ATIS-1000044.2011(S2021)

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

Table of Figures

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 References[1]

[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 References[2]

[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/ >