Recent NGN Security Standardization Trends in ITU-T

Takeo Hariu[†]*, Teruko Miyata, and Yoshihito Oshima*

Abstract

Standardization issues regarding the Next Generation Network (NGN) are being addressed by Study Group 13 (SG13) in ITU-T (International Telecommunication Union, Telecommunication Standardization Sector). Here, we present an overview of the recently completed Release 1, which deals with fundamental issues of security in the NGN. We also consider recent work on identity management, which has recently become a subject of enormous interest.

1. NGN security

Robust security is a fundamental attribute of the Next Generation Network (NGN) that will enable it to support safe, secure communications. Release 1 addresses a wide range of security-related issues focusing primarily on voice-over-Internet-protocol (VoIP) services.

Study Group 13 of ITU-T (International Telecommunication Union, Telecommunication Standardization Sector) [1] is charged with handling Question 15 (Q.15/13) related to standardization of NGN security. With the conventional networks, the number and variety of security breaches and incidents have continued to rise as networks have become an increasingly important public infrastructure. The need for operator authentication and maintenance of audit trails and logs has also become crucial for purposes of internal control. Against this backdrop, many representatives of carriers and vendors from around the world have participated in all the Q.15/13 sessions and contributed to lively deliberations on NGN security.

Security-related talks on the technologies to be used in the coming NGN have not been easy, and at this time, considerations on how to address wide-ranging issues and future extensibility are also important. For its part, NTT continues to play an active role in Q.15/13 deliberations by submitting proposals and other contributions and by pushing the talks forward to address broader issues without getting bogged down in controversies over individual schemes.

Security-related documents now under development by Q.15/13 are listed in **Table 1**. Here, we give summarize some of these key documents.

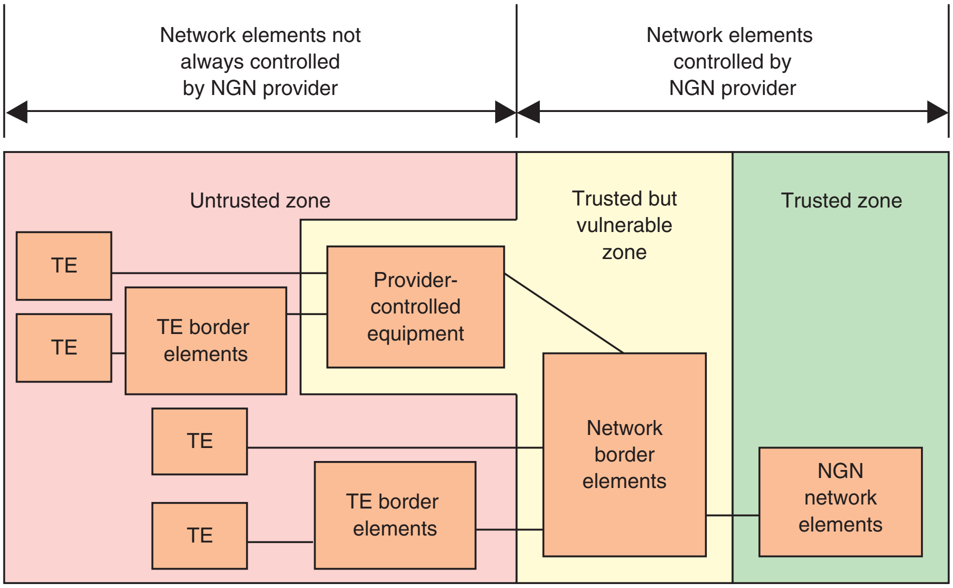
2. NGN Release 1: NGN security requirements

NGN Release 1, Recommendation Y.2701 detailing security requirements for the NGN, was completed in April 2007. Based on the idea that security requirements cannot be properly defined without awareness of the interface between devices, Y.2701 adopts a physical model. A security trust model based on the physical model defined in Y.2701 is shown in **Fig. 1**. The NGN is divided into three zones, and requirements are defined for each zone. First, the *untrusted zone* on the left describes user terminals and other groups of equipment that cannot be directly managed by an NGN provider. The *trusted but vulnerable zone* in the middle designates groups of equipment that are subject to control equivalent to firewall protection by NGN providers. And finally, the *trusted zone* on the right consists of groups of equipment that can be managed by NGN providers. NGN Release 1 security requirements address space separation, enhancements built into equipment, signaling, the safeguarding of management system communications, and other concerns.

[†] NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
Email: hariu.takeo@lab.ntt.co.jp

Table 1. ITU-T NGN security-related documents.

Recommendation No. or draft name	Title or content summary	Completion date
Y.2701	Security requirements for NGN Release 1	Apr. 2007
Y.secMechanisms	NGN security mechanisms	Second quarter 2008
Y.NGN Authentication	NGN authentication	First quarter 2008
Y.NGN Certificate Management	NGN certificate management	Second quarter 2008
Y.NGN AAA	Authentication, authorization, and accounting applications for implementing network and service security requirements over NGN	Second quarter 2008
Y.IdMsec	NGN identity management security	Third quarter 2008
Undecided	Security requirements for NGN Release 2	Undecided


Network elements not always controlled by NGN provider
Network elements controlled by NGN provider
Untrusted zone
Trusted but vulnerable zone
Trusted zone
TE
TE
TE border elements
Provider-controlled equipment
TE
TE
TE border elements
Network border elements
NGN network elements

TE: terminal equipment

Fig. 1. NGN security trust model.

3. NGN security mechanisms

Specific security mechanisms for satisfying NGN security requirements are covered in Draft ITU-T Recommendation *Y.secMechanisms* (NGN Security Mechanisms). For example, several schemes for authenticating users and subscribers are addressed in the Recommendation, including schemes based on X.509 certificates recommended by ITU-T, shared keys, and network addresses.

Use cases in which security for signaling and management systems is provided by transport layer security (TLS) and by encryption based on the security architecture for Internet protocol (IPsec) are being studied. For media security, several schemes are being considered in which the medium is encrypted by secure real-time transport protocol (SRTP). And regarding the audit trails and retention of log files, various issues are being considered, including the maintaining of management system access records, the use of a log server, and patch management, and other issues.

4. NGN authentication and authorization requirements

There are many different situations where authentication and authorization in the NGN will be required, such as cases where the transport and service layers are separated and, cases where services are offered by

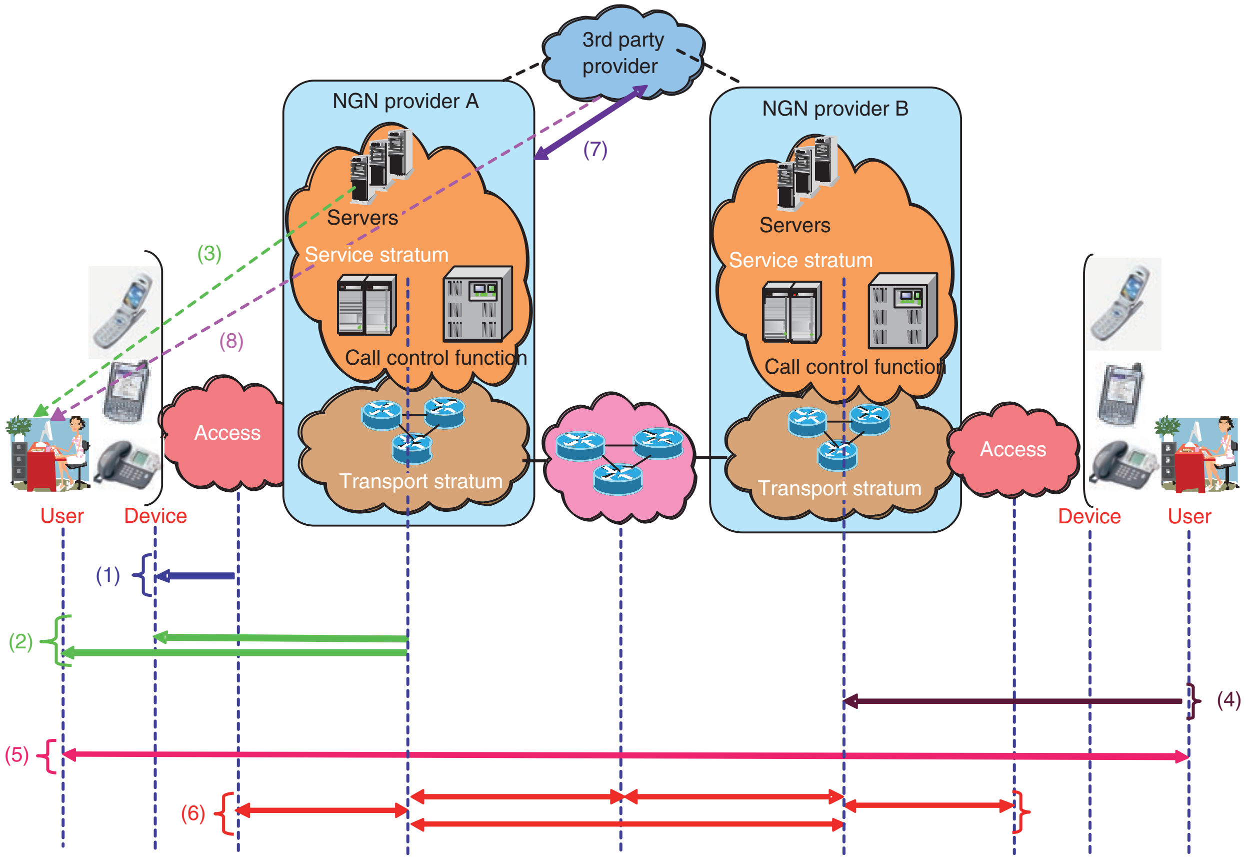


Fig. 2. NGN authentication and authorization model.

third parties. Draft ITU-T Recommendation *Y.NGN Authentication* (NGN authentication and authorization) defines the following authentication patterns and their requirements based on the authentication and authorization model presented in **Fig. 2**.

(1) Authentication and authorization of user for network access
(2) Service provider authentication and authorization of user for access to service/application
(3) Service provider authentication and authorization of user for access to specific service/application
(4) User authentication and authorization of network
(5) User peer-to-peer authentication and authorization
(6) Mutual network authentication and authorization
(7) Authentication and authorization of third-party service/application provider
(8) Use of third-party authentication service

For example, two issues now being considered are authentication at a visited network when multiple networks are involved and secure sharing of authentication results.

5. NGN certificate management

The public key infrastructure (PKI) plays an important role in implementing authentication, encryption, and other security mechanisms in legacy information technology and communications systems and plays a similarly important role in the NGN. Draft ITU-T Recommendation *Y.NGN Certificate Management* (NGN certificate management) is a document specifying how public-key certificates will be used in the NGN. It focuses primarily on the format and content of certificates and management of certificates.

First, the format of certificates used in the NGN is based on X.509 version 3, a certificate format that is already in widespread use. Regarding the content of each field in the certificate format (e.g., subject field and extension fields), detailed use cases are described according to the type of devices that store the certificate.

For certificate management, the Recommendation deals primarily with methods of issuing and distributing certificates, verifying their validity, and maintaining revocation information about them. Certificate issuing procedures are described in particular detail: Three types of certificates are defined in terms of ownership—NGN provider's network element certificates, NGN subscriber certificates, and NGN end user certificates—and recommended methods for key pair generation, certificate issuing, and certificate distribution are specified for each type of certificate.

6. NGN identity management security

Following the July 2007 meeting, identity management in the NGN emerged as a major issue from an NGN security aspect. The area of identity management technology has expanded greatly with the popularity of the Internet. OASIS [2], volunteer standardization bodies, and business alliances have led the way in developing technical specifications, organizing conformance events for the implementation of its specifications and also interoperability. Taking into account these remarkable activities, Q.15/13 reached agreement creating Draft ITU-T Recommendation *Y.IdMsec* (NGN Identity Management Security) from the perspective of security in the NGN and has compiled many relevant interests. Based on a great number of contributions, editing work on the Recommendation started from the October 2006 meeting. The current scope of the Draft Recommendation consists of the following six items:

1. Define basic concepts associated with NGN identity management.
2. Determine an identity management framework (the framework must be applicable to all NGN entities) based on the functional requirements and architecture of the NGN.
3. Assess security threats and vulnerabilities associated with identity management in the NGN environment.
4. Develop a reliability model for identity management in the NGN environment.
5. Define assurance targets and conditions for NGN identity management.
6. Discuss the many contributions already submitted and clarify the functions required to ensure cyber security and important infrastructure.

Three basic existing identity management technology specifications were consulted:

(1) ITU-T Recommendation X.1141 (OASIS SAML v2.0) covering single sign-on technology,

(2) User self-approved identity related and attribute exchange technology specifications developed by the Liberty Alliance [3], and

(3) OpenID [4], which uses a uniform resource identifier (URI) as a single sign-on identifier for accessing many websites.

Q.15/13 is also examining some of the same security issues that affect the NGN in much the same way as the Internet at large, including protection of individual privacy and personal data.

7. Focus Group on identity management

ITU-T authorizes the formation special focus groups (FGs) to concentrate attention on and speed up deliberations on especially important themes. For example, the NGN was one such important theme and was closely investigated during the study period of the FG NGN. Similarly, FG IPTV is currently studying Internet protocol television. A Focus Group on Identity Management (FG IdM) was formed in December 2006 under SG17 (the Study Group charged with considering issues related to security, language, and telecom software). The target range of ID management is so extensive that delimiting the scope is extremely important. For example, depending on how one defines a network (NGN, Internet, mobile networks, or a combination of these networks) or the range of ID management (does it encompass network subscribers, Web service accounts, RFID (radio frequency identification), and so on?), there could be an enormous number of problematic issues in delimiting the scope. The FG IdM is thus busily engaged in exchanging views with groups working on related issues within ITU-T and existing standardization groups outside ITU-T, making comparisons with legacy technologies, analyzing gaps, and drawing up use cases and requirements documents.

8. Conclusions

This article summarized recent NGN security-related standardization work by focusing on documents pertaining to security in NGN Release 1 and reviewing recent identity management initiatives. Based on extensive discussions on common international standards among carriers—including NTT—and vendors from around the world, work on Release 1 has been completed. Meanwhile, Release 2 is in the planning stage. In addition to ID management, it will also address IPTV, full mobility, and other security-related issues. Leveraging its expertise in advanced security technologies cultivated through pioneering work in the broadband environment, NTT Research Laboratories will continue its active involvement in international-standards-making activities.

References

[1] N. Morita, H. Imanaka, O. Kamatani, T. Ohba, and K. Tanida, “Overview and Status of NGN Standardization Activities at ITU-T,” NTT Technical Review, Vol. 5, No. 11, 2007.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200711gls.html

[2] http://www.oasis-open.org/

[3] T. Miyata, “Standardization Activities of the Liberty Alliance,” NTT Technical Review, Vol. 4, No. 5, pp. 51–53, 2006.

[4] http://openid.net/

Takeo Hariu
Senior Research Engineer, Supervisor, NTT Information Sharing Platform Laboratories.
He received the B.S. and M.S. degrees in electronic engineering from the University of Electro-Communications, Tokyo, in 1989 and 1991, respectively. He joined NTT Laboratories in 1991 and is currently engaged in NGN security. He is a member of the Institute of Electronics, Information and Communication Engineers of Japan.

Teruko Miyata
Senior Research Engineer, NTT Information Sharing Platform Laboratories.
She received the B.S. and M.S. degrees in mathematical science from Ochanomizu University, Tokyo, in 1991 and 1993, respectively. She joined NTT Laboratories in 1993. Her current field of interest is global standardization of identity management and security.

Yoshihito Oshima
Senior Research Engineer, NTT Information Sharing Platform Laboratories.
He received the B.E. and M.E. degrees in electrical engineering from Hokkaido University, Hokkaido, in 1994 and 1996, respectively. He joined NTT Laboratories in 1996 and is currently engaged in developing authentication technology for the NGN. He is a member of the Information Processing Society of Japan.