

American National Standard for Telecommunications

**ATIS Identity Management:
Requirements and Use Cases Standard**

Alliance for Telecommunications Industry Solutions

Approved March 1, 2011

American National Standards Institute, Inc.

Abstract

This standard provides Identity Management (IdM) example use cases and requirements for the Next Generation Network (NGN) and its interfaces. IdM functions and capabilities are used to increase confidence in identity information and support and enhance business and security applications including identity-based services. The requirements provided in this standard are intended for NGN (i.e., managed packet networks) as defined in ATIS-1000018, *NGN Architecture* [ATIS 1000018] and ITU-T Recommendation Y.2001 [ITU-T Y.2001].

The objectives and requirements in this standard are based on the IdM framework provided in ATIS-1000035, *NGN Identity Management Framework* [ATIS-1000035] and ITU-T Recommendation Y.2720 [ITU-T Y.2720] and an analysis of use case examples relevant to NGN. The example use cases are informative and are documented in the Appendices of this standard.

Foreword

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time it approved this document, PTSC, which is responsible for the development of this Standard, had the following members:

- M. Dolly, PTSC Chair (AT&T)
- V. Shaikh, PTSC Vice-Chair (Telcordia)
- V. Shaikh, Technical Editor (Telcordia)
- C. Underkoffler, ATIS Chief Editor

The Signalling, Architecture, and Control (SAC) Working Group, which was responsible for the development of this document, had the following members:

Table of Contents

1. Scope 1

2. Normative References 2

 2.1 ATIS References 2

 2.2 ITU-T References 2

3. Definitions 3

 3.1 Terms defined elsewhere 3

 3.2 Terms defined in this Standard 6

4. Abbreviations and acronyms 6

5. Conventions 8

6. IdM Overview 8

 6.1 General 8

 6.2 IdM Relationships 9

 6.3 Drivers and Motivations 12

 6.4 Multiple service provider and federated environment 13

 6.5 Identity Service Provider (IdSP) 13

 6.6 IdM in Context of NGN Architectures and Reference Models 14

 6.6.1 Relationship with NGN Functional Architecture 14

 6.6.2 External Interfaces and IdM Communications 16

 6.6.3 Transactional Models 16

7. IdM Objectives 16

8. IdM Requirements 17

 8.1 General Requirements 17

 8.2 Identity Lifecycle Management Requirements 18

 8.2.1 Enrollment and Issuance 18

 8.2.2 Maintenance and Updates 19

 8.2.3 Revocation 20

8.3	Identity Management OAM&P Functions	20
8.3.1	Data Model and Schema	20
8.3.2	Management of Identity Data	21
8.4	Signalling and Control Functions	21
8.4.1	Discovery of Identity Information	21
8.4.2	Identity Information Access Control	22
8.4.3	IdM Communications	22
8.4.4	Correlation and Binding	23
8.4.5	Authentication requirements	23
8.4.6	Authentication Assurance	24
8.4.7	Support of Services Requiring Priority Treatment	25
8.5	Identity Management Federated Identity Functions	26
8.6	User/Subscriber Functions and Protection of PII	27
8.7	Security	28
8.7.1	System and Data Access Control	28
8.7.2	System and Data Integrity	29
8.7.3	Data Confidentiality	29
8.7.5	Management Security	29
8.7.6	Security and Auditing Log	30
8.7.7	Protection Against Denial of Service (DoS) and Distributed DoS (DDoS) Attacks	30
8.7.8	Monitoring and Intrusion Detection	30
Appendix A – General IdM Use Cases		31
A.1	Introduction	31
A.2	Government	31
A.3	Business Enterprise	31
A.4	End User/Subscribers	32
Appendix B – IdM Use Cases for NGN Applications		33

B.1	Introduction	33
B.2	Basic Use Case Example	33
B.3	Use of Common IdM System to Support Multiple Application Services (e.g., Voice, Data, IPTV) within a Service Provider Network.....	35
B.3.1	Overview.....	35
B.3.2	Use Case Description.....	35
B.3.3	Implied Requirements	40
B.4	Single Sign-on/Single Sign-off to Multiple Application Services (e.g., Voice, Data and IPTV) within a Service Provider Network	40
B.4.1	Overview.....	40
B.4.2	Use Case Description.....	41
B.5	Correlation of Distributed Identity Information for Multi-factor Authentication Assurance	45
B.5.1	Overview.....	45
B.5.2	Use Case Example	45
B.6	Enforcement of User Control of Personally Identifiable Information Personally Identifiable Information (e.g., Preferences) Across Peer Network/Service Provider Domains	47
B.6.1	Overview.....	47
B.6.2	Use Case Description.....	47
B.7	Bridging/Mapping between Heterogeneous IdM Systems.....	50
B.7.1	Overview.....	50
B.7.2	Use Case Description.....	50
B.7.3	Implied Requirements	51
B.8	Support of Converged Services (e.g., Fixed and Mobile Access) within a Service Provider Network	51
B.8.1	Overview.....	51
B.8.2	Use Case Description.....	51
B.8.3	Implied Requirements	52

B.9	Example Use Case - User Authentication and Authorization of NGN Provider (Mutual Authentication and Authorization)	53
B.10	Example Use Case – Peer User Assertion (Non-cash Transactions)	54
B.11	IdM Use Case – Assurance of End User Device Identity and Integrity	55
B.11.1	Example Use Case – Assurance of User and Device Authentication	55
B.11.2	Example Use Case – Assurance of User Device Integrity	57
B.11.3	Example Use Case – Encryption of PII and Sensitive Files/Data	59
B.12	Real Time Verification Database	59
B.12.1	Overview.....	59
B.12.2	End User/Subscriber Perspective.....	60
B.12.3	Service Providers Perspective	60
B.12.3.1	<i>Database Structure and Contents</i>	61
B.12.3.2	<i>Database Security</i>	61
B.12.4	Implied Capabilities	62
B.12.5	Access Across Multiple Service/Network Providers	62
B.12.6	Example Use Cases	62
B.12.6.1	<i>IPTV and IP-based Services</i>	62
B.12.6.2	<i>Retail/Financial Applications</i>	63
Appendix C - Emergency Telecommunication Service (ETS) Related IdM Use Cases		65
C.1	Introduction	65
C.2	Authentication Assurance using device and user combination.....	65
C.3	Enhanced authentication of ETS users for next generation priority services (priority multimedia services).....	67
C.4	Authentication of called party and data communication sources.....	70
C.5	Trusted Identification and authentication of service providers in a multi-provider environment.....	73
C.6	Single Sign-On and Single Sign-Off.....	76
AppendixD - Mobile Related Use Cases.....		82
D.1	Introduction	82

D.2	Use Case Examples	82
Appendix E - Example IdM Transaction Models		86
E.1	Introduction	86
E.2	Examples of possible identity management transaction models	86
Appendix F - Example illustrative deployment scenario for IdM in NGN		89
F.1	Introduction	89
F.2	IdM Architecture Deployment.....	89
Appendix G -- Bibliography		92

Table of Figures

Figure 1 - IdM Relationships	10
Figure 2 - Figure 7-1 of [ITU-T Y.2012]	15
Figure B. 1- Basic Use Case Example	33
Figure B. 2 - Basic Use Case Example	36
Figure B. 3 - Multiple Application Services Use of Common IdM Infrastructure	37
Figure B. 4 - Single Sign-on	42
Figure B. 5 -Single Sign-off Service.....	44
Figure B. 6 - Correlation of Identity Information	46
Figure B. 7 - Anonymous User Identity	48
Figure B. 8 - Example Use Case: User Authentication and Authorization of NGN Provider	53
Figure B. 9 - Example Use Case: Peer User Assertion (Non-cash Transaction)	54
Figure B. 10 - Correlation of User and Device Authentication for Assurance	56
Figure B. 11 - Assurance of Device Integrity.....	58
Figure B. 12 - Example User Verification.....	60
Figure B. 13 - Example Use Case: User Verification for IPTV Transactions.....	63
Figure B. 14 - Example Use Case: User Verification for Retail/Financial Applications	64
Figure C. 1 - Combined user and device authentication	66
Figure C. 2 - Enhanced authentication for next generation priority services.....	68
Figure C. 3 - Biometric use case example.....	69
Figure C. 4 - Assertion of terminating user identity	71
Figure C. 5 - Assertion of text message source.....	73
Figure C. 6 - Validation of access service provider	74
Figure C. 7 - Validation of web service or content provider	76
Figure C. 8 - Single Sign-On.....	78
Figure C. 9 - Single Sign-off.....	80
Figure E. 1 - [ITU-T X.1250] – Basic query/response information exchange process	86

Figure E. 2 - [b-ITU-T X.1250] – An example of a three-party identity management model..... 87
Figure E. 3 - An example of a user-centric five-party identity management model..... 87
Figure F. 1 - Example IdM deployment in NGN 90

currently in preview, click buy full version

American National Standard for Telecommunications –

ATIS Identity Management: Requirements and Use Cases Standard

1. Scope

This standard provides Identity Management (IdM) objectives, requirements, guidelines, and example use cases for the Next Generation Network (NGN) and its interfaces. IdM functions and capabilities are used to increase confidence in identity information and support and enhance business and security applications including identity-based services.

The scope of this standard includes objectives, requirements, guidelines, and example uses cases addressing:

- Increasing confidence in the identity information of an NGN entity (e.g., user, group, user device, service provider, enterprise, federation, network element, and object).
- Secure management of the lifecycle (e.g., registration, validation, revocation) of identity information subject to user's specific and informed consent.
- IdM as an enabler of business (e.g., single sign-on and sign-off for multiple application services) and security applications (e.g., access controls), including identity-based services (e.g., authentication, assertions and federated identity).
- Secure discovery and exchange of information associated with an NGN entity's identity or identities subject to user's specific and informed consent. This includes information that may be located within an NGN and across different administrative domains or federations.
- Interworking/interoperability among the IdM systems and capabilities within a NGN provider domain (i.e., intra-network).
- Interworking/interoperability of the IdM systems and capabilities among different provider domains or federations subject to user's specific and informed consent where user information is concern (e.g., among NGN providers, web services providers, and content providers).
- Enforcement of applicable policy (e.g., protection of personally identifiable information) associated with an entity's identity or identity information.
- Security of IdM systems, functions, capabilities, data, and communications.

The objectives and requirements provided in this standard are intended for NGN (i.e., managed packet networks) as defined in [ATIS 1000018], *NGN Architecture*, and [ITU-T Y.2001], *General overview of NGN*.

The objectives and requirements in this standard are based on the IdM framework provided in [ATIS-1000035] and Recommendation [ITU-T Y.2720], and an analysis of use case examples documented in the Appendices of this standard.

Notes:

1. In this standard, the use of the term "Identity" relating to IdM does not indicate its absolute meaning. In particular, it does not constitute any positive validation of a person.
2. In this standard, a user can be a person, groups, companies, juridical entities, or any other entities which make use of NGN services.
3. In this standard, the term "NGN/Identity Service Provider (NGN/IdSP)" is used to indicate that it could be an NGN provider or third party that provides IdM services.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the edition indicated was valid. All standards are subject to revision, and the parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below.

2.1 ATIS References¹

[ATIS-1000018], ATIS-1000018, *NGN Architecture*

[ATIS-1000035], ATIS-1000035.2009, *NGN Identity Management Framework*

[ATIS-1000029], ATIS-1000029.2008, *NGN Security Requirements*

[ATIS-1000030], ATIS-1000030.2008, *Authentication and Authorization Requirements for Next generation Network*

[ATIS-1000010], ATIS-1000010.2006(R2011), *Support of Emergency Telecommunications Service in IP Networks*

2.2 ITU-T References²

[ITU-T Y.2720] ITU-T Recommendation Y.2720 (01/09), *NGN identity management framework*

[ITU-T Y.2702] ITU-T Recommendation Y.2702 (09/08), *Authentication and authorization requirements for NGN Release 1*

[ITU-T Y.2201] ITU-T Recommendation Y.2201 (09/09), *Requirements and capabilities for ITU-T NGN*

¹ This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < <https://www.atis.org/docstore/default.aspx> >

² This document is available from the International Telecommunications Union. < <http://www.itu.int/ITU-T/> >