TTA Standard

정보통신단체표준
TTAS.IT-X1141.5

제정일: 2007 년 12 월 26 일

SAML 2.0 인증 문맥

SAML 2.0 Authentication Context

한국정보통신기술협회
Telecommunications Technology Association

정보통신단체표준 제정일 : 2007 년 12 월 26 일
TTAS.IT-X1141.5

SAML 2.0 인증 문맥

SAML 2.0 Authentication Context

TTA 한국정보통신기술협회
Telecommunications Technology Association

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 인증 문맥을 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 12. SAML 인증 문맥

부록 IV. SSL의 사용

부록 VI. 인증 문맥 타입들 XML 스키마

2. 주요 내용 요약

이 표준은 SAML 인증 문맥의 개념을 설명하며 인증 문맥 선언과 클래스에 대하여 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 국외표준(권고)

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

4.2 국내표준

- 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 참조표준(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 12 (SAML authentication context)의 내용, Appendix IV(Use of SSL)과 Appendix VI(Authentication Context types XML Schema)를 포함하는 국내표준이다.

5.2 참조한 표준(권고)과 본 표준의 비교표

상기 국제 권고에 대한 추가사항은 없으며, 장 구성은 다음과 같다.

본 표준	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 인증 문맥	12. SAML 인증 문맥	동일(번역)
부록 Ⅰ. SSL 의 사용	부록 Ⅳ. SSL 의 사용	동일(번역)
부록 Ⅱ. 인증 문맥 타입들 XML 스키마	부록 Ⅵ. 인증 문맥 타입들 XML 스키마	동일(번역)

6. 지적재산권 관련사항

2007년 12월 현재까지 이 표준과 관련하여 확인된 지적재산권은 없음

7. 적합인증 관련사항

7.1 적합인증 대상 여부

해당사항 없음

7.2 시험표준제정여부(해당 시험표준번호)

해당사항 없음

8. 표준의 이력

판수	제/개정일	제/개정내역
제1판	2007. 12. 26	제정

[참고사항]

본 표준은 영문표준을 한글화한 국내 표준으로, 본문 내용의 의미파악이 어렵거나 혼동이 발생할 경우, 영문표준 원문을 참조하시기 바랍니다.

Preface

1. The 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 authentication context.

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 12. SAML authentication context

Appendix Ⅳ. Use of SSL

Appendix Ⅵ. Authentication Context types XML Schema

2. The summary of contents

This standard describes the concept of authentication context and specifies authentication context declarations and classes.

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 The relationship of Reference Standards

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 12 (SAML authentication context), Appendix Ⅳ(Use of SSL) and Appendix Ⅵ (Authentication Context types XML Schema).

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.

This Standard	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 authentication context	12. SAML authentication context	equaled(trans)
Appendix Ⅰ. Use of SSL	Appendix Ⅳ. Use of SSL	equaled(trans)
Appendix Ⅱ. Authentication Context types XML Schema	Appendix Ⅵ. Authentication Context types XML Schema	equaled(trans)

6. The Statement of Intellectual Property Rights

As of December 2007, any IPRs related to this standard cannot be found.

7. The Statement of Conformance Testing and Certification

None

8. The History of Standard

Edition	Issued date	Contents
The 1st edition	2007. 12. 26	Established

목 차

Contents

SAML 2.0 인증 문맥

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. 용어정의

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).

f) 풀(Pull).

e) 푸시(Push).

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 용어정의(Additional definitions)

1.3.2.1 **접근 권한(Access rights)**: 주체가 자원에 대하여 가질수 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.

1.3.2.3 **능동적인 역할(Active role)**: 예를 들어 자원에 접근하는 등, 어떤 연산을 수행할 때, 시스템 엔티티가 가지는 역할.

1.3.2.4 **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.

1.3.2.5 **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.

1.3.2.6 **가맹, 가맹 그룹(Affiliation, affiliation Group)**: 사용자(principal)에 대한 식별자들의 (연계 관점에서) 단일한 네임스페이스를 공유하는 시스템 엔티티 집합.

1.3.2.7 **익명성(Anonymity)**: 익명 상태. 이것은 이름이나 신원이 알려지거나 노출되지

않도록 하는 조건을 나타냄.

1.3.2.8 **보장하는 기관(Asserting party)**: 공식적으로, 하나 또는 그 이상의 SAML 기관을 호스트팅하는 관리 도메인. 비공식적으로, SAML 기관의 한 인스턴스.

1.3.2.9 **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.

1.3.2.10 **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.

1.3.2.11 **속성 주장(Attribute assertion)**: 주체의 속성들에 대한 정보를 운반하는 주장.

1.3.2.12 **속성기관(Attribute authority)**: 속성 주장들을 생성하는 시스템 엔티티.

1.3.2.13 **인증(Authentication)**: 인증은 어떤 사람 또는 어떤 사물이 어느 정도의 신뢰 내에서 그것이 자신이 그렇다고 선언하는 것이 정말로 맞는지 아닌지를 결정하는 과정이다.

1.3.2.14 **인증 주장(Authentication assertion)**: 주체에 대하여 발생된 성공적인 인증 행위에 대한 정보를 운반하는 주장.

1.3.2.15 **인증 기관(Authentication authority)**: 인증 주장들을 생성하는 시스템 엔티티.

1.3.2.16 **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.

1.3.2.17 **인가 결정(Authorization decision)**: 인가 행위의 결과. 그 결과는 부정적인 될 수 있다. 즉, 그것은 주체가 자원에 대한 어떠한 접근 권한도 없음을 가리킨다.

1.3.2.18 **인가 결정 주장(Authorization decision assertion)**: 인가 결정에 대한 정보를 운반하는 주장.

1.3.2.19 **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.

1.3.2.20 **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.

1.3.2.21 **크리덴셜(Credentials)**: 주장되는 사용자(principal) 신원을 확인하기 위해 전송되는 데이터.

1.3.2.22 **최종 사용자(End user)**: 응용 목적으로 자원을 사용하는 자연인(natural person).

1.3.2.23 **엔티티(Entity)**: “시스템 엔티티”를 참고한다.

1.3.2.24 **연계하다(Federate)**: 둘 또는 그 이상의 엔티티들을 함께 연결하거나 또는 바인딩하기.

1.3.2.25 **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).

1.3.2.26 **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.

1.3.2.27 **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.

1.3.2.28 **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.

1.3.2.29 **아이덴터티, 신원(Identity)**: 엔티티의 본질. 어떤 사물의 아이덴터티는 어떤 사물의 특징들로 종종 설명된다. 이 특성들 중에 식별자들이 포함될 수 있다.

1.3.2.30 **아이덴터티 탈연계(Identity defederation)**: 제공자들이 일정 집합의 식별자와/또는 속성들을 통해 사용자(principal)을 참조하는 것을 그만두기로 동의할 때, 발생하는 동작.

1.3.2.31 **아이덴터티 연계(Identity federation)**: 사용자(principal)을 위해 연계된 아이덴터티를 생성하는 동작.

1.3.2.32 **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.

1.3.2.33 **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.

1.3.2.34 **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.

1.3.2.35 **로그아웃, 로그오프, 사인-오프(Logout, logoff, sign-off)**: 일종의 처리. 이 처리를 통해 사용자는 단순 세션 또는 리치(rich) 세션을 종료하기를 원한다는 것을 알린다.

1.3.2.36 **마크업 언어(Markup language)**: 특수한 목적으로 XML 문서의 구조에 적용되

는 일단의 XML 요소들과 XML 속성들. 마크업 언어는 일반적으로 일단의 XML 스키마들과 동반되는 문서로 정의된다.

1.3.2.37 **이름 제한자(Name qualifier)**: 다른 사용자들(principals)을 나타내기 위해, (연계 관점에서) 하나 이상의 네임스페이스에서 사용될 수 있는 하나의 식별자가 모호해지지 않도록 해 주는 문자열.

1.3.2.38 **기관, 당사자(Party)**: 비공식적으로, 주장을 수신하거나 또는 자원을 접근하는 것과 같은 어떤 처리나 통신에 참여하는 하나 또는 그 이상의 사용자들(principals).

1.3.2.39 **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.

1.3.2.40 **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.

1.3.2.41 **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.

1.3.2.42 **사용자 아이덴터티(Principal identity)**: 일반적으로 식별자인 어떤 사용자 아이덴터티의 표현.

1.3.2.43 **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.

1.3.2.44 **프로토콜 바인딩(Protocol binding)**: “바인딩”을 참고한다.

1.3.2.45 **제공자(Provider)**: 아이덴터티 제공자들과 서비스 제공자들 둘 다를 가리키는 포괄적인 표현.

1.3.2.46 **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.

1.3.2.47 **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.

1.3.2.48 **자원(Resource)**: (예를 들어, 파일 형태나 메모리 형태, 등등으로) 하나의 정

보 시스템에 포함되는 데이터, 또한:

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

1.3.2.49 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.

1.3.2.50 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.

1.3.2.51 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.

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

1.3.2.53 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.

1.3.2.54 보안 주장(Security assertion): 보안 아키텍처의 문맥에서 철저히 검사된 주장.

1.3.2.55 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.

1.3.2.56 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.

1.3.2.57 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.

1.3.2.58 **서비스 제공자(Service provider)**: 어떤 시스템 엔티티에게 주어진 역할. 이 역할을 통해 그 시스템 엔티티는 사용자들(principals) 또는 다른 시스템 엔티티들에게 서비스들을 제공한다.

1.3.2.59 **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.

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

1.3.2.61 **세션 기관(Session authority)**: 세션들과 관련된 상태를 어떤 시스템 엔티티가 유지할 때, 그 기관에게 주어진 역할.

1.3.2.62 **세션 참여자(Session participant)**: 어떤 기관이 적어도 하나의 세션 기관과 어떤 세션에 참여할 때, 그 기관에게 주어진 역할.

1.3.2.63 **사인-오프(Sign-off)**: “로그아웃”을 참고한다.

1.3.2.64 **사인-온(Sign-on)**: “로그인”을 참고한다.

1.3.2.65 **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.

1.3.2.66 **주체(Subject)**: 어떤 보안 도메인 문맥에서 하나의 사용자(principal). SAML 주장들은 주체에 대한 선언들을 생성한다.

1.3.2.67 **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.

1.3.2.68 **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.

1.3.2.69 **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.

1.3.2.70 **XML 요소(XML attribute)**: XML 요소의 시작-태그(start-tag)에 포함되어 있고, 이름과 값을 가지는 XML 데이터 구조.

1.3.2.71 **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.

1.3.2.72 **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 $10_{Decimal}$)을 사용하여 나타내도록 정규화된다. 문자열들 (또는 문자열로부터 유도된 타입들)로 정의된 XML 속성 값

들은 W3C XML 1.0, 3.3.3절에서 설명된 것처럼 정규화된다. 모든 공백 문자들은 스페이스(blanks) (ASCII code $32_{Decimal}$)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 내에서 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. ID와 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. 인증 문맥 개념

이 표준은 인증 문맥(authentication context) 선언(declarations)들의 정의에 대한 문법과 인증 문맥 클래스들의 초기 리스트를 정의한다.

만약 의지하는 기관이 인증 기관에 의한 사용자 인증을 의지한다면, 의지하는 기관은 어떠한 신뢰 수준에서 인증이 수행되었는지를 평가하기 위해 주장뿐만 아니라 추가적인 정보를 요구할 수 있다. 이 표준은 인증 문맥 선언의 생성을 위한 XML 스키마를 정의한다. 인증 문맥 선언은 인증 기관이 의지하는 기관에게 이러한 추가적인 정보를 제공하는 것을 허용하는 XML 문서이다. 추가적으로, 이 표준은 많은 인증 문맥 클래스를 정의한다. 인증 문맥 클래스는 많은 인증 문맥 선언들이 속하게 되는 범주(category)들로써, 인증 문맥 클래스는 인증 문맥의 해석을 단순화시킬 수 있다.

SAML은 인증 기관들이 사용자에게 아이덴터티들을 발급하고 사용자들이 그들 자신을 인증 기관에 인증하는데 있어 단일 기술, 단일 프로토콜 또는 단일 정책을 규정하지는 않는다. 다른 인증 기관들은 그들이 사용자들을 어떻게 인증하는지에 대해 다른 기술들을 선택하고 다른 처리 절차를 따르며 다른 법률적인 의무를 가질 수 있다.

인증 기관의 선택들은 인증기관들과 상호 작용하는 의지하는 기관들의 요구사항에 따라 대부분 결정될 것이다. 이들 요구사항은 그 자체로 의지하는 기관이 사용자에게 제공할 서비스의 본질에 따라 결정될 것이다. 이들 서비스의 본질은 교환되는 정보의 민감도, 연관된 금융 가치(financial value), 의지하는 기관들의 위험 허용도(risk tolerance) 등을 포함한다.

따라서, 사소하지 않은 어떠한 서비스에 대해서도, 만약 의지하는 기관이 인증 기관으로부터 수신하는 인증 주장에 대해 충분히 신뢰하려 한다면, 의지하는 기관은 인증 기관이 사용자에 대한 인증 주장을 생성하는데 있어, 어떤 기술, 프로토콜 그리고 어떤 절차를 따라 인증하였는지 알 필요할 것이다. 실제 주장의 출처에 대한 신뢰와 이러한 정보를 가지고, 의지하는 기관은 인증 주장의 주체가 어떠한 서비스에 접근하는 것을 허용할 지에 대한 자격 판단(entitlement decision)을 더 잘 결정할 것이다.

인증 문맥은 의지하는 기관이 인증 주장에 대한 자격 판단을 하기 전에 요구할 수 있는, 인증 주장 그 자체에 대한 추가적인 정보로써 정의된다. 이와 같은 문맥은 실제 사용된 인증 방식을 포함할 수 있지만, 인증 방식에만 한정되지는 않는다.

3. 인증 문맥 선언

의지하는 기관이 인증 기관에 의해 다른 엔티티의 인증을 신뢰하려 한다면, 의지하는 기관은 인증에 대한 위험-관리(risk-management)를 수행하기 위해서 인증 사실 자체뿐만 아니라 추가적인 정보를 요구할 수 있다. 추가적인 정보는 다음을 포함할 수 있다.

- 초기 사용자 식별 메커니즘 (예를 들어, 대면, 온라인, 공유 비밀 방식 등)
- 크리덴셜의 훼손(compromise)을 최소화하기 위한 메커니즘들 (예를 들어, 크리덴셜의 갱신 주가, 클라이언트-측 키 생성 방식)
- 크리덴션을 저장하고 보호하기 위한 메커니즘들 (예를 들어, 스마트카드, 패스워드 규칙들)
- 인증 메커니즘이나 또는 방식 (예를 들어, 패스워드)

위에 나열된 특성에 대한 변이와 순열(variations and permutations)은 모든 인증 주장들이 의지하는 기관에서 그 주장에 대해 가질 수 있는 신뢰도에 대해 동일하지는 않다는 것을 보장한다. 특정 인증 보장은 이들 변수들의 각각에 대한 값들에 의해 특징지어질 수 있을 것이다.

하나의 SAML 인증 기관은 의지하는 기관에게 인증 문맥 선언의 형태로 추가적인 인증 문맥 정보를 전달할 수 있다. 인증 문맥 선언은 인증 기관이 의지하는 기관에게 제공하는, 인증 주장 내에 직접적으로 삽입되거나 또는 참조되는 하나의 XML 문서이다.

SAML 요청자는 인증 요청에 있는 문맥을 식별함으로써 엔티티 인증이 특정 인증 문맥에 부합되어 이루어지도록 요청할 수 있다. 요청자는 또한 인증이 (협약된 “exceeds”의 정의에 대해) 표기된 요청 값을 초과하는 인증 문맥으로 인증이 수행되어야 한다는 것을 기술할 수 있다.

3.1. 데이터 모델

이 표준에서 정의된 특정 인증 문맥 선언은 인증 기관이 아이덴터티를 발급하기 전에 주체를 검증하고, 인증의 기반이 되는 비밀들(secrets)을 보호하고, 이 인증에 사용된 처리들(processes), 절차들(procedures)과 메커니즘들의 특성들을 표현할 수 있다. 이들 특성들은 다음과 같이 인증 문맥 스키마로 범주화된다.

- 식별 – 인증 기관이 주체와 주체로 알려진 아이덴터티 (또는 이름)과의 연관성을 초기에 생성하는데 사용하는 프로세스들과 메커니즘을 설명하는 특성들이다.
- 기술적 보호 – 주체가 인증 기관에게 인증되도록 해 주는 지식 또는 소유(possession)인 “secret” 이 어떻게 안전하게 관리되는지를 설명하는 특성들이다.

- 운영 보호 장치(operational protection) – 인증 기관이 채택한 절차적인 보안 제어들을 설명하는 특성들이다. 예를 들어, 보안 감사(security audits), 레코드 기록(record archival)
- 인증 방식 – 발급된 주장의 주체가 인증 기관에서 인증되는 메커니즘을 정의하는 특성들이다. 예를 들어, 패스워드 대 스마트카드 방식이 이에 해당한다.
- 규율 협약들(governing agreements) – 인증 사건 그리고/또는 그것과 연관된 기술적인 인증 기반 구조의 기반이 되는 법체계 틀(legal framework)을 설명하는 특성들이다. 예를 틀어 책임 제한들과 계약상의 의무들이 이에 해당한다.

3.2. 확장성

인증 문맥 선언 스키마는 <Extension> 요소를 통해 잘 정의된 확장성을 가진다. 인증 기관은 이 요소를 사용하여 (소비하는 의지하는 기관이 이 확장들을 이해할 수 있다는 것을 가정하면) 그들이 발급하는 SAML 주장들에 대한 추가적인 인증 문맥 세부사항들을 삽입할 수 있다. 이러한 추가적인 요소들은 선언 자체에 적용되는 인증 문맥 기본(base) 또는 클래스 스키마와는 분리된 XML 네임스페이스로 존재해야만 한다.

3.3. 처리 규칙들

인증 문맥 선언들에 대한 추가적인 처리는 ITU-T X.1141 8장에 기술된다. 이들 처리 규칙들은 결과적으로 특정 인증 문맥 선언들의 상대적인 강도(strength)와 품질(quality)의 공통적인 해석을 공유하는 배치환경을 가정하며, 절대적인 조건이나 구현물들이 반드시 따라야 하는 규칙으로 표현될 수는 없다.

3.4. 스키마

이 절은 비 규범적(non-normative)이다.

개별적으로 일반화된 선언의 검증을 위해 사용되는 완전한 인증 문맥 타입 XML 스키마와 인증 문맥 XML 스키마 자체의 내용은 부록 II에 나열된다.

4. 인증 문맥 클래스

서로 다른 특성들의 순열의 개수는 이론적으로는 유일한 인증 문맥이 무한대 있음을 보장한다. 이것은 이론적으로는 어떠한 특정 의지하는 기관도 임의의 인증 문맥 선언들을 분석(parsing)할 수 있으며, 더욱 중요한 것은 연관된 인증 주장의 “품질”을 평가하기 위해 선언들을 분석할 수 있어야 된다는 것을 암시한다. 이와 같은 평가는 단순한 문제가 아니다.

다행히, 최적화가 가능하다. 실제로, 많은 인증 문맥은 산업 관례와 기술(industry practice and technology)에 의해 결정된 범주에 속할 것이다. 예를 들어, 많은 B2C 웹 브라우저 인증 문맥들은 사용자가 TLS로 보호되는 세션상에서 패스워드를 제출하는 것을 통해 인증 기관의 인증이 이루어지는 것으로써 정의될 것이다. 기업 세계에서는 인증서 기반 인증이 일반적일 것이다. 물론 완전한 인증 문맥은 사용자가 어떻게 인증되는지에 대한 사항으로만 제약되지는 않는다. 그럼에도 불구하고 인증 방식은 종종 가장 분명한 특성이 되고, 이와 같이 관련된 인증 문맥들의 클래스에 대한 유용한 구분자로 작용할 수 있다.

이 표준에서는 인증 문맥 개념을 일련의 인증 문맥 클래스들의 정의로 표시한다. 각각의 클래스는 완전한 인증 문맥들 집합의 적절한 부분 집합(subset)을 정의한다. 클래스들은 인증 기술들에 대한 현재의 관례와 기술들에 대한 대표로써 선택되어 왔으며, 보장하는 기관과 의지하는 기관들에게 인증 문맥 이슈를 참조할 때, 편리한 속기(shorthand)를 제공한다.

예를 들어, 인증 기관은 그것이 의지하는 기관에게 주장을 제공할 때, 완전한 인증 문맥 선언과 함께 해당 인증 문맥이 속하는 인증 문맥 클래스를 포함할 수 있다. 일부 의지하는 기관에 대해서, 이 주장은 의지하는 기관이 연관된 인증 주장에게 적절한 수준의 신뢰를 할당할 수 있을 만큼 충분할 수 있다. 다른 의지하는 기관들은 완전한 인증 선언 자체를 평가하는 것을 선호할 수 있을 것이다. 마찬가지로, 특정 인증 문맥 선언의 완전한 세부 사항을 나열하는 것이 요구되기보다는 인증 문맥 클래스를 참조하는 능력이, 의지하는 기관이 인증 기관에게 기자신의 요구(desire and requirement)를 표현하는 방식을 단순화시킬 수 있을 것이다.

4.1. 인증 문맥 클래스의 이점

추가적인 클래스 계층(layer)의 도입과 대표적이며 유연한(flexible) 클래스들의 초기 리스트는 다음과 같은 상황을 기대할 수 있도록 해준다.

- 인증 기관과 의지하는 기관에게 토론의 프레임워크를 제공함으로써 어떤 것이 받아들일 수 있는 인증 문맥들인지에 대해 그들이 협의를 도출하는 것을 더 쉽게 해 준다.

- 의지하는 기관이 인증 기관에게 한 단계 더 높은 주장을 요청할 때, 그들의 선호도를 가리키는 것을 더 쉽게 해 준다.
- 의지하는 기관들에게 연관된 클래스에 의해 충족되는 선택권을 제공함으로써, 의지하는 기관이 인증 문맥 선언을 처리하는 부담을 단순화시킨다.
- 의지하는 기관을 새로운 인증 기술의 충격으로부터 격리시킨다.
- 인증 기관이 예를 들어 WSDL을 통해 그들의 인증 능력을 게시하는 것을 더 쉽게 해 준다.

4.2. 처리 규칙들

인증 문맥 클래스들에 대한 추가적인 처리는 ITU-T X.1141 8장에 기술된다. 대부분의 경우, 이들 처리 규칙들은 결과적으로 특정 인증 문맥 클래스들의 상대적인 강도(strength)와 품질(quality)의 공통적인 해석을 공유하는 배치환경을 가정하며, 절대적인 조건이나 구현물들이 반드시 따라야 하는 규칙으로 표현될 수는 없다.

4.3. 확장성

핵심 인증 문맥 선언 스키마가 그렇듯이, 별도의 인증 문맥 클래스는 트리 구조의 어떤 위치에도 <Extension> 요소를 허용한다. 일반적으로, <Extension> 요소가 <xs:choice> 요소의 자식으로 나타날 때, 기본 타입(base type)의 제약으로서 적절한 클래스 스키마 정의를 생성할 때 이 옵션은 제거된다. <Extension> 요소가 <xs:sequence> 요소의 선택적인 자식으로 나타날 때, <Extension> 요소는 어떠한 필수 요소들에 추가적으로 남겨지는 것이 허용된다.

따라서, 인증 문맥 선언들은 (다른 네임스페이스를 가진 추가적인 요소와 함께) <Extension> 요소를 포함할 수 있으며, 만약 그들이 스키마의 다른 요구 조건을 만족한다면, 여전이 인증 문맥 클래스 스키마들에 적합할 수 있게 된다.

인증 문맥 클래스 스키마들은 기본 인증 문맥 스키마에 있는 타입 정의를 제약한다. 확장점으로써, 인증 문맥 클래스 스키마들은 자체적으로 더욱 더 제약될 수 있다. 그들의 타입 정의는 더욱 더 강력하게 정의된 인증 문맥을 원하는 일부 커뮤니티에 의해 정의될 수 있는 다른 스키마에서 기본 타입으로 동작할 수 있다. 논리적인 불일치를 해소하기 위해, 이와 같은 어떠한 스키마 확장들로 클래스 스키마의 타입 정의를 더 제약할 수 있다. 이러한 제약을 하기 위해, 인증 문맥 클래스 스키마들은 이 타입의 유도(derivation)을 방지하기 위해 <schema> 요소의 finalDefault 속성의 값을 "extension"으로 정의할 수 있다.

4.4. 스키마들

인증 문맥 클래스들은 다음 절에 나열된다. 이들 클래스들은 알파벳 순서로 나열된다. 클래스가 나열되는 순서는 그들의 순위와 무관하다. 구현자들은 ITU-T X.1141의 13장에서 기술된 것과 같이 어떤 클래스들 지원할 지를 선택할 수 있다. 클래스들은 다음과

같은 처음 부분을 갖는 URI들로 유일하게 식별된다.

```
urn:oasis:names:tc:SAML:2.0:ac:classes
```

클래스 스키마들은 기본 인증 문맥 “types” 스키마의 부분들을 제약함으로써 정의된다. 어떤 인증 문맥 클래스 스키마에 대해 유효한 XML 인스턴스(instance)는 해당 인증 문맥 클래스에 순응(conform)한다고 말할 수 있다.

클래스 스키마가 요소들과 타입을 클래스 스키마 네임스페이스에 임포트(import)하고 재정의하기 때문에, 클래스와 호환하는 인증 문맥 선언들은 동시에 기본 인증 문맥 스키마에 대해 유효하지는 않는다.

4.4.1. Internet protocol

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol

사용자가 제공된 IP 주소를 사용함으로써 인증될 때, 인터넷 프로토콜 클래스가 적용될 수 있다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
  targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
        Document identifier: saml-schema-authn-context-ip-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
```

```
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="IPAddress"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

4.4.2. InternetProtocolPassword

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword

인터넷 프로토콜 패스워드(Internet Protocol Password) 클래스는 제공된 IP 주소의 사용과 함께 추가적으로 사용자 이름/패스워드를 제공함으로써 사용자를 인증할 때, 적용될 수 있다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
  targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
```

```
xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword"
finalDefault="extension"
blockDefault="substitution"
version="2.0">

<xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

  <xs:annotation>
    <xs:documentation>
      Class identifier:
           urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword
      Document identifier: saml-schema-authn-context-ippword-2.0
      Location: http://docs.oasis-open.org/security/saml/v2.0/
      Revision history:
        V2.0 (March, 2005):
          New authentication context class schema for SAML V2.0.
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclarationBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection" minOccurs="0"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="GoverningAgreements" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthnMethodBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorBaseType">
        <xs:sequence>
          <xs:element ref="Password"/>
          <xs:element ref="IPAddress"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
```

```
            </xs:sequence>
          </xs:restriction>
        </xs:complexContent>
      </xs:complexType>

    </xs:redefine>

</xs:schema>
```

4.4.3. Kerberos

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos

사용자가 커버로스 티켓(Kerberos ticket)을 획득하기 위해, 지역 인증 기관에 패스워드를 사용하여 인증하였을 때, 이 클래스가 적용될 수 있다. 해당 커버로스 티켓은 이후 네트워크 인증을 위해 사용된다.

주의 : 인증 기관이 사용자를 인증할 때 IETF RFC 1510 커버로스 키 분배 센터에 의해 사용된 선-인증(pre-authentication) 데이터 타입을 이 인증 문맥을 통해 가리키는 것이 가능하다. 이 정보를 얻기 위해 인증 기관이 사용한 방식은 이 표준 영역 밖이다. 그러나 선-인증 데이터 타입과 다른 어떠한 커버로스 관련 문맥 세부사항(예를 들면, 티켓 생명주기)을 인증 기관에 전달하기 위해 신뢰 모델이 채택되는 것을 강력하게 권고한다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
        Document identifier: saml-schema-authn-context-kerberos-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
```

```
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
              <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="SharedSecretChallengeResponse"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SharedSecretChallengeResponseType">
      <xs:complexContent>
        <xs:restriction base="SharedSecretChallengeResponseType">
          <xs:attribute name="method" type="xs:anyURI"
                fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>
```

```
</xs:schema>
```

이 클래스에 순응하는 XML 인스턴스의 예는 다음과 같다.

```
<AuthenticationContextDeclaration
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos">

  <AuthnMethod>

    <PrincipalAuthenticationMechanism preauth="0">
      <RestrictedPassword>
        <Length min="4"/>
      </RestrictedPassword>
    </PrincipalAuthenticationMechanism>

    <Authenticator>
      <AuthenticatorSequence>
        <SharedSecretChallengeResponse
method="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"/>
      </AuthenticatorSequence>
    </Authenticator>

  </AuthnMethod>

</AuthenticationContextDeclaration>
```

주의 : SSL의 사용은 부록 I에 제시된다.

4.4.4. MobileOneFactorUnregistered

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered

어떠한 모바일(mobile) 고객 등록 절차도 없으며, 명시적인 최종 사용자와의 상호작용이 없는 모바일 기기의 인증을 반영한다. 이 문맥 클래스는 단지 디바이스만을 인증하며 결코 사용자를 인증하지는 않는다. 모바일 연산자(mobile operator)가 아닌 서비스가 그들의 인증 프로세스에 안전한 디바이스 인증을 추가하기를 원할 때, 이 클래스가 유용하다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
  targetNamespace=
        "urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
```

```
<xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

  <xs:annotation>
    <xs:documentation>
      Class identifier:
           urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered
      Document identifier: saml-schema-authn-context-mobileonefactor-unreg-2.0
      Location: http://docs.oasis-open.org/security/saml/v2.0/
      Revision history:
        V2.0 (March, 2005):
          New authentication context class schema for SAML V2.0.
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclarationBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection" minOccurs="0"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="GoverningAgreements" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthnMethodBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="DigSig"/>
            <xs:element ref="ZeroKnowledge"/>
            <xs:element ref="SharedSecretChallengeResponse"/>
            <xs:element ref="SharedSecretDynamicPlaintext"/>
            <xs:element ref="AsymmetricDecryption"/>
            <xs:element ref="AsymmetricKeyAgreement"/>
```

```
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="SSL"/>
              <xs:element ref="MobileNetworkNoEncryption"/>
              <xs:element ref="MobileNetworkRadioEncryption"/>
              <xs:element ref="MobileNetworkEndToEndEncryption"/>
              <xs:element ref="WTLS"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="OperationalProtectionType">
      <xs:complexContent>
        <xs:restriction base="OperationalProtectionType">
          <xs:sequence>
            <xs:element ref="SecurityAudit"/>
            <xs:element ref="DeactivationCallCenter"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="TechnicalProtectionBaseType">
      <xs:complexContent>
        <xs:restriction base="TechnicalProtectionBaseType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="PrivateKeyProtection"/>
              <xs:element ref="SecretKeyProtection"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrivateKeyProtectionType">
      <xs:complexContent>
        <xs:restriction base="PrivateKeyProtectionType">
          <xs:sequence>
            <xs:element ref="KeyStorage"/>
```

```
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SecretKeyProtectionType">
      <xs:complexContent>
        <xs:restriction base="SecretKeyProtectionType">
          <xs:sequence>
            <xs:element ref="KeyStorage"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyStorageType">
      <xs:complexContent>
        <xs:restriction base="KeyStorageType">
          <xs:attribute name="medium" use="required">
            <xs:simpleType>
              <xs:restriction base="mediumType">
                <xs:enumeration value="MobileDevice"/>
                <xs:enumeration value="MobileAuthCard"/>
                <xs:enumeration value="smartcard"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SecurityAuditType">
      <xs:complexContent>
        <xs:restriction base="SecurityAuditType">
          <xs:sequence>
            <xs:element ref="SwitchAudit"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="IdentificationType">
      <xs:complexContent>
        <xs:restriction base="IdentificationType">
          <xs:sequence>
            <xs:element ref="GoverningAgreements"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="nym">
            <xs:simpleType>
              <xs:restriction base="nymType">
                <xs:enumeration value="anonymity"/>
```

```
                    <xs:enumeration value="pseudonymity"/>
                  </xs:restriction>
                </xs:simpleType>
              </xs:attribute>
            </xs:restriction>
          </xs:complexContent>
        </xs:complexType>

    </xs:redefine>

</xs:schema>
```

주의 : SSL의 사용은 부록 I에 제시된다.

4.4.5. MobileTwoFactorUnregistered

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered

어떠한 모바일 고객 등록 절차도 없으며, 안전한 디바이스와 사용자 PIN과 같이 두 가지 요인(two-factor)에 기반한 인증 방식을 반영한다. 모바일 연산자(mobile operator)가 아닌 서비스가 등록시 모바일 전화기 데이터를 획득함으로써 그들의 고객 ID를 모바일에서 제공된 두 가지 요인 인증 서비스와 연결시키기를 원할 때, 이 클래스가 유용하다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
      targetNamespace=
          "urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered"
    finalDefault="extension"
    blockDefault="substitution"
    version="2.0">

    <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

      <xs:annotation>
        <xs:documentation>
          Class identifier:
              urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
          Document identifier: saml-schema-authn-context-mobiletwofactor-unreg-2.0
          Location: http://docs.oasis-open.org/security/saml/v2.0/
          Revision history:
            V2.0 (March, 2005):
              New authentication context class schema for SAML V2.0.
        </xs:documentation>
      </xs:annotation>

      <xs:complexType name="AuthnContextDeclarationBaseType">
        <xs:complexContent>
          <xs:restriction base="AuthnContextDeclarationBaseType">
```

```
        <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection" minOccurs="0"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="GoverningAgreements" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthnMethodBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="DigSig"/>
            <xs:element ref="ZeroKnowledge"/>
            <xs:element ref="SharedSecretChallengeResponse"/>
            <xs:element ref="SharedSecretDynamicPlaintext"/>
            <xs:element ref="AsymmetricDecryption"/>
            <xs:element ref="AsymmetricKeyAgreement"/>
            <xs:element ref="ComplexAuthenticator"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="ComplexAuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ComplexAuthenticatorType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="SharedSecretChallengeResponse"/>
            <xs:element ref="SharedSecretDynamicPlaintext"/>
          </xs:choice>
          <xs:element ref="Password"/>
        </xs:sequence>
```

```
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorTransportProtocolType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorTransportProtocolType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="SSL"/>
            <xs:element ref="MobileNetworkNoEncryption"/>
            <xs:element ref="MobileNetworkRadioEncryption"/>
            <xs:element ref="MobileNetworkEndToEndEncryption"/>
            <xs:element ref="WTLS"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="OperationalProtectionType">
    <xs:complexContent>
      <xs:restriction base="OperationalProtectionType">
        <xs:sequence>
          <xs:element ref="SecurityAudit"/>
          <xs:element ref="DeactivationCallCenter"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="TechnicalProtectionBaseType">
    <xs:complexContent>
      <xs:restriction base="TechnicalProtectionBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="PrivateKeyProtection"/>
            <xs:element ref="SecretKeyProtection"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrivateKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="PrivateKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyActivation"/>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
```

```
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="SecretKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="SecretKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyActivation"/>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="KeyStorageType">
    <xs:complexContent>
      <xs:restriction base="KeyStorageType">
        <xs:attribute name="medium" use="required">
          <xs:simpleType>
            <xs:restriction base="mediumType">
              <xs:enumeration value="MobileDevice"/>
              <xs:enumeration value="MobileAuthCard"/>
              <xs:enumeration value="smartcard"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="SecurityAuditType">
    <xs:complexContent>
      <xs:restriction base="SecurityAuditType">
        <xs:sequence>
          <xs:element ref="SwitchAudit"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="IdentificationType">
    <xs:complexContent>
      <xs:restriction base="IdentificationType">
        <xs:sequence>
          <xs:element ref="GoverningAgreements"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="nym">
          <xs:simpleType>
            <xs:restriction base="nymType">
              <xs:enumeration value="anonymity"/>
              <xs:enumeration value="pseudonymity"/>
```

```
                </xs:restriction>
              </xs:simpleType>
            </xs:attribute>
          </xs:restriction>
        </xs:complexContent>
      </xs:complexType>

    </xs:redefine>

</xs:schema>
```

4.4.6. MobileOneFactorContract

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract

모바일 고객 등록 절차와 단일 요인 인증을 반영한다. 예를 들어, 실시간 사용자 인증을 위해 PIN이나 생체정보를 요구하지 않지만, 키 저장소에 대한 변형 억제(tamper resistant) 메모리를 가진 모바일 MSISDN(Mobile Station Integrated Services Digital Network)과 같은 전자 서명 디바이스에서 적용할 수 있다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
  targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
            urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract
        Document identifier: saml-schema-authn-context-mobileonefactor-reg-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
```

```
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="DigSig"/>
              <xs:element ref="ZeroKnowledge"/>
              <xs:element ref="SharedSecretChallengeResponse"/>
              <xs:element ref="SharedSecretDynamicPlaintext"/>
              <xs:element ref="AsymmetricDecryption"/>
              <xs:element ref="AsymmetricKeyAgreement"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="SSL"/>
              <xs:element ref="MobileNetworkNoEncryption"/>
              <xs:element ref="MobileNetworkRadioEncryption"/>
              <xs:element ref="MobileNetworkEndToEndEncryption"/>
              <xs:element ref="WTLS"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
```

```
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="OperationalProtectionType">
    <xs:complexContent>
      <xs:restriction base="OperationalProtectionType">
        <xs:sequence>
          <xs:element ref="SecurityAudit"/>
          <xs:element ref="DeactivationCallCenter"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="TechnicalProtectionBaseType">
    <xs:complexContent>
      <xs:restriction base="TechnicalProtectionBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="PrivateKeyProtection"/>
            <xs:element ref="SecretKeyProtection"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrivateKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="PrivateKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="SecretKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="SecretKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="KeyStorageType">
    <xs:complexContent>
      <xs:restriction base="KeyStorageType">
        <xs:attribute name="medium" use="required">
```

```
            <xs:simpleType>
              <xs:restriction base="mediumType">
                <xs:enumeration value="smartcard"/>
                <xs:enumeration value="MobileDevice"/>
                <xs:enumeration value="MobileAuthCard"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SecurityAuditType">
      <xs:complexContent>
        <xs:restriction base="SecurityAuditType">
          <xs:sequence>
            <xs:element ref="SwitchAudit"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="IdentificationType">
      <xs:complexContent>
        <xs:restriction base="IdentificationType">
          <xs:sequence>
            <xs:element ref="PhysicalVerification"/>
            <xs:element ref="WrittenConsent"/>
            <xs:element ref="GoverningAgreements"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="nym">
            <xs:simpleType>
              <xs:restriction base="nymType">
                <xs:enumeration value="anonymity"/>
                <xs:enumeration value="verinymity"/>
                <xs:enumeration value="pseudonymity"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

4.4.7. MobileTwoFactorContract

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract

모바일 고객 등록 절차와 두 가지 요인 인증을 반영한다. 예를 들어, PIN 또는 생체 정보를 통해 사용자 아이덴터티와 의도의 명시적인 증명을 요구하는 GSM SIM과 같이 키 저장소에 대한 변형 억제 메모리를 가진 전자 서명 디바이스에서 적용될 수 있다..

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace=
          "urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
             urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
        Document identifier: saml-schema-authn-context-mobiletwofactor-reg-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
```

```
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="DigSig"/>
            <xs:element ref="ZeroKnowledge"/>
            <xs:element ref="SharedSecretChallengeResponse"/>
            <xs:element ref="SharedSecretDynamicPlaintext"/>
            <xs:element ref="AsymmetricDecryption"/>
            <xs:element ref="AsymmetricKeyAgreement"/>
            <xs:element ref="ComplexAuthenticator"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="ComplexAuthenticatorType">
    <xs:complexContent>
      <xs:restriction base="ComplexAuthenticatorType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="SharedSecretChallengeResponse"/>
            <xs:element ref="SharedSecretDynamicPlaintext"/>
          </xs:choice>
          <xs:element ref="Password"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorTransportProtocolType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorTransportProtocolType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="SSL"/>
            <xs:element ref="MobileNetworkNoEncryption"/>
            <xs:element ref="MobileNetworkRadioEncryption"/>
            <xs:element ref="MobileNetworkEndToEndEncryption"/>
            <xs:element ref="WTLS"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="OperationalProtectionType">
```

```
    <xs:complexContent>
      <xs:restriction base="OperationalProtectionType">
        <xs:sequence>
          <xs:element ref="SecurityAudit"/>
          <xs:element ref="DeactivationCallCenter"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="TechnicalProtectionBaseType">
    <xs:complexContent>
      <xs:restriction base="TechnicalProtectionBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="PrivateKeyProtection"/>
            <xs:element ref="SecretKeyProtection"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrivateKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="PrivateKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyActivation"/>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="SecretKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="SecretKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyActivation"/>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="KeyStorageType">
    <xs:complexContent>
      <xs:restriction base="KeyStorageType">
        <xs:attribute name="medium" use="required">
          <xs:simpleType>
            <xs:restriction base="mediumType">
```

```
                    <xs:enumeration value="MobileDevice"/>
                    <xs:enumeration value="MobileAuthCard"/>
                    <xs:enumeration value="smartcard"/>
                  </xs:restriction>
                </xs:simpleType>
              </xs:attribute>
            </xs:restriction>
          </xs:complexContent>
        </xs:complexType>

        <xs:complexType name="SecurityAuditType">
          <xs:complexContent>
            <xs:restriction base="SecurityAuditType">
              <xs:sequence>
                <xs:element ref="SwitchAudit"/>
                <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
              </xs:sequence>
            </xs:restriction>
          </xs:complexContent>
        </xs:complexType>

        <xs:complexType name="IdentificationType">
          <xs:complexContent>
            <xs:restriction base="IdentificationType">
              <xs:sequence>
                <xs:element ref="PhysicalVerification"/>
                <xs:element ref="WrittenConsent"/>
                <xs:element ref="GoverningAgreements"/>
                <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
              </xs:sequence>
              <xs:attribute name="nym">
                <xs:simpleType>
                  <xs:restriction base="nymType">
                    <xs:enumeration value="anonymity"/>
                    <xs:enumeration value="verinymity"/>
                    <xs:enumeration value="pseudonymity"/>
                  </xs:restriction>
                </xs:simpleType>
              </xs:attribute>
            </xs:restriction>
          </xs:complexContent>
        </xs:complexType>

      </xs:redefine>

    </xs:schema>
```

주의 : SSL의 사용은 부록 I에 제시된다.

4.4.8. Password

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:Password

사용자가 보호되지 않은 HTTP 세션에서 패스워드를 제출함으로써 인증기관에 인증할 때, 이 클래스가 적용 가능하다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Password
        Document identifier: saml-schema-authn-context-pword-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
```

```
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
Following is an example of an XML instance that conforms to the context class schema:
<AuthenticationContextDeclaration
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password">

  <AuthnMethod>
    <Authenticator>
      <AuthenticatorSequence>
        <RestrictedPassword>
          <Length min="4"/>
        </RestrictedPassword>
      </AuthenticatorSequence>
    </Authenticator>
  </AuthnMethod>

</AuthenticationContextDeclaration>
```

4.4.9. PasswordProtectedTransport

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

사용자가 보호되는 HTTP 세션에서 패스워드를 제출함으로써 인증기관에 인증할 때, 이 클래스가 적용 가능하다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
    targetNamespace=
        "urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
            urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
```

```
      Document identifier: saml-schema-authn-context-ppt-2.0
      Location: http://docs.oasis-open.org/security/saml/v2.0/
      Revision history:
        V2.0 (March, 2005):
          New authentication context class schema for SAML V2.0.
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclarationBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection" minOccurs="0"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="GoverningAgreements" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthnMethodBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorBaseType">
        <xs:sequence>
          <xs:element ref="RestrictedPassword"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorTransportProtocolType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorTransportProtocolType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="SSL"/>
            <xs:element ref="MobileNetworkRadioEncryption"/>
            <xs:element ref="MobileNetworkEndToEndEncryption"/>
```

```
            <xs:element ref="WTLS"/>
            <xs:element ref="IPSec"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:redefine>

</xs:schema>
```

주의 : SSL의 사용은 부록 I에 제시된다.

4.4.10. PreviousSession

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession

사용자가 인증 기관에서 지원되는 어떠한 인증 문맥을 사용하여 과거 어느 시점에 인증 기관에서 인증되었을 때, 이 클래스가 적용 가능하다. 따라서, 인증 기관에서 의지하는 기관에게 보장하는 후속 인증 이벤트가 사용자의 현재 자원 접근 요청과 시각적으로(in time) 많이 분리될 수 있다.

이전에 인증된 세션에 대한 문맥은 이 문맥 클래스에 명시적으로 포함되지 않는다. 이것은 사용자가 현 세션 중에 인증된 것이 아니고 따라서 사용자가 과거 세션에서 인증하는데 사용한 메커니즘이 현재 자원 접근을 허가할지 여부에 대한 판단의 일부로써 사용되어서는 안되기 때문이다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
        Document identifier: saml-schema-authn-context-session-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>
```

```
    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="PreviousSession"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

4.4.11. Public key – X.509

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:X509

이 인증 문맥은 사용자가 전자서명을 통해 인증되었으며, 이 곳에서 공개키가 X.509 공개키 기반구조의 일부로써 검증되었음을 가리킨다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:X509
        Document identifier: saml-schema-authn-context-x509-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
```

```
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="DigSig"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PublicKeyType">
      <xs:complexContent>
        <xs:restriction base="PublicKeyType">
          <xs:attribute name="keyValidation" type="xs:anyURI"
                fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

4.4.12. Public key – PGP

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:PGP

이 인증 문맥은 사용자가 전자서명을 통해 인증되었으며, 이 곳에서 공개키가 PGP 공개키 기반구조의 일부로써 검증되었음을 가리킨다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:PGP
```

```
      Document identifier: saml-schema-authn-context-pgp-2.0
      Location: http://docs.oasis-open.org/security/saml/v2.0/
      Revision history:
        V2.0 (March, 2005):
          New authentication context class schema for SAML V2.0.
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclarationBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection" minOccurs="0"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="GoverningAgreements" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthnMethodBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="PrincipalAuthenticationMechanism"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrincipalAuthenticationMechanismType">
    <xs:complexContent>
      <xs:restriction base="PrincipalAuthenticationMechanismType">
        <xs:sequence>
          <xs:element ref="RestrictedPassword"/>
        </xs:sequence>
        <xs:attribute name="preauth" type="xs:integer" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorBaseType">
        <xs:sequence>
          <xs:element ref="DigSig"/>
        </xs:sequence>
      </xs:restriction>
```

```
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PublicKeyType">
      <xs:complexContent>
        <xs:restriction base="PublicKeyType">
          <xs:attribute name="keyValidation"
                fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

4.4.13. Public key – SPKI

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI

이 인증 문맥은 사용자가 전자서명을 통해 인증되었으며, 이 곳에서 공개키가 SPKI 기반구조의 일부로써 검증되었음을 가리킨다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI
        Document identifier: saml-schema-authn-context-spki-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
```

```
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="DigSig"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PublicKeyType">
      <xs:complexContent>
        <xs:restriction base="PublicKeyType">
          <xs:attribute name="keyValidation"
                  fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>
```

```
</xs:schema>
```

4.4.14. Public key - XML digital signature

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig

이 인증 문맥은 W3C XML 전자서명에서 기술된 처리 규칙을 따르는 전자서명을 통해 사용자가 인증되었다는 것을 가리킨다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig
        Document identifier: saml-schema-authn-context-xmldsig-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
```

```
            <xs:sequence>
              <xs:element ref="PrincipalAuthenticationMechanism"/>
              <xs:element ref="Authenticator"/>
              <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
              <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
          </xs:restriction>
        </xs:complexContent>
      </xs:complexType>

      <xs:complexType name="PrincipalAuthenticationMechanismType">
        <xs:complexContent>
          <xs:restriction base="PrincipalAuthenticationMechanismType">
            <xs:sequence>
              <xs:element ref="RestrictedPassword"/>
            </xs:sequence>
            <xs:attribute name="preauth" type="xs:integer" use="optional"/>
          </xs:restriction>
        </xs:complexContent>
      </xs:complexType>

      <xs:complexType name="AuthenticatorBaseType">
        <xs:complexContent>
          <xs:restriction base="AuthenticatorBaseType">
            <xs:sequence>
              <xs:element ref="DigSig"/>
            </xs:sequence>
          </xs:restriction>
        </xs:complexContent>
      </xs:complexType>

      <xs:complexType name="PublicKeyType">
        <xs:complexContent>
          <xs:restriction base="PublicKeyType">
            <xs:attribute name="keyValidation" type="xs:anyURI" fixed="urn:ietf:rfc:3075"/>
          </xs:restriction>
        </xs:complexContent>
      </xs:complexType>

    </xs:redefine>

  </xs:schema>
```

4.4.15. Smartcard

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard

이 인증 문맥은 사용자가 스마트카드를 사용하여 사용자가 인증 기관에 인증되었다는 것을 가리킨다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
        Document identifier: saml-schema-authn-context-smartcard-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
```

```
            <xs:element ref="Smartcard"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

4.4.16. SmartcardPKI

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI

사용자가 봉인된(enclosed) 개인키를 가진 스마트카드와 PIN을 사용하는 두 가지 요인 인증 메커니즘을 통해 인증 기관에 인증될 때, 이 인증 문맥이 적용 가능하다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI
        Document identifier: saml-schema-authn-context-smartcardpki-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
```

```
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthnMethodBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="PrincipalAuthenticationMechanism"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="TechnicalProtectionBaseType">
    <xs:complexContent>
      <xs:restriction base="TechnicalProtectionBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="PrivateKeyProtection"/>
          </xs:choice>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrincipalAuthenticationMechanismType">
    <xs:complexContent>
      <xs:restriction base="PrincipalAuthenticationMechanismType">
        <xs:sequence>
          <xs:element ref="Smartcard"/>
          <xs:element ref="ActivationPin"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="DigSig"/>
            <xs:element ref="AsymmetricDecryption"/>
            <xs:element ref="AsymmetricKeyAgreement"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
```

```
    <xs:complexType name="PrivateKeyProtectionType">
      <xs:complexContent>
        <xs:restriction base="PrivateKeyProtectionType">
          <xs:sequence>
            <xs:element ref="KeyActivation"/>
            <xs:element ref="KeyStorage"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyActivationType">
      <xs:complexContent>
        <xs:restriction base="KeyActivationType">
          <xs:sequence>
            <xs:element ref="ActivationPin"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyStorageType">
      <xs:complexContent>
        <xs:restriction base="KeyStorageType">
          <xs:attribute name="medium" use="required">
            <xs:simpleType>
              <xs:restriction base="mediumType">
                <xs:enumeration value="smartcard"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

4.4.17. SoftwarePKI

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI

사용자가 소프트웨어에 저장된 X.509 인증서를 이용하여 인증 기관에 인증될 때, 이 인증 문맥이 적용 가능하다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
```

```
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
finalDefault="extension"
blockDefault="substitution"
version="2.0">

<xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

  <xs:annotation>
    <xs:documentation>
      Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI
      Document identifier: saml-schema-authn-context-softwarepki-2.0
      Location: http://docs.oasis-open.org/security/saml/v2.0/
      Revision history:
        V2.0 (March, 2005):
          New authentication context class schema for SAML V2.0.
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclarationBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="GoverningAgreements" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthnMethodBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="PrincipalAuthenticationMechanism"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="TechnicalProtectionBaseType">
    <xs:complexContent>
      <xs:restriction base="TechnicalProtectionBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="PrivateKeyProtection"/>
          </xs:choice>
```

```
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrincipalAuthenticationMechanismType">
    <xs:complexContent>
      <xs:restriction base="PrincipalAuthenticationMechanismType">
        <xs:sequence>
          <xs:element ref="ActivationPin"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="DigSig"/>
            <xs:element ref="AsymmetricDecryption"/>
            <xs:element ref="AsymmetricKeyAgreement"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrivateKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="PrivateKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyActivation"/>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="KeyActivationType">
    <xs:complexContent>
      <xs:restriction base="KeyActivationType">
        <xs:sequence>
          <xs:element ref="ActivationPin"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="KeyStorageType">
```

```
        <xs:complexContent>
          <xs:restriction base="KeyStorageType">
            <xs:attribute name="medium" use="required">
              <xs:simpleType>
                <xs:restriction base="mediumType">
                  <xs:enumeration value="memory"/>
                </xs:restriction>
              </xs:simpleType>
            </xs:attribute>
          </xs:restriction>
        </xs:complexContent>
      </xs:complexType>

    </xs:redefine>
</xs:schema>
```

4.4.18. Telephony

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony

이 클래스는 사용자가 ADSL과 같은 전화 통신 프로토콜을 통해 전송되는 고정-회선 (fixed-line) 전화 번호를 통해 인증되었다는 것을 가리킬 때 사용된다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony
        Document identifier: saml-schema-authn-context-telephony-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
```

```
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="SubscriberLineNumber"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="PSTN"/>
              <xs:element ref="ISDN"/>
              <xs:element ref="ADSL"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

4.4.19. Telephony (nomadic)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony

이 클래스는 사용자가 전화 카드를 사용하여 로밍(roaming)을 하고 있고 라인 번호, 사용자 접미사(user suffix) 및 패스워드 요소를 통해 인증한다는 것을 가리킨다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace=
        "urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony
        Document identifier: saml-schema-authn-context-nomad-telephony-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"/>
```

```
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="Password"/>
            <xs:element ref="SubscriberLineNumber"/>
            <xs:element ref="UserSuffix"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="PSTN"/>
              <xs:element ref="ISDN"/>
              <xs:element ref="ADSL"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

4.4.20. Telephony (personalized)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalTelephony

이 클래스는 사용자가 ADSL과 같은 전화 통신 프로토콜을 통해 전송되는 고정-회선 전화 번호와 사용자 접미사를 통해 인증되었다는 것을 가리키는데 사용된다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace=
        "urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony"
  finalDefault="extension"
```

```
blockDefault="substitution"
version="2.0">

<xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

  <xs:annotation>
    <xs:documentation>
      Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony
      Document identifier: saml-schema-authn-context-personal-telephony-2.0
      Location: http://docs.oasis-open.org/security/saml/v2.0/
      Revision history:
        V2.0 (March, 2005):
          New authentication context class schema for SAML V2.0.
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclarationBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection" minOccurs="0"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="GoverningAgreements" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthnMethodBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorBaseType">
        <xs:sequence>
          <xs:element ref="SubscriberLineNumber"/>
          <xs:element ref="UserSuffix"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
```

```
    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="PSTN"/>
              <xs:element ref="ISDN"/>
              <xs:element ref="ADSL"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

4.4.21. Telephony (authenticated)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony

이것은 사용자가 회신 번호, 사용자 접미사와 패스워드 요소를 통해 인증되었다는 것을 가리킨다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace=
          "urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony
        Document identifier: saml-schema-authn-context-auth-telephony-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>
```

```
<xs:complexType name="AuthnContextDeclarationBaseType">
  <xs:complexContent>
    <xs:restriction base="AuthnContextDeclarationBaseType">
      <xs:sequence>
        <xs:element ref="Identification" minOccurs="0"/>
        <xs:element ref="TechnicalProtection" minOccurs="0"/>
        <xs:element ref="OperationalProtection" minOccurs="0"/>
        <xs:element ref="AuthnMethod"/>
        <xs:element ref="GoverningAgreements" minOccurs="0"/>
        <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:attribute name="ID" type="xs:ID" use="optional"/>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="AuthnMethodBaseType">
  <xs:complexContent>
    <xs:restriction base="AuthnMethodBaseType">
      <xs:sequence>
        <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
        <xs:element ref="Authenticator"/>
        <xs:element ref="AuthenticatorTransportProtocol"/>
        <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="AuthenticatorBaseType">
  <xs:complexContent>
    <xs:restriction base="AuthenticatorBaseType">
      <xs:sequence>
        <xs:element ref="Password"/>
        <xs:element ref="SubscriberLineNumber"/>
        <xs:element ref="UserSuffix"/>
      </xs:sequence>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="AuthenticatorTransportProtocolType">
  <xs:complexContent>
    <xs:restriction base="AuthenticatorTransportProtocolType">
      <xs:sequence>
        <xs:choice>
          <xs:element ref="PSTN"/>
          <xs:element ref="ISDN"/>
          <xs:element ref="ADSL"/>
        </xs:choice>
        <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:restriction>
  </xs:complexContent>
```

```
    </xs:complexType>
  </xs:redefine>

</xs:schema>
```

4.4.22. Secure remote password

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword

인증이 IETF RFC 2945에 기술된 안전한 원격 패스워드(remote password) 방식으로 수행되었을 때, 이 클래스가 적용 가능하다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace
        ="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword
        Document identifier: saml-schema-authn-context-srp-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
```

```
    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="SharedSecretChallengeResponse"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SharedSecretChallengeResponseType">
      <xs:complexContent>
        <xs:restriction base="SharedSecretChallengeResponseType">
          <xs:attribute name="method" type="xs:anyURI" fixed="urn:ietf:rfc:2945"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

4.4.23. TLS certificate-based client authentication

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient

이 클래스는 사용자가 TLS로 보호된 클라이언트 인증서를 통해 인증되었다는 것을 가리킨다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
        Document identifier: saml-schema-authn-context-sslcert-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
```

```
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="DigSig"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PublicKeyType">
      <xs:complexContent>
        <xs:restriction base="PublicKeyType">
          <xs:attribute name="keyValidation" type="xs:anyURI"
                fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="SSL"/>
              <xs:element ref="WTLS"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

주의 : SSL의 사용은 부록 I에 제시된다.

4.4.24. TimeSyncToken

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken

사용자가 시각 동기화 토큰(time synchronization token)을 통해 인증될 때, 이 클래스가 적용 가능하다.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken
        Document identifier: saml-schema-authn-context-timesync-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
```

```
            <xs:element ref="Token"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="TokenType">
      <xs:complexContent>
        <xs:restriction base="TokenType">
          <xs:sequence>
            <xs:element ref="TimeSyncToken"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="TimeSyncTokenType">
      <xs:complexContent>
        <xs:restriction base="TimeSyncTokenType">
          <xs:attribute name="DeviceType" use="required">
            <xs:simpleType>
              <xs:restriction base="DeviceTypeType">
                <xs:enumeration value="hardware"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>

          <xs:attribute name="SeedLength" use="required">
            <xs:simpleType>
              <xs:restriction base="xs:integer">
                <xs:minInclusive value="64"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>

          <xs:attribute name="DeviceInHand" use="required">
            <xs:simpleType>
              <xs:restriction base="booleanType">
                <xs:enumeration value="true"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

4.4.25. Unspecified

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:Unspecified

이 클래스는 인증이 명기되지 않은 방식으로 수행되었다는 것을 가리킨다.

부록 I. SSL의 사용

일부 SAML 구현은 SSL 3.0의 사용을 추가로 지원하거나 또는 TLS 1.0의 대안으로써 SSL을 지원할 수 있다. SSL 3.0을 사용하는 구현들은 해당 구현물의 전체적인 보안성이 TLS의 암호(cipher)들에 놓여진 제약들과 일치한다는 것을 보장해야 한다. 예를 들어, 암호 슈트(suite) TLS_RSA_WITH_3DES_EDE_CBC_SHA를 사용하는 것을 요구하는 것은 암호 슈트 SSL_RSA_WITH_3DES_EDE_CBC_SHA의 사용으로 변형된다. FIPS SSL이 가능한 구현들은 SSL SSL_RSA_WITH_3DES_EDE_CBC_SHA 암호 슈트에 대응되는 FIPS 암호 슈트를 사용한다.

TLS_RSA_WITH_3DES_EDE_CBC_SHA 암호 슈트를 지원하는 웹 SSO SAML 프로파일의 TLS 구현들은 SSL_RSA_WITH_3DES_EDE_CBC_SHA 암호 슈트를 사용할 것이다.

II. 인증 문맥 타입들 XML 스키마

이 부록은 개별적으로 일반화된 선언의 검증을 위해 사용되는 완전한 인증 문맥 타입 XML 스키마와 인증 문맥 XML 스키마 자체를 나열한다. 이 스키마는 목적(target) 네임스페이스를 가지고 있지 않으며, 본문에서 정의된 각각의 스키마에 포함된다.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified"
  version="2.0">

  <xs:annotation>
    <xs:documentation>
      Document identifier: saml-schema-authn-context-types-2.0
      Location: http://docs.oasis-open.org/security/saml/v2.0/
      Revision history:
           V2.0 (March, 2005):
           New core authentication context schema types for SAML V2.0.
    </xs:documentation>
  </xs:annotation>

  <xs:element name="AuthenticationContextDeclaration"
        type="AuthnContextDeclarationBaseType">
    <xs:annotation>
      <xs:documentation>
        A particular assertion on an identity
        provider's part with respect to the authentication
        context associated with an authentication assertion.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Identification" type="IdentificationType">
    <xs:annotation>
      <xs:documentation>
        Refers to those characteristics that describe the
        processes and mechanisms
        the Authentication Authority uses to initially create
        an association between a Principal
        and the identity (or name) by which the Principal will
        be known
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="PhysicalVerification">
    <xs:annotation>
      <xs:documentation>
        This element indicates that identification has been
```

```
        performed in a physical
        face-to-face meeting with the principal and not in an
        online manner.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:attribute name="credentialLevel">
        <xs:simpleType>
          <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="primary"/>
            <xs:enumeration value="secondary"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:complexType>
  </xs:element>

  <xs:element name="WrittenConsent" type="ExtensionOnlyType"/>

  <xs:element name="TechnicalProtection" type="TechnicalProtectionBaseType">
    <xs:annotation>
      <xs:documentation>
        Refers to those characterstics that describe how the
        'secret' (the knowledge or possession
        of which allows the Principal to authenticate to the
        Authentication Authority) is kept secure
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="SecretKeyProtection" type="SecretKeyProtectionType">
    <xs:annotation>
      <xs:documentation>
        This element indicates the types and strengths of
        facilities
        of a UA used to protect a shared secret key from
        unauthorized access and/or use.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="PrivateKeyProtection" type="PrivateKeyProtectionType">
    <xs:annotation>
      <xs:documentation>
        This element indicates the types and strengths of
        facilities
        of a UA used to protect a private key from
        unauthorized access and/or use.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="KeyActivation" type="KeyActivationType">
    <xs:annotation>
      <xs:documentation>The actions that must be performed
```

```
        before the private key can be used. </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="KeySharing" type="KeySharingType">
    <xs:annotation>
        <xs:documentation>Whether or not the private key is shared
            with the certificate authority.</xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="KeyStorage" type="KeyStorageType">
    <xs:annotation>
        <xs:documentation>
            In which medium is the key stored.
            memory - the key is stored in memory.
            smartcard - the key is stored in a smartcard.
            token - the key is stored in a hardware token.
            MobileDevice - the key is stored in a mobile device.
            MobileAuthCard - the key is stored in a mobile
            authentication card.
        </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="SubscriberLineNumber" type="ExtensionOnlyType"/>
<xs:element name="UserSuffix" type="ExtensionOnlyType"/>

<xs:element name="Password" type="PasswordType">
    <xs:annotation>
        <xs:documentation>
            This element indicates that a password (or passphrase)
            has been used to
            authenticate the Principal to a remote system.
        </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="ActivationPin" type="ActivationPinType">
    <xs:annotation>
        <xs:documentation>
            This element indicates that a Pin (Personal
            Identification Number) has been used to authenticate the Principal to
            some local system in order to activate a key.
        </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="Token" type="TokenType">
    <xs:annotation>
        <xs:documentation>
            This element indicates that a hardware or software
            token is used
            as a method of identifying the Principal.
        </xs:documentation>
```

```
    </xs:annotation>
  </xs:element>

  <xs:element name="TimeSyncToken" type="TimeSyncTokenType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that a time synchronization
        token is used to identify the Principal. hardware -
        the time synchonization
        token has been implemented in hardware. software - the
        time synchronization
        token has been implemented in software. SeedLength -
        the length, in bits, of the
        random seed used in the time synchronization token.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Smartcard" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that a smartcard is used to
        identity the Principal.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Length" type="LengthType">
    <xs:annotation>
      <xs:documentation>
        This element indicates the minimum and/or maximum
        ASCII length of the password which is enforced (by the UA or the
        IdP). In other words, this is the minimum and/or maximum number of
        ASCII characters required to represent a valid password.
        min - the minimum number of ASCII characters required
        in a valid password, as enforced by the UA or the IdP.
        max - the maximum number of ASCII characters required
        in a valid password, as enforced by the UA or the IdP.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="ActivationLimit" type="ActivationLimitType">
    <xs:annotation>
      <xs:documentation>
        This element indicates the length of time for which an
        PIN-based authentication is valid.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Generation">
    <xs:annotation>
      <xs:documentation>
        Indicates whether the password was chosen by the
```

```
        Principal or auto-supplied by the Authentication Authority.
        principalchosen - the Principal is allowed to choose
        the value of the password. This is true even if
        the initial password is chosen at random by the UA or
        the IdP and the Principal is then free to change
        the password.
        automatic - the password is chosen by the UA or the
        IdP to be cryptographically strong in some sense,
        or to satisfy certain password rules, and that the
        Principal is not free to change it or to choose a new password.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType>
      <xs:attribute name="mechanism" use="required">
        <xs:simpleType>
          <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="principalchosen"/>
            <xs:enumeration value="automatic"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:complexType>
  </xs:element>

  <xs:element name="AuthnMethod" type="AuthnMethodBaseType">
    <xs:annotation>
      <xs:documentation>
        Refers to those characteristics that define the
        mechanisms by which the Principal authenticates to the Authentication
        Authority.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="PrincipalAuthenticationMechanism"
        type="PrincipalAuthenticationMechanismType">
    <xs:annotation>
      <xs:documentation>
        The method that a Principal employs to perform
        authentication to local system components.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Authenticator" type="AuthenticatorBaseType">
    <xs:annotation>
      <xs:documentation>
        The method applied to validate a principal's
        authentication across a network
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="ComplexAuthenticator" type="ComplexAuthenticatorType">
```

```
    <xs:annotation>
      <xs:documentation>
        Supports Authenticators with nested combinations of
        additional complexity.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="PreviousSession" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        Indicates that the Principal has been strongly
        authenticated in a previous session during which the IdP has set a
        cookie in the UA. During the present session the Principal has only
        been authenticated by the UA returning the cookie to the IdP.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="ResumeSession" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        Rather like PreviousSession but using stronger
        security. A secret that was established in a previous session with
        the Authentication Authority has been cached by the local system and
        is now re-used (e.g. a Master Secret is used to derive new session
        keys in TLS, WTLS).
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="ZeroKnowledge" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Principal has been
        authenticated by a zero knowledge technique as specified in ISO/IEC
        9798-5.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="SharedSecretChallengeResponse"
        type="SharedSecretChallengeResponseType"/>

  <xs:complexType name="SharedSecretChallengeResponseType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Principal has been
        authenticated by a challenge-response protocol utilizing shared secret
        keys and symmetric cryptography.
      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
```

```
    <xs:attribute name="method" type="xs:anyURI" use="optional"/>
  </xs:complexType>

  <xs:element name="DigSig" type="PublicKeyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Principal has been
        authenticated by a mechanism which involves the Principal computing a
        digital signature over at least challenge data provided by the IdP.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="AsymmetricDecryption" type="PublicKeyType">
    <xs:annotation>
      <xs:documentation>
        The local system has a private key but it is used
        in decryption mode, rather than signature mode. For example, the
        Authentication Authority generates a secret and encrypts it using the
        local system's public key: the local system then proves it has
        decrypted the secret.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="AsymmetricKeyAgreement" type="PublicKeyType">
    <xs:annotation>
      <xs:documentation>
        The local system has a private key and uses it for
        shared secret key agreement with the Authentication Authority (e.g.
        via Diffie Helman).
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:complexType name="PublicKeyType">
    <xs:sequence>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="keyValidation" use="optional"/>
  </xs:complexType>

  <xs:element name="IPAddress" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Principal has been
        authenticated through connection from a particular IP address.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="SharedSecretDynamicPlaintext" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        The local system and Authentication Authority
```

```
        share a secret key. The local system uses this to encrypt a
        randomised string to pass to the Authentication Authority.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="AuthenticatorTransportProtocol"
        type="AuthenticatorTransportProtocolType">
    <xs:annotation>
      <xs:documentation>
        The protocol across which Authenticator information is
        transferred to an Authentication Authority verifier.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="HTTP" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Authenticator has been
        transmitted using bare HTTP utilizing no additional security
        protocols.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="IPSec" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Authenticator has been
        transmitted using a transport mechanism protected by an IPSEC session.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="WTLS" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Authenticator has been
        transmitted using a transport mechanism protected by a WTLS session.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="MobileNetworkNoEncryption" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Authenticator has been
        transmitted solely across a mobile network using no additional
        security mechanism.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="MobileNetworkRadioEncryption" type="ExtensionOnlyType"/>
```

```
<xs:element name="MobileNetworkEndToEndEncryption" type="ExtensionOnlyType"/>

<xs:element name="SSL" type="ExtensionOnlyType">
  <xs:annotation>
    <xs:documentation>
      This element indicates that the Authenticator has been
      transmitted using a transport mechanism protected by an SSL or TLS
      session.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="PSTN" type="ExtensionOnlyType"/>
<xs:element name="ISDN" type="ExtensionOnlyType"/>
<xs:element name="ADSL" type="ExtensionOnlyType"/>

<xs:element name="OperationalProtection" type="OperationalProtectionType">
  <xs:annotation>
    <xs:documentation>
      Refers to those characteristics that describe
      procedural security controls employed by the Authentication Authority.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="SecurityAudit" type="SecurityAuditType"/>
<xs:element name="SwitchAudit" type="ExtensionOnlyType"/>
<xs:element name="DeactivationCallCenter" type="ExtensionOnlyType"/>

<xs:element name="GoverningAgreements" type="GoverningAgreementsType">
  <xs:annotation>
    <xs:documentation>
      Provides a mechanism for linking to external (likely
      human readable) documents in which additional business agreements,
      (e.g. liability constraints, obligations, etc) can be placed.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="GoverningAgreementRef" type="GoverningAgreementRefType"/>

<xs:simpleType name="nymType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="anonymity"/>
    <xs:enumeration value="verinymity"/>
    <xs:enumeration value="pseudonymity"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="AuthnContextDeclarationBaseType">
  <xs:sequence>
    <xs:element ref="Identification" minOccurs="0"/>
    <xs:element ref="TechnicalProtection" minOccurs="0"/>
    <xs:element ref="OperationalProtection" minOccurs="0"/>
    <xs:element ref="AuthnMethod" minOccurs="0"/>
```

```
      <xs:element ref="GoverningAgreements" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="ID" type="xs:ID" use="optional"/>
  </xs:complexType>

  <xs:complexType name="IdentificationType">
    <xs:sequence>
      <xs:element ref="PhysicalVerification" minOccurs="0"/>
      <xs:element ref="WrittenConsent" minOccurs="0"/>
      <xs:element ref="GoverningAgreements" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="nym" type="nymType">
      <xs:annotation>
        <xs:documentation>
          This attribute indicates whether or not the
          Identification mechanisms allow the actions of the Principal to be
          linked to an actual end user.
        </xs:documentation>
      </xs:annotation>
    </xs:attribute>
  </xs:complexType>

  <xs:complexType name="TechnicalProtectionBaseType">
    <xs:sequence>
      <xs:choice minOccurs="0">
        <xs:element ref="PrivateKeyProtection"/>
        <xs:element ref="SecretKeyProtection"/>
      </xs:choice>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="OperationalProtectionType">
    <xs:sequence>
      <xs:element ref="SecurityAudit" minOccurs="0"/>
      <xs:element ref="DeactivationCallCenter" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="AuthnMethodBaseType">
    <xs:sequence>
      <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
      <xs:element ref="Authenticator" minOccurs="0"/>
      <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="GoverningAgreementsType">
    <xs:sequence>
      <xs:element ref="GoverningAgreementRef" maxOccurs="unbounded"/>
    </xs:sequence>
```

```
</xs:complexType>

<xs:complexType name="GoverningAgreementRefType">
  <xs:attribute name="governingAgreementRef" type="xs:anyURI" use="required"/>
</xs:complexType>

<xs:complexType name="PrincipalAuthenticationMechanismType">
  <xs:sequence>
    <xs:element ref="Password" minOccurs="0"/>
    <xs:element ref="RestrictedPassword" minOccurs="0"/>
    <xs:element ref="Token" minOccurs="0"/>
    <xs:element ref="Smartcard" minOccurs="0"/>
    <xs:element ref="ActivationPin" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="preauth" type="xs:integer" use="optional"/>
</xs:complexType>

<xs:group name="AuthenticatorChoiceGroup">
  <xs:choice>
    <xs:element ref="PreviousSession"/>
    <xs:element ref="ResumeSession"/>
    <xs:element ref="DigSig"/>
    <xs:element ref="Password"/>
    <xs:element ref="RestrictedPassword"/>
    <xs:element ref="ZeroKnowledge"/>
    <xs:element ref="SharedSecretChallengeResponse"/>
    <xs:element ref="SharedSecretDynamicPlaintext"/>
    <xs:element ref="IPAddress"/>
    <xs:element ref="AsymmetricDecryption"/>
    <xs:element ref="AsymmetricKeyAgreement"/>
    <xs:element ref="SubscriberLineNumber"/>
    <xs:element ref="UserSuffix"/>
    <xs:element ref="ComplexAuthenticator"/>
  </xs:choice>
</xs:group>

<xs:group name="AuthenticatorSequenceGroup">
  <xs:sequence>
    <xs:element ref="PreviousSession" minOccurs="0"/>
    <xs:element ref="ResumeSession" minOccurs="0"/>
    <xs:element ref="DigSig" minOccurs="0"/>
    <xs:element ref="Password" minOccurs="0"/>
    <xs:element ref="RestrictedPassword" minOccurs="0"/>
    <xs:element ref="ZeroKnowledge" minOccurs="0"/>
    <xs:element ref="SharedSecretChallengeResponse" minOccurs="0"/>
    <xs:element ref="SharedSecretDynamicPlaintext" minOccurs="0"/>
    <xs:element ref="IPAddress" minOccurs="0"/>
    <xs:element ref="AsymmetricDecryption" minOccurs="0"/>
    <xs:element ref="AsymmetricKeyAgreement" minOccurs="0"/>
    <xs:element ref="SubscriberLineNumber" minOccurs="0"/>
    <xs:element ref="UserSuffix" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:group>
```

```
<xs:complexType name="AuthenticatorBaseType">
  <xs:sequence>
    <xs:group ref="AuthenticatorChoiceGroup"/>
    <xs:group ref="AuthenticatorSequenceGroup"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ComplexAuthenticatorType">
  <xs:sequence>
    <xs:group ref="AuthenticatorChoiceGroup"/>
    <xs:group ref="AuthenticatorSequenceGroup"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="AuthenticatorTransportProtocolType">
  <xs:sequence>
    <xs:choice minOccurs="0">
      <xs:element ref="HTTP"/>
      <xs:element ref="SSL"/>
      <xs:element ref="MobileNetworkNoEncryption"/>
      <xs:element ref="MobileNetworkRadioEncryption"/>
      <xs:element ref="MobileNetworkEndToEndEncryption"/>
      <xs:element ref="WTLS"/>
      <xs:element ref="IPSec"/>
      <xs:element ref="PSTN"/>
      <xs:element ref="ISDN"/>
      <xs:element ref="ADSL"/>
    </xs:choice>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="KeyActivationType">
  <xs:sequence>
    <xs:element ref="ActivationPin" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="KeySharingType">
  <xs:attribute name="sharing" type="xs:boolean" use="required"/>
</xs:complexType>

<xs:complexType name="PrivateKeyProtectionType">
  <xs:sequence>
    <xs:element ref="KeyActivation" minOccurs="0"/>
    <xs:element ref="KeyStorage" minOccurs="0"/>
    <xs:element ref="KeySharing" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="PasswordType">
  <xs:sequence>
```

```
      <xs:element ref="Length" minOccurs="0"/>
      <xs:element ref="Alphabet" minOccurs="0"/>
      <xs:element ref="Generation" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="ExternalVerification" type="xs:anyURI" use="optional"/>
  </xs:complexType>

  <xs:element name="RestrictedPassword" type="RestrictedPasswordType"/>

  <xs:complexType name="RestrictedPasswordType">
    <xs:complexContent>
      <xs:restriction base="PasswordType">
        <xs:sequence>
          <xs:element name="Length" type="RestrictedLengthType" minOccurs="1"/>
          <xs:element ref="Generation" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ExternalVerification" type="xs:anyURI" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="RestrictedLengthType">
    <xs:complexContent>
      <xs:restriction base="LengthType">
        <xs:attribute name="min" use="required">
          <xs:simpleType>
            <xs:restriction base="xs:integer">
              <xs:minInclusive value="3"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="max" type="xs:integer" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="ActivationPinType">
    <xs:sequence>
      <xs:element ref="Length" minOccurs="0"/>
      <xs:element ref="Alphabet" minOccurs="0"/>
      <xs:element ref="Generation" minOccurs="0"/>
      <xs:element ref="ActivationLimit" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="Alphabet" type="AlphabetType"/>
  <xs:complexType name="AlphabetType">
    <xs:attribute name="requiredChars" type="xs:string" use="required"/>
    <xs:attribute name="excludedChars" type="xs:string" use="optional"/>
    <xs:attribute name="case" type="xs:string" use="optional"/>
  </xs:complexType>
```

```
<xs:complexType name="TokenType">
  <xs:sequence>
    <xs:element ref="TimeSyncToken"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:simpleType name="DeviceTypeType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="hardware"/>
    <xs:enumeration value="software"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="booleanType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="true"/>
    <xs:enumeration value="false"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="TimeSyncTokenType">
  <xs:attribute name="DeviceType" type="DeviceTypeType" use="required"/>
  <xs:attribute name="SeedLength" type="xs:integer" use="required"/>
  <xs:attribute name="DeviceInHand" type="booleanType" use="required"/>
</xs:complexType>

<xs:complexType name="ActivationLimitType">
  <xs:choice>
    <xs:element ref="ActivationLimitDuration"/>
    <xs:element ref="ActivationLimitUsages"/>
    <xs:element ref="ActivationLimitSession"/>
  </xs:choice>
</xs:complexType>

<xs:element name="ActivationLimitDuration" type="ActivationLimitDurationType">
  <xs:annotation>
    <xs:documentation>
      This element indicates that the Key Activation Limit is
      defined as a specific duration of time.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="ActivationLimitUsages" type="ActivationLimitUsagesType">
  <xs:annotation>
    <xs:documentation>
      This element indicates that the Key Activation Limit is
      defined as a number of usages.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="ActivationLimitSession" type="ActivationLimitSessionType">
  <xs:annotation>
```

```
      <xs:documentation>
        This element indicates that the Key Activation Limit is
        the session.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:complexType name="ActivationLimitDurationType">
    <xs:attribute name="duration" type="xs:duration" use="required"/>
  </xs:complexType>

  <xs:complexType name="ActivationLimitUsagesType">
    <xs:attribute name="number" type="xs:integer" use="required"/>
  </xs:complexType>

  <xs:complexType name="ActivationLimitSessionType"/>

  <xs:complexType name="LengthType">
    <xs:attribute name="min" type="xs:integer" use="required"/>
    <xs:attribute name="max" type="xs:integer" use="optional"/>
  </xs:complexType>

  <xs:simpleType name="mediumType">
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="memory"/>
      <xs:enumeration value="smartcard"/>
      <xs:enumeration value="token"/>
      <xs:enumeration value="MobileDevice"/>
      <xs:enumeration value="MobileAuthCard"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="KeyStorageType">
    <xs:attribute name="medium" type="mediumType" use="required"/>
  </xs:complexType>

  <xs:complexType name="SecretKeyProtectionType">
    <xs:sequence>
      <xs:element ref="KeyActivation" minOccurs="0"/>
      <xs:element ref="KeyStorage" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="SecurityAuditType">
    <xs:sequence>
      <xs:element ref="SwitchAudit" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ExtensionOnlyType">
    <xs:sequence>
      <xs:element ref="Extension" minOccurs="0"   maxOccurs="unbounded"/>
    </xs:sequence>
```

```
  </xs:complexType>

  <xs:element name="Extension" type="ExtensionType"/>

  <xs:complexType name="ExtensionType">
    <xs:sequence>
      <xs:any namespace="##other" processContents="lax" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

</xs:schema>

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac"
  blockDefault="substitution"
  version="2.0">

  <xs:annotation>
    <xs:documentation>
      Document identifier: saml-schema-authn-context-2.0
      Location: http://docs.oasis-open.org/security/saml/v2.0/
      Revision history:
        V2.0 (March, 2005):
          New core authentication context schema for SAML V2.0.
          This is just an include of all types from the Àu99 ?hema
          referred to in the include statement below.
    </xs:documentation>
  </xs:annotation>

  <xs:include schemaLocation="saml-schema-authn-context-types-2.0.xsd"/>

</xs:schema>
```

주의 : SSL의 사용은 부록 I에 제시된다.

표준작성 공헌자

표준 번호 : TTAS.IT-X1141.5

이 표준의 제.개정 및 발간을 위해 아래와 같이 여러분들이 공헌하였습니다.

구분	성명	위원회 및 직위	연락처	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

SAML 2.0 인증문맥
(SAML 2.0 Authentication Context)

발행인 : 김원식
발행처 : 한국정보통신기술협회
463-824, 경기도 성남시 분당구 서현동 267-2
Tel : 031-724-0114, Fax : 031-724-0119
발행일 : 2007.12.