은 추가적인 resource record들이 처리되어야 한다는 것을 암시한다. “U” 플래그는 이 규칙의 출력이 URI라는 것을 가리킨다.

(5) 서비스 필드(The service field)

다음 BNF에서 설명되는 것과 같이 SAML에 한정된 서비스 필드는 인스턴스 문서들이 이용 가능하도록 하는 모드들을 선언한다.

```
servicefield = 1("PID2U" / "NID2U") "+" proto [*(":" class) *(":" servicetype)]
proto = 1("https" / "uddi")
class = 1[ "entity" / "entitygroup" )
servicetype = 1(si / "spsso" / "idpsso" / "authn" / "authnauth" / "pdp" / "attrauth"
                / alphanum )
si = "si" [":" alphanum] [":endpoint"]
alphanum = 1*32(ALPHA / DIGIT)
```

이곳에서:

- servicefield PID2U는 엔티티의 유일한 식별자를 메타데이터 URL로 변환한다.
- servicefield NID2U는 사용자의 <NameID>를 메타데이터 URL로 변환한다.
- Proto는 검색 프로토콜 (https 또는 uddi)을 설명한다. UDDI의 경우, URL은 WSDL 문서를 참조하는 http(s) URL이 될 것이다.
- class는 참조되는 메타데이터 문서가 단일 엔티티 또는 다중 엔티티들 설명하는지 여부를 식별한다. 후자의 경우, 참조되는 문서는 <AffiliationDescriptor> 또는 <EntitiesDescriptor>와 같이 문서 자체 내에 원래의 유일한 식별자에 의해 정의된 엔티티를 엔티티 그룹의 멤버로써 포함해야만 한다.
- servicetype은 엔티티가 서로 다른 역할과 서비스를 위해 메타데이터를 분리된 문서들로 게시할 수 있도록 해 준다. 다중 servicetype 선언들을 만나는 해결자는 어떤 서비스가 연산에 필요한지에 따라 적절한 URI를 역참조할 것이다. 예를 들어 아이덴터티 제공자와 서비스 제공자 둘 모두로 동작하는 엔티티는 각각의 역할에 대한 메타데이터를 서로 다른 위치에 게시할 수 있다. authn 서비스 타입은 <SingleSignOnService> 종점을 나타낸다.

- 선택적인 종점 컴포넌트를 가지는 si는 게시자가 서비스 인스턴스에 대한 메타데이터를 직접적으로 게시하거나 종점을 사용하는 SOAP 종점을 자세히 표현하는 것을 허용한다.

예:

- PID2U+https:entity – https 프로토콜을 통해 이용 가능한 엔티티의 완전한 메타데이터 문서를 나타낸다.
- PID2U+uddi:entity:si:foo – 서비스 인스턴스 “foo”를 설명하는 WSDL 문서 위치를 나타낸다.
- PID2U+https:entitygroup:idpsso – SSO 아이덴터티 제공자로 동작하는 엔티티 그룹에 대한 메타데이터를 나타낸다. 원래의 엔티티는 이 그룹의 멤버이다.
- NID2U+https:idp – 사용자의 SSO 아이덴터티 제공자에 대한 메타데이터를 나타낸다.

(6) The regex and replacement 필드들

regex를 통해 입력 문자열을 처리한 후, 예상되는 출력은 반드시 유효한 https URL이거나 또는 UDDI 노드(WSDL 문서) 주소이어야만 한다.

(7) NAPTR 예들

이 절에서는 NAPTR(IETF RFC 2915 참조)를 지원하는 엔티티들에 의해 사용될 수 있는 URL과 e-mail의 일부 예를 나열한다.

A. 엔티티 메타데이터 NAPTR 예들

엔티티들은 다음과 같은 방식으로 메타데이터 URI들을 게시한다.

```
$ORIGIN provider.biz

;; order pref f service regexp or replacement

IN NAPTR 100 10 "U" PID2U+https:entity
    "!^.*$!https://host.provider.biz/some/directory/trust.xml!" ""
IN NAPTR 110 10 "U" PID2U+https: entity:trust
    "!^.*!https://foo.provider.biz:1443/mdtrust.xml!" ""
IN NAPTR 125 10 "U" PID2U+https:"
IN NAPTR 110 10 "U" PID2U+uddi:entity
    "!^.*$!https://this.uddi.node.provider.biz/libmd.wsdl" ""
```

B. 이름 식별자 예들

사용자의 고용주 “example.int”는 사무 비품을 제공하는 회사가 인가된 구입자들을 인증하는데 사용할 수 있는 아이덴터티 제공자를 운영한다. 제공자는 사용자의 전자우면 주소인 “buyer@example.int”을 해결 처리의 입력으로 선택하여 전자우편 주소를 분석하여 전체도메인 이름 (Fully-Qualified Domain Name, FQDN) “example.int”을 추출한다. 고용주는 “example.int” DNS에 다음 NAPTR record를 게시한다.

```
$ORIGIN example.int

IN NAPTR 100 10 "U" NID2U+https:authn
    "!^([^@]+)@(.*)$!https://serv.example.int:8000/cgi-bin/getmd?₩1!" ""
IN NAPTR 100 10 "U" NID2U+https:idp
    "!^([^@]+)@(.*)$!https://auth.example.int/app/auth?₩1" ""
```

4.2.2. 해결

DNS를 통해 엔티티에 대한 메타데이터를 해결할 때, 엔티티의 유일한 식별자가 해결 처리의 초기 입력으로 사용된다. 처리 진행은 다음과 같다.

- 만약 유일한 식별자가 URN이면, IETF RFC 3403에서 정의된 것과 같은 해결 단계대로 진행된다.
- 그렇지 않다면, 전체 도메인 이름을 얻기 위해 식별자를 분석한다.
- 종료 resource record가 반환될 때까지, 도메인의 NAPTR resource record에 대해 DNS에 반복적으로 질의를 한다.
- service 필드, 그 다음 order 필드, 그 다음 결과 집합의 preference 필드에 기반하여 어떠한 resource record가 사용될 지를 식별한다.
- 제공되는 위치에서 응용에서 요구되는 문서(들)을 얻는다.

메타데이터 정보의 위치를 해결하는 것을 시작하기 위해, 어떤 경우에는 하나의 URI로 표현된 엔티티의 유일한 식별자를 하나 또는 그 이상의 단위 요소들로 분해(decompose)하는 것이 필요할 것이다.

다음 정규(regular) 표현식은 분해 처리를 시작할 때 사용되어야 한다.

```
^([^:/?#]+:)?/*([^:/?#]*@)?(([^/?:#]*₩.)*([^/?#:₩.]+)₩.([^/?#:₩.]+)))(:₩d+)
?([^?#]*)(₩?[^#]*)?(#.*)?$
     1            2           34           56            7            8
9       10        11
```

하부수식(Subexpression) 3은 전체 도메인 이름을 결과로 출력해야만 한다. 이 전체 도메인 이름은 이 영역으로부터 메타데이터 위치들을 검색하는 기초가 될 것이다.

식별자의 분석이 완료되면, 그 다음 응용은 NAPTR resource records에 대하여 결과 도메인에 DNS 질의를 수행한다(하부수식 5). 이것은 하나 또는 그 이상의 응답을 예상해야 한다. 응용은 결과 집합으로부터 현재의 요청 연산에 관련이 없는 어떠한 서비스 정

의들도 배제할 수 있다.

해결하는 응용들은 이후 order 필드에 따라 결과 집합을 정돈해야만 한다. 그리고 preference 집합을 기준으로 결과 집합을 정돈시킬 수 있다. 해결자가 preferences 필드의 순서를 따를 필요는 없다. 처리 결과인 NAPTR resource record들은 종료 NAPTR resource record에 이를 때까지 order 플래그를 기반으로 반복적으로 정돈된다.

최종 결과는 적합한 형식의(well-formed) 절대 URL일 것이며, 이것은 다시 메타데이터 문서를 검색하는데 사용된다.

4.2.3. 메타데이터 위치 캐싱

위치 캐싱은 위치가 추출되는 DNS 영역의 유지 시간(TTL, time-to-limit)을 초과해서는 안된다. 해결자는 해당 영역의 TTL이 만료되면, 메타데이터 위치에 대한 새로운 복사본을 얻어와야만 한다.

메타데이터 문서 게시자는 메타데이터 문서의 위치를 변화시킬 때, 영역의 TTL을 주의 깊게 고려해야 한다. 이와 같은 위치 변화가 발생한다면, 게시자는 모든 준용하는(conforming) 해결자가 확실히 갱신된 위치를 가질 때까지 예전 위치와 새로운 위치 양쪽에 메타데이터 문서를 보유해야만 한다. 만약 그렇지 않다면, 예전 위치에 대해 새로운 위치를 기술하는 HTTP 리다이렉트 응답을 제공해야만 한다.

4.3. 메타데이터의 후처리

본 절은 메타데이터 후처리를 설명한다.

4.3.1. 메타데이터 인스턴스 캐싱

문서 캐싱은 subject 요소의 validUntil 또는 cacheDuration 속성의 값을 초과해서는 안된다. 만약 메타데이터 요소가 캐싱 정책을 포함하는 부모 요소들을 가지고 있다면, 부모 요소들이 우선권을 갖는다.

cacheDuration 속성을 적절하게 처리하기 위해, 소비자들은 문서가 검색된 날짜와 시각을 보유해야만 한다.

문서나 또는 요소가 만료되면, 소비자는 새로운 복사본을 검색해야만 하고, 이것은 문서 위치의 갱신(refresh)을 요청할 수 있다. 소비자는 IETF RFC 2616의 13장에서 설명된 것과 같은 방식으로 문서의 캐싱 처리를 수행해야 하며, HTTP 서버로부터 Last-Modified 날짜와 시각을 요청할 수 있다. 게시자는 IETF RFC 2616, 10.3.5절(304 Not Modified)에서 설명된 것과 같이 허용가능한 캐싱 처리를 보장해야 한다.

4.3.2. HTTPS 리다이렉트 처리

게시자들은 IETF RFC 2626에서 정의된 것처럼 HTTP Redirect (301 Moved Permanently, 302 or 307 Temporary Redirect)를 응답할 수 있다. 그리면 사용자 에이전트는 리다이렉트 응답에 기술된 URL을 따라가야만 한다. 리다이렉트는 초기 요청과 같은 프로토콜이어야 한다.

4.3.3. XML 서명과 일반적인 신뢰 처리

메타데이터 처리는 메타데이터 자체와 메타데이터가 설명하는 엔티티에 속한 신뢰 모두에 대한 신뢰 협상을 위해 여러 가지 메커니즘을 제공한다.

- 메타데이터 위치 URL이 해결된 DNS 영역의 서명으로부터 얻어진 신뢰 방식. 이것은 메타데이터 문서 위치의 정확성을 보장한다.
- 메타데이터 문서 자체의 서명 처리로부터 얻어진 신뢰 방식. 이것은 XML 문서의 무결성을 보장한다.
- 메타데이터 위치 URL의 TLS 서버 인증으로부터 얻어진 신뢰 방식. 이것은 메타데이터 게시자의 신원(identity)를 보장한다.

메타데이터 문서의 후처리는 XML 문서 수준에서 전자서명 처리를 반드시 포함해야만 하고 다른 두 가지 처리 중에 하나를 포함할 수 있다. 명확하게, 의지하는 측은 해결과

분석 처리에서 인용된 기관들 중에 어떠한 것을 신뢰할 것인지를 선택할 수 있다. 메타데이터의 게시자는 문서-무결성을 채택해야만 하며, 구현 정책에 따라 결정되는 메타데이터 문서내의 신뢰를 설정하기 위해 다른 두 가지 처리 프로파일 중에 하나를 채택할 수 있다. 다음과 같은 사항들이 고려되어야만 한다.

(1) 서명된 DNS 영역 처리

DNS 영역 서명의 검증은 만약 존재하면, IETF RFC 2535에서 설명된 것처럼 처리되어야 한다.

(2) 서명된 문서와 조각 처리

게시된 메타데이터 문서들은 문서의 주체에 대해 발급된 인증서나 또는 다른 신뢰 기관을 통해 이 표준에서 설명된 방식으로 서명되어야 한다. 게시자는 신뢰의 운반 수단으로써 다른 기관들의 서명을 고려할 수 있다.

메타데이터 소비자는 서명이 존재하면, 이 표준에서 설명된 방식으로 메타데이터에 대한 서명을 검증해야만 한다.

(3) TLS를 통한 메타데이터 검색 동안 서버 인증 처리

게시자가 TLS URL을 구현할 것을 강력하게 권고한다. 따라서, 소비자는 TLS 인증서의 발급자로부터 상속된 신뢰를 고려해야 한다. 게시 URL이 항상 메타데이터 문서 주체의 도메인에 위치되는 것이 아닐 수 있다. 따라서, 소비자는 엔티티가 또 다른 신뢰 기관에 의해 운영(host)될 수 있기 때문에 인증서의 주체가 해당 엔티티일 것이라고 가정해서는 안된다.

이 신뢰의 기초가 캐시된 문서에 대해서는 이용가능하지 않을 수 있기 때문에, 이와 같은 상황 아래서는 다른 메커니즘이 사용되어야 한다.

부 속 서 A

SAML 메타데이터 스키마

다음은 SAML 메타데이터 스키마이다.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema
    targetNamespace="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <import namespace="http://www.w3.org/2000/09/xmldsig#"
        schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd"/>
    <import namespace="http://www.w3.org/2001/04/xmlenc#"
        schemaLocation="http://www.w3.org/TR/2002/REC-xmlenc-core-
20021210/xenc-schema.xsd"/>
    <import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
        schemaLocation="saml-schema-assertion-2.0.xsd"/>
    <import namespace="http://www.w3.org/XML/1998/namespace"
        schemaLocation="http://www.w3.org/2001/xml.xsd"/>
    <annotation>
        <documentation>
            Document identifier: saml-schema-metadata-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
              V2.0 (March, 2005):
                Schema for SAML metadata, first published in SAML 2.0.
        </documentation>
    </annotation>

    <simpleType name="entityIDType">
        <restriction base="anyURI">
            <maxLength value="1024"/>
        </restriction>
    </simpleType>
    <complexType name="localizedNameType">
        <simpleContent>
            <extension base="string">
                <attribute ref="xml:lang" use="required"/>
            </extension>
        </simpleContent>
    </complexType>
    <complexType name="localizedURIType">
        <simpleContent>
            <extension base="anyURI">
                <attribute ref="xml:lang" use="required"/>
```

```
        </extension>
    </simpleContent>
</complexType>

<element name="Extensions" type="md:ExtensionsType"/>
<complexType final="#all" name="ExtensionsType">
    <sequence>
        <any namespace="##other" processContents="lax"
                maxOccurs="unbounded"/>
    </sequence>
</complexType>

<complexType name="EndpointType">
    <sequence>
        <any namespace="##other" processContents="lax" minOccurs="0"
                maxOccurs="unbounded"/>
    </sequence>
    <attribute name="Binding" type="anyURI" use="required"/>
    <attribute name="Location" type="anyURI" use="required"/>
    <attribute name="ResponseLocation" type="anyURI" use="optional"/>
    <anyAttribute namespace="##other" processContents="lax"/>
</complexType>

<complexType name="IndexedEndpointType">
    <complexContent>
        <extension base="md:EndpointType">
            <attribute name="index" type="unsignedShort" use="required"/>
            <attribute name="isDefault" type="boolean" use="optional"/>
        </extension>
    </complexContent>
</complexType>

<element name="EntitiesDescriptor" type="md:EntitiesDescriptorType"/>
<complexType name="EntitiesDescriptorType">
    <sequence>
        <element ref="ds:Signature" minOccurs="0"/>
        <element ref="md:Extensions" minOccurs="0"/>
        <choice minOccurs="1" maxOccurs="unbounded">
            <element ref="md:EntityDescriptor"/>
            <element ref="md:EntitiesDescriptor"/>
        </choice>
    </sequence>
    <attribute name="validUntil" type="dateTime" use="optional"/>
    <attribute name="cacheDuration" type="duration" use="optional"/>
    <attribute name="ID" type="ID" use="optional"/>
    <attribute name="Name" type="string" use="optional"/>
</complexType>

<element name="EntityDescriptor" type="md:EntityDescriptorType"/>
<complexType name="EntityDescriptorType">
    <sequence>
        <element ref="ds:Signature" minOccurs="0"/>
        <element ref="md:Extensions" minOccurs="0"/>
        <choice>
            <choice maxOccurs="unbounded">
                <element ref="md:RoleDescriptor"/>
```

```
                    <element ref="md:IDPSSODescriptor"/>
                    <element ref="md:SPSSODescriptor"/>
                    <element ref="md:AuthnAuthorityDescriptor"/>
                    <element ref="md:AttributeAuthorityDescriptor"/>
                    <element ref="md:PDPDescriptor"/>
                </choice>
                <element ref="md:AffiliationDescriptor"/>
            </choice>
            <element ref="md:Organization" minOccurs="0"/>
            <element ref="md:ContactPerson" minOccurs="0" maxOccurs="unbounded"/>
            <element ref="md:AdditionalMetadataLocation" minOccurs="0"
                     maxOccurs="unbounded"/>
        </sequence>
        <attribute name="entityID" type="md:entityIDType" use="required"/>
        <attribute name="validUntil" type="dateTime" use="optional"/>
        <attribute name="cacheDuration" type="duration" use="optional"/>
        <attribute name="ID" type="ID" use="optional"/>
        <anyAttribute namespace="##other" processContents="lax"/>
    </complexType>

    <element name="Organization" type="md:OrganizationType"/>
    <complexType name="OrganizationType">
        <sequence>
            <element ref="md:Extensions" minOccurs="0"/>
            <element ref="md:OrganizationName" maxOccurs="unbounded"/>
            <element ref="md:OrganizationDisplayName" maxOccurs="unbounded"/>
            <element ref="md:OrganizationURL" maxOccurs="unbounded"/>
        </sequence>
        <anyAttribute namespace="##other" processContents="lax"/>
    </complexType>
    <element name="OrganizationName" type="md:localizedNameType"/>
    <element name="OrganizationDisplayName" type="md:localizedNameType"/>
    <element name="OrganizationURL" type="md:localizedURIType"/>
    <element name="ContactPerson" type="md:ContactType"/>
    <complexType name="ContactType">
        <sequence>
            <element ref="md:Extensions" minOccurs="0"/>
            <element ref="md:Company" minOccurs="0"/>
            <element ref="md:GivenName" minOccurs="0"/>
            <element ref="md:SurName" minOccurs="0"/>
            <element ref="md:EmailAddress" minOccurs="0" maxOccurs="unbounded"/>
            <element ref="md:TelephoneNumber" minOccurs="0"
                     maxOccurs="unbounded"/>
        </sequence>
        <attribute name="contactType" type="md:ContactTypeType" use="required"/>
        <anyAttribute namespace="##other" processContents="lax"/>
    </complexType>
    <element name="Company" type="string"/>
    <element name="GivenName" type="string"/>
    <element name="SurName" type="string"/>
    <element name="EmailAddress" type="anyURI"/>
    <element name="TelephoneNumber" type="string"/>
    <simpleType name="ContactTypeType">
        <restriction base="string">
            <enumeration value="technical"/>
            <enumeration value="support"/>
```

```
            <enumeration value="administrative"/>
            <enumeration value="billing"/>
            <enumeration value="other"/>
        </restriction>
    </simpleType>

    <element name="AdditionalMetadataLocation"
            type="md:AdditionalMetadataLocationType"/>
    <complexType name="AdditionalMetadataLocationType">
        <simpleContent>
            <extension base="anyURI">
                <attribute name="namespace" type="anyURI" use="required"/>
            </extension>
        </simpleContent>
    </complexType>

    <element name="RoleDescriptor" type="md:RoleDescriptorType"/>
    <complexType name="RoleDescriptorType" abstract="true">
        <sequence>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="md:Extensions" minOccurs="0"/>
            <element ref="md:KeyDescriptor" minOccurs="0" maxOccurs="unbounded"/>
            <element ref="md:Organization" minOccurs="0"/>
            <element ref="md:ContactPerson" minOccurs="0" maxOccurs="unbounded"/>
        </sequence>
        <attribute name="ID" type="ID" use="optional"/>
        <attribute name="validUntil" type="dateTime" use="optional"/>
        <attribute name="cacheDuration" type="duration" use="optional"/>
        <attribute name="protocolSupportEnumeration" type="md:anyURIListType"
                use="required"/>
        <attribute name="errorURL" type="anyURI" use="optional"/>
        <anyAttribute namespace="##other" processContents="lax"/>
    </complexType>
    <simpleType name="anyURIListType">
        <list itemType="anyURI"/>
    </simpleType>

    <element name="KeyDescriptor" type="md:KeyDescriptorType"/>
    <complexType name="KeyDescriptorType">
        <sequence>
            <element ref="ds:KeyInfo"/>
            <element ref="md:EncryptionMethod" minOccurs="0"
                    maxOccurs="unbounded"/>
        </sequence>
        <attribute name="use" type="md:KeyTypes" use="optional"/>
    </complexType>
    <simpleType name="KeyTypes">
        <restriction base="string">
            <enumeration value="encryption"/>
            <enumeration value="signing"/>
        </restriction>
    </simpleType>
    <element name="EncryptionMethod" type="xenc:EncryptionMethodType"/>

    <complexType name="SSODescriptorType" abstract="true">
        <complexContent>
```

```
            <extension base="md:RoleDescriptorType">
                <sequence>
                    <element ref="md:ArtifactResolutionService" minOccurs="0"
                                maxOccurs="unbounded"/>
                    <element ref="md:SingleLogoutService" minOccurs="0"
                                maxOccurs="unbounded"/>
                    <element ref="md:ManageNameIDService" minOccurs="0"
                                maxOccurs="unbounded"/>
                    <element ref="md:NameIDFormat" minOccurs="0"
                                maxOccurs="unbounded"/>
                </sequence>
            </extension>
        </complexContent>
    </complexType>
    <element name="ArtifactResolutionService" type="md:IndexedEndpointType"/>
    <element name="SingleLogoutService" type="md:EndpointType"/>
    <element name="ManageNameIDService" type="md:EndpointType"/>
    <element name="NameIDFormat" type="anyURI"/>

    <element name="IDPSSODescriptor" type="md:IDPSSODescriptorType"/>
    <complexType name="IDPSSODescriptorType">
        <complexContent>
            <extension base="md:SSODescriptorType">
                <sequence>
                    <element ref="md:SingleSignOnService" maxOccurs="unbounded"/>
                    <element ref="md:NameIDMappingService" minOccurs="0"
                                maxOccurs="unbounded"/>
                    <element ref="md:AssertionIDRequestService" minOccurs="0"
                                maxOccurs="unbounded"/>
                    <element ref="md:AttributeProfile" minOccurs="0"
                                maxOccurs="unbounded"/>
                    <element ref="saml:Attribute" minOccurs="0"
                                maxOccurs="unbounded"/>
                </sequence>
                <attribute name="WantAuthnRequestsSigned" type="boolean"
                                use="optional"/>
            </extension>
        </complexContent>
    </complexType>
    <element name="SingleSignOnService" type="md:EndpointType"/>
    <element name="NameIDMappingService" type="md:EndpointType"/>
    <element name="AssertionIDRequestService" type="md:EndpointType"/>
    <element name="AttributeProfile" type="anyURI"/>

    <element name="SPSSODescriptor" type="md:SPSSODescriptorType"/>
    <complexType name="SPSSODescriptorType">
        <complexContent>
            <extension base="md:SSODescriptorType">
                <sequence>
                    <element ref="md:AssertionConsumerService"
                                maxOccurs="unbounded"/>
                    <element ref="md:AttributeConsumingService" minOccurs="0"
                                maxOccurs="unbounded"/>
                </sequence>
                <attribute name="AuthnRequestsSigned" type="boolean" use="optional"/>
                <attribute name="WantAssertionsSigned" type="boolean" use="optional"/>
```

```
            </extension>
        </complexContent>
    </complexType>
    <element name="AssertionConsumerService" type="md:IndexedEndpointType"/>
    <element name="AttributeConsumingService"
             type="md:AttributeConsumingServiceType"/>
    <complexType name="AttributeConsumingServiceType">
        <sequence>
            <element ref="md:ServiceName" maxOccurs="unbounded"/>
            <element ref="md:ServiceDescription" minOccurs="0"
                     maxOccurs="unbounded"/>
            <element ref="md:RequestedAttribute" maxOccurs="unbounded"/>
        </sequence>
        <attribute name="index" type="unsignedShort" use="required"/>
        <attribute name="isDefault" type="boolean" use="optional"/>
    </complexType>
    <element name="ServiceName" type="md:localizedNameType"/>
    <element name="ServiceDescription" type="md:localizedNameType"/>
    <element name="RequestedAttribute" type="md:RequestedAttributeType"/>
    <complexType name="RequestedAttributeType">
        <complexContent>
            <extension base="saml:AttributeType">
                <attribute name="isRequired" type="boolean" use="optional"/>
            </extension>
        </complexContent>
    </complexType>

    <element name="AuthnAuthorityDescriptor" type="md:AuthnAuthorityDescriptorType"/>
    <complexType name="AuthnAuthorityDescriptorType">
        <complexContent>
            <extension base="md:RoleDescriptorType">
                <sequence>
                    <element ref="md:AuthnQueryService" maxOccurs="unbounded"/>
                    <element ref="md:AssertionIDRequestService" minOccurs="0"
                             maxOccurs="unbounded"/>
                    <element ref="md:NameIDFormat" minOccurs="0"
                             maxOccurs="unbounded"/>
                </sequence>
            </extension>
        </complexContent>
    </complexType>
    <element name="AuthnQueryService" type="md:EndpointType"/>

    <element name="PDPDescriptor" type="md:PDPDescriptorType"/>
    <complexType name="PDPDescriptorType">
        <complexContent>
            <extension base="md:RoleDescriptorType">
                <sequence>
                    <element ref="md:AuthzService" maxOccurs="unbounded"/>
                    <element ref="md:AssertionIDRequestService" minOccurs="0"
                             maxOccurs="unbounded"/>
                    <element ref="md:NameIDFormat" minOccurs="0"
                             maxOccurs="unbounded"/>
                </sequence>
            </extension>
        </complexContent>
```

```
    </complexType>
    <element name="AuthzService" type="md:EndpointType"/>

    <element                                                name="AttributeAuthorityDescriptor"
type="md:AttributeAuthorityDescriptorType"/>
    <complexType name="AttributeAuthorityDescriptorType">
        <complexContent>
            <extension base="md:RoleDescriptorType">
                <sequence>
                    <element ref="md:AttributeService" maxOccurs="unbounded"/>
                    <element ref="md:AssertionIDRequestService" minOccurs="0"
                             maxOccurs="unbounded"/>
                    <element ref="md:NameIDFormat" minOccurs="0"
                             maxOccurs="unbounded"/>
                    <element ref="md:AttributeProfile" minOccurs="0"
                             maxOccurs="unbounded"/>
                    <element ref="saml:Attribute" minOccurs="0"
                             maxOccurs="unbounded"/>
                </sequence>
            </extension>
        </complexContent>
    </complexType>
    <element name="AttributeService" type="md:EndpointType"/>

    <element name="AffiliationDescriptor" type="md:AffiliationDescriptorType"/>
    <complexType name="AffiliationDescriptorType">
        <sequence>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="md:Extensions" minOccurs="0"/>
            <element ref="md:AffiliateMember" maxOccurs="unbounded"/>
            <element ref="md:KeyDescriptor" minOccurs="0" maxOccurs="unbounded"/>
        </sequence>
        <attribute name="affiliationOwnerID" type="md:entityIDType" use="required"/>
        <attribute name="validUntil" type="dateTime" use="optional"/>
        <attribute name="cacheDuration" type="duration" use="optional"/>
        <attribute name="ID" type="ID" use="optional"/>
        <anyAttribute namespace="##other" processContents="lax"/>
    </complexType>
    <element name="AffiliateMember" type="md:entityIDType"/>
</schema>
```

표준 작성 공헌자

표준 번호 : TTAS.IT-X1141.4

이 표준의 제정·개정 및 발간을 위해 아래와 같이 여러분들이 공헌하였습니다.

구분	성명	위원회 및 직위	연락처 (E-mail 등)	소속사
과제 제안	조영섭	PG101 위원	042-860-6942 yscho@etri.re.kr	ETRI
표준 초안 제출	조영섭	PG101 위원	042-860-6942 yscho@etri.re.kr	ETRI
표준 초안 검토 및 작성	이석래	PG101 의장	02-405-5330 sllee@kisa.or.kr	KISA
	진승헌	PG101 부의장	042-860-1254 jinsh@etri.re.kr	ETRI
	백종현	PG101 간사	02-405-5423 jhbaek@kisa.or.kr	KISA
	조상래	선임연구원	042-860-6939 slcho@etri.re.kr	ETRI
		외 PG101 위원		
표준안 심의	정교일	공통기반기술위워회 의장	042-860-1920 kyoil@etri.re.kr	ETRI
	원유재	공통기반기술위원회 부의장	02-405-5360 yjwon@kisa.or.kr	KISA
	이필중	공통기반기술위원회 부의장	054-279-2232 pjl@postech.ac.kr	포항공대
	김응배	공통기반기술위원회 부의장	042-860-5296 ebkim@etri.re.kr	ETRI
		외 TC1 위원		
사무국 담당	김 선	팀 장	031-724-0080 skim@tta.or.kr	TTA
	오흥룡	과 장	031-724-0083 hroh@tta.or.kr	TTA

정보통신단체표준(국문표준)

SAML 2.0 메타데이터
(SAML 2.0 Metadata)

발행인 : 김원식
발행처 : 한국정보통신기술협회
463-824, 경기도 성남시 분당구 서현동 267-2
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2007.12.