International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1163

(05/2015)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services – Peer-to-peer security

Security requirements and mechanisms of peer-to-peer-based telecommunication networks

Recommendation ITU-T X.1163

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	**X.1160–X.1169**
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1163

Security requirements and mechanisms of peer-to-peer-based telecommunication networks

Summary

Because of the obvious merits of peer-to-peer (P2P) networks (such as lower cost, scalability and fault tolerance), some operators began to consider the possibility of constructing the next-generation kernel network based on P2P. In order to implement an operable and manageable P2P-based telecommunication network, the security solution must be a critical part of it.

The distributed service network (DSN) defined in Recommendations ITU-T Y.2206 and ITU-T Y.2080 is designed as a telecommunication network based on P2P. The capability requirements and the functional architecture are defined in Recommendations ITU-T Y.2206 and ITU-T Y.2080, respectively; however, the security aspects are not addressed in either of these two Recommendations. The security requirements and mechanisms defined in Recommendation ITU-T X.1163 complement the DSN-related work.

Recommendation ITU-T X.1163 provides a security guideline for a telecommunication network based on P2P technology. It briefly introduces the characteristics of the network, it also analyses the security requirements of the network and the services, and it specifies the security mechanisms to fulfil these requirements.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1163	2015-05-29	17	11.1002/1000/12476

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1163

Security requirements and mechanisms of peer-to-peer-based telecommunication networks

1 Scope

This Recommendation provides a security guideline for a telecommunication network based on peer-to-peer (P2P) technology, including the network characteristics, the security requirements of the network and the services, as well as security mechanisms to fulfil these requirements.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.2080] Recommendation ITU-T Y.2080 (2012), *Functional architecture for distributed service networking*.

[3GPP TS 33.102] 3GPP TS 33.102 V7.1.0 (2006), *3G Security; Security architecture*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 ContentID: An identity number which is the same in different content fragments to identify the fragments of the same content file.

3.2.2 copyright problem: Legal issue resulting from spreading copies without the permission and authorization of the owner.

3.2.3 privacy problem: Attackers steal private information without the permission of or authorization by the owner.

3.2.4 KeyID: An identity number to identify a key in the security algorithms.

3.2.5 KeySeed: A random number based on a key which will be produced in the security algorithms.

3.2.6 trust: The relationship between two entities where each one is certain that the other will behave exactly as it expects.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AF Application Function

AKA	Authentication and Key Agreement
AUTN	Authentication Token
AV	Authentication Vector
CDF	Content Delivery Function
CK	Confidentiality Key
C/S	Client/Server
CS	Content Server
CSAF	Content Service Application Function
DHT	Distributed Hash Table
DoS	Denial of Service
DRM	Digital Rights Management
DSN	Distributed Service Network
EF	End-user Function
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HLR	Home Location Register
ICT	Information and Communication Technology
ID	Identity
IK	Integrity Key
IP	Internet Protocol
MF	Management Function
NAT	Network Address Translation
NEF	Node Enrolment Function
NGN	Next-Generation Network
P2P	Peer-to-Peer
PC	Personal Computer
QoS	Quality of Service
RAND	Random number (used for authentication)
RES	Response
RF	Relay Function
RLF	Resource Location Function
SCF	Service Control Function
SP	Streaming Packer
SS	Streaming Server
TOCF	Traffic Optimization Control Function
UE	User Equipment
USIM	Universal Subscriber Identity Module

VoIP Voice over IP

WLAN Wireless Local Area Network

XRES expected Response

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

6 Architecture of a telecommunication network based on P2P

The architecture of constructing a telecommunication network based on P2P technology is as shown in Figure 6-1.

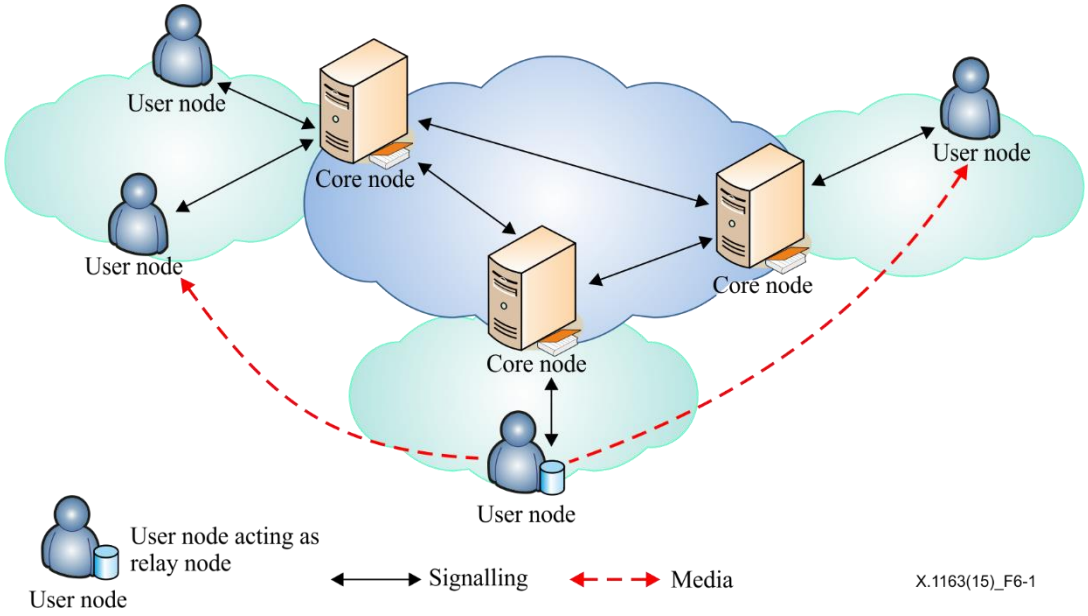

Figure 6-1 – Telecommunication network architecture based on P2P

In Figure 6-1, the core network based on P2P technology is connected with users through the access network (e.g., the global system for mobile communications (GSM), the general packet radio service (GPRS), the wireless local area network (WLAN)) and provides different services to them.

The distributed service network (DSN) architecture defined in [ITU-T Y.2080] can be regarded as a conceptual model of the telecommunication network architecture based on P2P. For the convenience of defining the security requirements and mechanisms of a P2P-based telecommunication network, the network elements are simplified in Figure 6-1 compared to the architecture defined in [ITU-T Y.2080]. See Appendix II for the mapping relationship between the two architectures.

The nodes in this architecture can be divided into three types:

Core node: Nodes of this type are deployed and configured by the operator. Operators are able to control these nodes completely. The main functions of these nodes include signal processing, data transmission and billing generation, etc.

User node: Nodes of this type are terminals owned by users, e.g., personal computers (PCs), mobile terminals, etc., and use the services provided by the network. In some cases, user nodes have the

ability to transfer data packets to other user nodes. Those user nodes which transfer data to other user nodes can be called relay nodes.

Relay node: Nodes of this type relay data packets in order to improve node reachability. If a node cannot meet the request of the origin, the node relays the packet(s). Additionally, these nodes can relay multicasting packets to neighbouring peers in multicasting service.

The main characteristics of such a telecommunication network based on P2P are as follows:

1) Distributed network architecture

   The P2P-based core network has no centralized node. Such a network is highly decentralized and hence has only weak ability for resource coordination. The network exploits diverse connectivity between nodes and the rich set of resources (e.g., computing power and storage) available at each node rather than conventional centralized resources to provide distributed computing power and services. With the rapid advancement of ICT, many more aggregate information and computing resources are available from distributed nodes than from a limited number of centralized servers.

2) Robustness and scalability

   First, as services are provided by distributed servers and nodes, the influence on other nodes is limited when some nodes are subject to intrusion or destruction. Second, the P2P network is self-organized and can adjust the topology automatically to maintain connectivity between peers when parts of the nodes have failed. Third, the network can adjust itself automatically according to the change of network bandwidth, load balance, and the number of nodes.

3) Privacy protection

   Because the transferring path of the data is distributed, there is no single point at which to intercept data packets. This reduces significantly wiretapping threats and information leakage.

4) Load balance

   The P2P-based architecture reduces the requirements for computing capability and storage capacity as in a traditional client/server (C/S) structure. As the resources are stored in different server peers in a distributed manner, the network can afford better load balance.

5) Self-management

   In P2P-based networks, nodes are not fully controlled by a central system. The network nodes can manage themselves to a large extent in many aspects including security policy definition, resource and service providing. This facilitates network management and also makes the network flexible.

6) Deployment costs

   The P2P network does not have high requirements for computing capability at each node and the nodes can be set up on low-cost computing platforms such as PCs. This reduces deployment costs considerably.

7 Security requirements analysis

The security requirements of P2P-based telecommunication networks are analysed in this clause. Security requirements of general P2P networks are given in [b-ITU-T X.1161].

During the security requirements analysis of service scenario, two basic services provided on the P2P-based telecommunication network are considered: voice over Internet protocol (VoIP) and streaming. VoIP is the basic voice service and streaming is the basic data service on a P2P network.

7.1 Authentication and authorization

Authentication and authorization are the basic security mechanisms of the P2P-based telecommunication network. User nodes and core nodes all need strict authentication and authorization. The identity of a peer shall be remotely validated securely through the network. Furthermore, access of the resources and services shall be strictly authorized.

7.2 Trust management

Due to the open and anonymous nature of P2P networks, a P2P-based telecommunication network provides an open, unrestricted environment for P2P-based VoIP, streaming and content-sharing services. This openness of a P2P-based telecommunication network makes it an environment susceptible to attackers spreading malicious content. If there is no effective trust evaluation and management mechanism, a P2P-based telecommunication system cannot provide a trust- and privacy-preserved service. A trust mechanism is needed to determine whether remote nodes can be trusted and to what extent.

In VoIP services, where user nodes can be used as relay nodes to transfer voice data, a trust mechanism is required to help the core nodes select the appropriate user nodes. A P2P-based network can be protected against attack from hostile nodes by using this mechanism.

7.3 Confidentiality

Confidentiality for data and signalling are required in any telecommunication network. In the service scenario:

1) VoIP service

   If the signal and data flow in the network are unencrypted, attackers may have chance to intercept users' private conversations. Therefore, the confidentiality protection of signalling and data is recommended.

2 Streaming service

   In streaming services, key information can be transferred and temporarily stored in user nodes and relay nodes, so it is recommended that confidentiality protection for signalling message, user-profile and data contents be provided.

7.4 Integrity

Integrity for data and signalling is required in any telecommunication network. In the service scenario:

1) VoIP service

   In VoIP services, attackers can modify signals and data packets or insert malicious signals and data into the users' connection. The integrity for signals and data is very important. Therefore, it is required to implement integrity protection in VoIP.

2) Streaming service

   In streaming services, user information such as the Internet protocol (IP) address can suffer from security threats such as malicious spoofing during the authentication process. This causes denial of service (DoS) attacks. When the connection is established between a user and network, if attackers can modify the user's request, the user will not be able to get the right streaming file. Therefore, it is required to implement integrity protection in streaming.

7.5 Digital rights management

Digital rights management (DRM) is mainly used in streaming services. Streaming files can spread faster than ever before in a P2P environment. As a result, control of content and digital rights is more difficult. This situation can cause serious problems to operators. DRM can provide methods for the

control and management of streaming content, confirmation of the validity of streaming files and the avoidance of copyright issues between operators and content providers. Thus, it is recommended that DRM be used in streaming services of P2P-based telecommunication networks.

8 Security mechanisms

Two basic security mechanisms for P2P-based telecommunication networks are defined in this Recommendation, including the authentication and authorization mechanism, and the trust management mechanism. See Appendix I for service use cases of the security mechanisms.

8.1 Authentication and authorization mechanism

The authentication and key agreement (AKA) mechanism, which is specified in [3GPP TS 33.102], is well accepted in telecommunication networks.

In this mechanism, a pre-shared root key *K* is stored in the universal subscriber identity module (USIM) card and home location register (HLR). Mutual authentication between the user and the network is provided, based on the authentication vectors that are computed based on the pre-shared root key.

An authentication mechanism based on AKA is defined to provide mutual authentication in a P2P-based telecommunication network.

8.1.1 Authentication scenario

When a user node needs to access the network, mutual authentication between the user node and the network is executed based on AKA. As shown in Figure 8-1, the authentication scenario is described as follows:

1) A P2P ring is constructed by all the core nodes based on the distributed hash table (DHT) routing.
2) Core nodes in the DHT ring may be out of service due to overload or other reasons.
3) Users' authentication data (such as the user's identity (ID) and root key *K*) can be stored on any core node.
4) User node A's authentication data can be stored on several core nodes at the same time (such as core nodes B, D and E).
5) Each core node has the capability to compute which core node a user's authentication data is stored on, based on the user's information.
6) A user node chooses a core node (e.g., core node A) based on a specific policy to connect to the network.

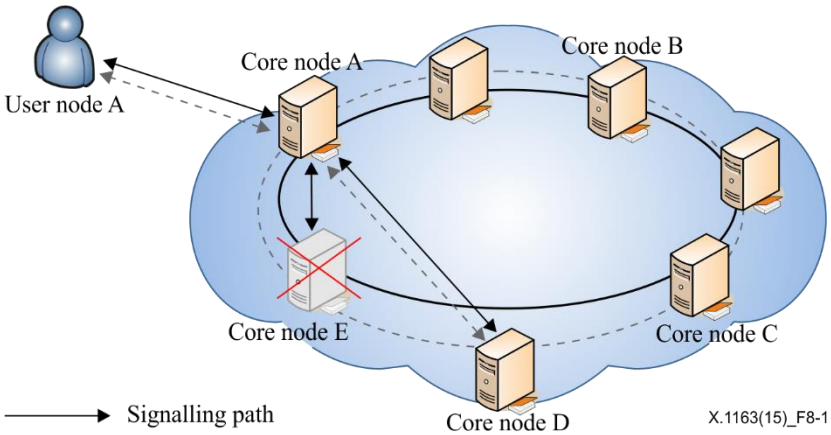

Figure 8-1 – Authentication scenario

8.1.2 Authentication mechanism

When user node A sends a request to core node A to access the network, core node A will check if it already stores user node A's authentication data. If this is true, then core node A will generate AKA authentication vectors (AVs) and AKA authentication is executed between user node A and core node A.

Otherwise, if core node A cannot find user node A's authentication data, core node A will search the next core node that has user node A's authentication data in the DHT routing ring (core node E in this case) and detect whether it can provide AVs to user A. If core node E works properly, it will generate and send AVs to core node A, then AKA authentication can be executed between core node A and user node A.

If core node E has no ability to provide AVs, core node A will search the next core node that has user node A's authentication data in the DHT routing ring (core node D in this case) and will repeat the above procedures. If no core node can provide AVs for user node A, a notification will be sent to user node A from core node A to announce the authentication failure.

When core node A receives user node A's request, a timer starts to limit the time of the authentication procedure. When time is out, the authentication procedure fails. Core node A stops searching and sends a notification to user node A to announce the authentication failure.

The authentication procedure is as follows:

1. User node A sends a user authentication request message to core node A.
2. Core node A first tries to find user node A's subscription in local storage. If core node A finds user node A's subscription in a local database, core node A generates the authentication vector directly and proceeds to step 5.
   - 2a) If core node A cannot find user node A's subscription, core node A will try to connect to the main node (e.g., core node E) to get the authentication vector. If the core node E is online, core node A will send an authentication data request to core node E.
   - 2b) If core node A finds core node E is offline, core node A will try to connect to the other backup node (e.g., core node D), then core node A will send an authentication data request to the nearest backup node that is online. If none of the backup nodes is online or the time is out, core node A will send an authentication failure message to user node A.
3. Core node E/D computes the authentication data as in the AKA authentication steps.
4. Core node E/D sends an authentication data response message to core node A.
5. Core node A sends an authentication data request (containing a random number (RAND), and an authentication token (AUTN) elements) message to user node A.
6. When the authentication message is received from core node A, user node A shall verify whether AUTN is correct. If the verification is successful, user node A generates a response message containing a response parameter (RES) to core node A. Furthermore, user node A shall compute session keys such as a confidentiality key (CK) and an integrity key (IK). Otherwise, user node A shall send back a user authentication reject message with an appropriate reason.
7. A user authentication response (RES) message shall be sent to core node A.
8. Core node A shall verify whether RES is equal to expected response (XRES). If equal, the authentication procedure is successful. Otherwise, core node A shall send an authentication failure message to user node A. The confidentiality and integrity between the user node and the core node can be protected based on the CK and IK.

8.2 Trust management mechanism

8.2.1 Trust management scenario

Figure 8-2 shows a basic trust management scenario for VoIP services. Trust management can be used to select a relay node to provide voice data forwarding for VoIP services. The relay node can be either a user node or a core node.

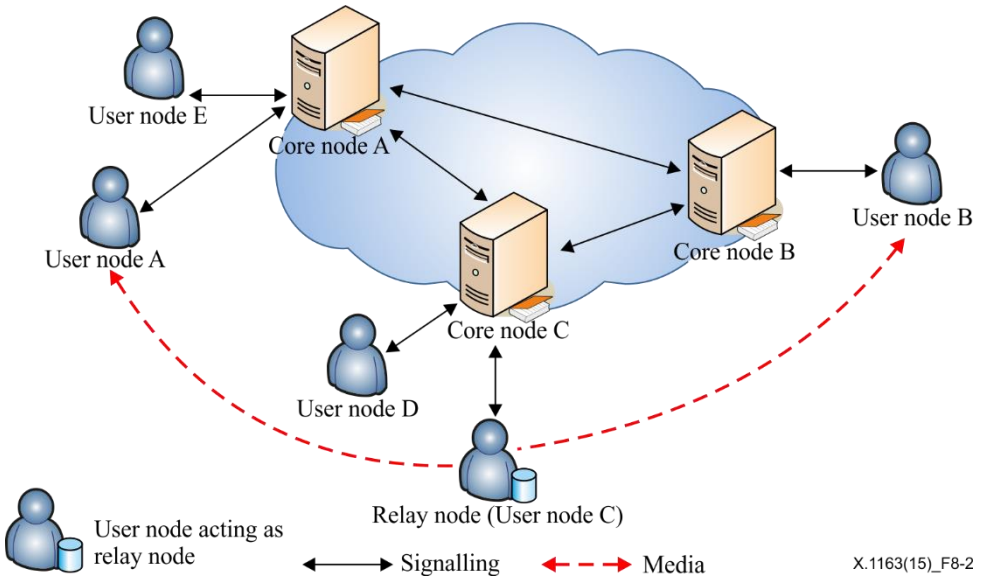

Figure 8-2 – Trust scenario in VoIP services

Figure 8-3 shows the basic trust management scenario for streaming services. In reputation-based trust management, user nodes may benefit when they provide content to other nodes. A malicious user node may report more than the amount of data it uploads in reality. Therefore, trust management is required on the streaming traffic.

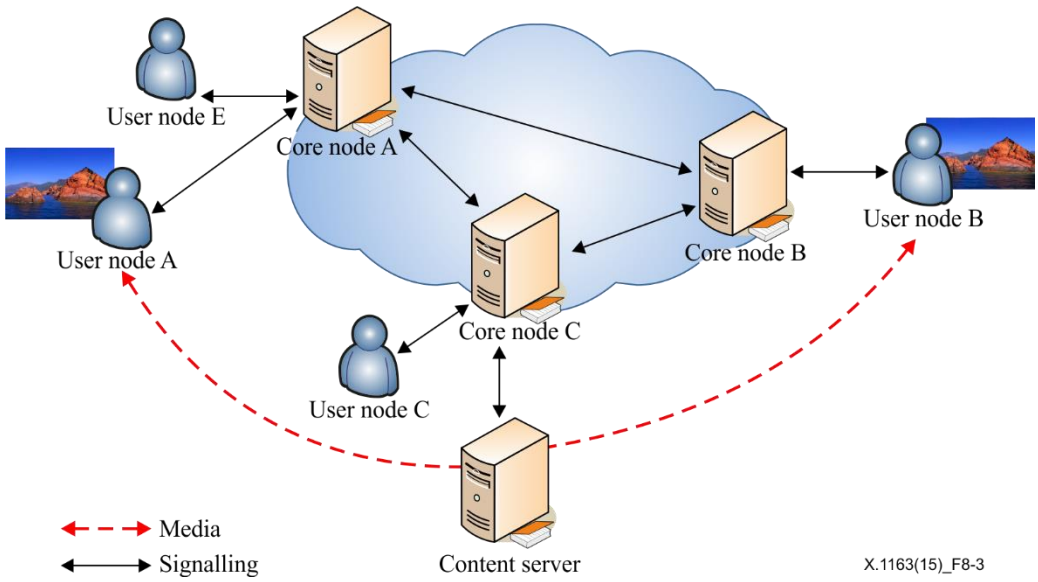

Figure 8-3 – Trust scenario in streaming services

8.2.2 Trust management mechanism

Trust management can be used to select a suitable user node as a relay node, to prevent fraud-reporting streaming traffic or to provide good reputation for two users with no credit. A good reputation evaluation criterion is the key part of the trust management mechanism.

The reputation evaluation criteria are as follows:

a) The online time. The more time a user stays online, the higher is the probability they will also stay online in future. The longer the online time is, the higher the trust credit is of a user node.

b) The forwarded data volume. The larger the forwarded data volume is, the higher the trust credit is of a user node.

c) The security capabilities. Whether a user node carries a virus, whether it has been recorded to attack other nodes, and so on.

P2P-based telecommunication services, especially video or audio streaming services, are based on one-to-many communication channels. A content provider does not know which one is involved and how to evaluate its trustworthiness. However, every peer should share a common secret key and network management server configuration to manage a plurality of nodes and distributed service resources. Each node, including user and core nodes, corresponds to one of a secure type and general type which depends on the trust evaluation results.

In different scenarios, the importance of each evaluation criterion is not the same. A criterion weight is introduced to reflect such differences. According to the various services, different criterion weights are applied. The choice of criterion weight depends on the operator's policies. For example, in VoIP services, the core node can choose criteria a) and b) with a higher weight to compose the judgment rules. In streaming services, criteria a) and c) with a higher weight can be used.

8.2.3 Trust group management mechanism

Trust groups share trusted knowledge, such as a secret key or operation code. In general, core nodes are well managed and have a good reputation; however, P2P networks consist of several types of nodes and link even though some nodes are malicious.

Therefore, trust groups provide the following two features:

– They create a virtual group for content delivery: to provide efficient delivery, streaming services use a group-based delivery mechanism; therefore P2P networks provide efficient group management.

– They create a control message between trust nodes: when a P2P network uses a core node, the network provider restricts network resources by a policy. Then the policy and some operational codes are delivered to the core node for the purposes of signalling and controlling.

See Figure 8-4.

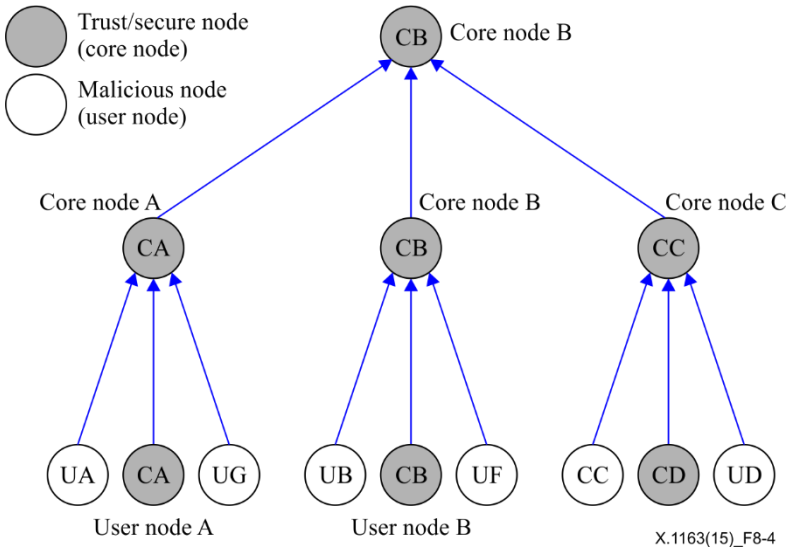

Figure 8-4 – Hierarchical trust/secure group management

Group management uses a public key or private key for asymmetric control logic and dynamic group management. A trust node delivers the contents to the leaf node and enforces the policy of the network/service/content provider, such as key update, addition and deletion of node.

– Each core node and user node corresponds to one of a secure type and a general type, the secure type of node shares a private key for decrypting the encrypted one and the encrypted data is encrypted by using a public key corresponding to the private key.
– The secure type of node shares a public key and a private key that are provided by the management node and decrypt the encrypted operational code by using the private key. The management node is a representative node of a first subgroup or centralized control node.
– The pluralities of nodes are classified into at least one or more subgroups based on proximity to a network. Each member of the subgroup comprises at least one or more secure node, and one of the secure nodes is a representative node of each subgroup and the representative node of each subgroup supports addition or deletion of a new node to or from each subgroup.
– When an approval request for addition of a secure type node is received from a representative node of a subgroup, the management node transfers a public key or a private key, which corresponds to the approval request, to the representative node of the first subgroup. Otherwise (addition of a general type node), only a public key is transferred to the representative node.
– When an update request for a public key or a private key due to deletion of a secure type of node is received from a representative node of the first subgroup, the management node updates the public key or the private key according to the update request, and transmits the updated public key or private key to the representative nodes of the subgroups.

For streaming services, the security system is based on rights management and group access control. A P2P network does not control group members, but provides a group management mechanism and related control mechanism for efficient network operation.

8.3 Confidentiality and integrity mechanisms

8.3.1 VoIP security scenario

In the VoIP scenario (see Figure 8-5), user node A accesses the P2P network through core node A, user node B accesses P2P network through core node B, and user A communicates with user B through VoIP.

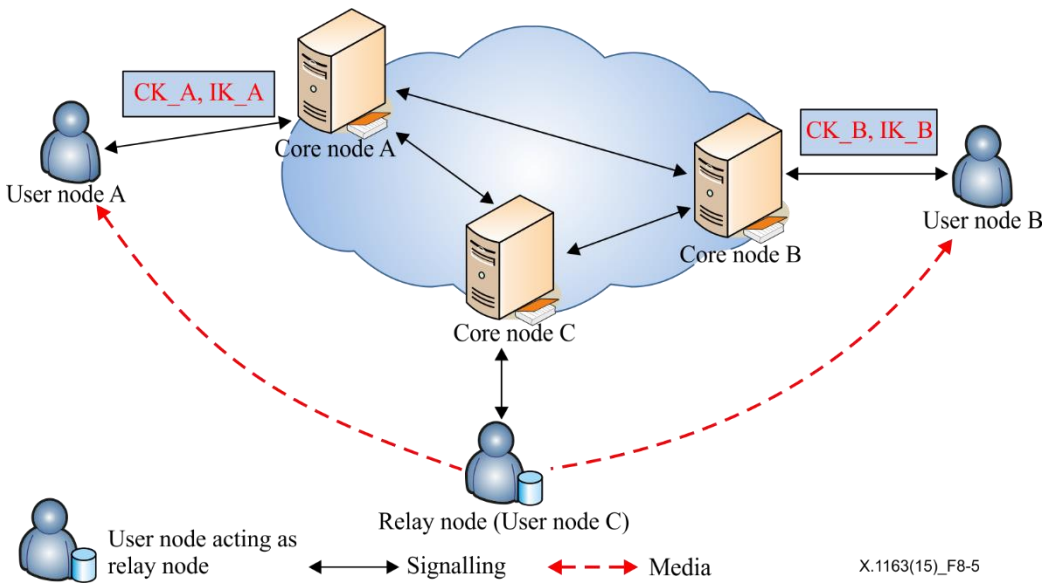

Figure 8-5 – VoIP security scenario

Because P2P communications use open networks, anonymous attackers may eavesdrop its communications by capturing traffic. Moreover, peers may be able to gather various kinds of data that are exchanged on P2P networks, if malicious users join the P2P network as peers. When peers of a P2P network relay data from one another, attackers can easily inject and modify the data. Therefore, if the data are relayed by malicious or compromised peers, the relayed data may be altered by such peers. Moreover, it may be easy to distribute malicious software, such as viruses, worms, and bots, as well as malicious information, such as false file indexes, false IP addresses or false routing tables.

Confidentiality and integrity mechanisms are required to protect users' data against eavesdropping, as well as injection and modification threats.

8.3.2 Protection of voice data

Core nodes control whether voice data are encrypted. If required, core nodes conduct the encryption algorithm negotiation, generate encryption keys, and send the results to the user nodes.

When user nodes A and B join the DSN network, they need to be authenticated. After authentication, user node A shares confidentiality key CK_A and integrity key IK_A with core node A, and user node B shares confidentiality key CK_B and integrity key IK_B with core node B.

The procedures are as follows:

1) Core node A sends its voice encryption requirement to core node B.
2) When core node B receives the message:
   a) If both core node A and core node B do not need confidentiality, core node B replies to core node A that voice encryption is not required.
   b) If either core node A and core node B needs confidentiality, core node B generates random number *RandB*, and sends *RandB* and the security capability of user B (which is stored locally) to core node A.
3) Core node A compares the security capability of user node A and user node B:
   a) If user node A and user node B do not have any common encryption algorithm version, the connection will be released.
   b) If user node A and user node B share at least one encryption algorithm version, user node A will choose one encryption algorithm as $Voice\_CF_{AB}$.
4) Core node A generates random number *RandA*, and sends *RandA* and $Voice\_CF_{AB}$ to core node B. Then core node A generates the encryption key $Voice\_CK\_{}_{AB}$ = *RandA* xor *RandB*.
5) Core node B also generates encryption key $Voice\_CK\_{}_{AB}$ = *RandA* xor *RandB*.
6) Core node A and core node B send the voice encryption key $Voice\_CK\_{}_{AB}$, and algorithm $Voice\_CF_{AB}$ to user node A and user node B separately.

After this process, all the voice data between the VoIP user nodes can be protected with encryption.

8.4 Digital rights management mechanism in streaming services

8.4.1 DRM scenario

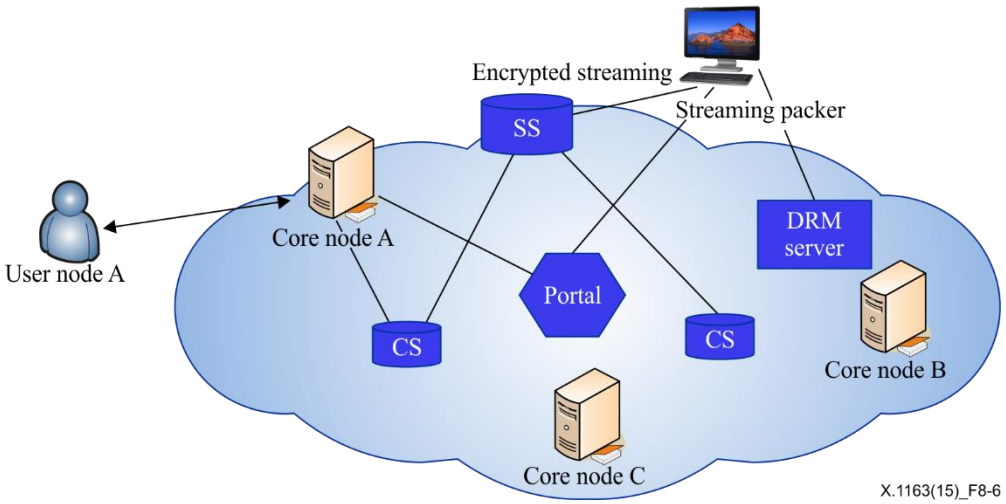

Figure 8-6 – DRM scenario in streaming services

When users access streaming media files through DSN, the typical scenario is shown in Figure 8-6. Here are the major elements:

- Streaming server (SS): Provides streaming media content in the network;
- Streaming packer (SP): Encrypts streaming media files and creates the necessary cryptographic information for streaming media file rights management;
- Content server (CS): Transits and distributes the content in the streaming server;
- DRM server: Stores the streaming media file decryption information and distributes licenses of the streaming media file;
- Portal: Serves as the entrance for users to access the streaming media files and maintains the address of the DRM server.

8.4.2 Streaming media files package

Content providers use the streaming packer to encrypt media files and to create and transfer rights management information to the DRM server and the portal.

The packaging process of a streaming media file is as follows:

1) Streaming packer shares the KeySeed with the DRM server.
2) In order to package a streaming media file, the packer generates a *KeyID*. A key is generated from *KeySeed* and *KeyID* and packaged in every fragment.
3) A *ContentID* is shared by fragments which are within one streaming media file and packaged in the head of every fragment.
4) The streaming packer encrypts the streaming media files using a particular algorithm, and the information of this algorithm is packaged in the head of files.
5) The packaged streaming fragments are distributed to SS and CS for users to access.
6) The streaming decryption information files, containing content provider ID, copyright, decryption algorithm and *KeyID* information, are transmitted to the DRM server. The streaming production information files, containing file name, size, title, introduction, price, author, publisher, copyright, content provider *ID*, *ContentID*, and DRM server address information, are transmitted to the portal.

8.4.3 DRM mechanism

When a user accesses a streaming media file, the procedure is as follows:

1) A service request is sent from the client A to the core node A.
2) Core node A gets CS information from the portal and selects one CS to get the first fragment.
3) This streaming file will be played if there is a valid licence within client A; otherwise, continue to step 4.
4) The subscription service type and heads of the streaming media file are sent from client A to core node A.
5) Core node A interacts with the portal to determine the address of the DRM server and subscription service type, and heads of the streaming media file are sent to the DRM server.
6) The type of user permission (containing the number of plays, period of validity, etc.) and playback licence (containing decryption key, decryption technology, the number of plays, period of validity, etc.) are generated from *ContentID* and the subscription service type.
7) The playback licence sent from the DRM server is forwarded to client A and the corresponding fee is deducted from the user account by core node A.
8) Client A receives the playback licence, and the streaming media file is decrypted and played.

Appendix I

Relationship of Recommendation ITU-T X.1163 and DSN-related Recommendations

(This appendix does not form an integral part of this Recommendation.)

This Recommendation focuses on a telecommunication network based on peer-to-peer mechanism. A distributed service network (DSN) is a functional model that is logically laid over the application layer. A DSN focuses mainly on content delivery and multimedia services and can use and choose P2P, CDN (content delivery network), NGN (next-generation network) or other techniques as a physical infrastructure.

I.1 Comparison between this Recommendation and [b-ITU-T Y.2206] and [ITU-T Y.2080]

Table I.1 – Comparison of this Recommendation and DSN-related Recommendations

	This Recommendation	[b-ITU-T Y.2206] and [ITU-T Y.2080]
Overall objective	Develops the security requirements and mechanisms for a P2P-based telecommunication network.	Develop the capability requirements and functional architecture of the DSN.
Scope	Provides a security guideline for a telecommunication network based on P2P technology, including the security requirements of the network and services, and the security mechanisms to fulfil these requirements.	[b-ITU-T Y.2206] specifies requirements for DSN capabilities necessary to guide the design of networks, services and applications. [ITU-T Y.2080] describes the functional architecture of DSN and its relationships with next-generation networks (NGNs). Security considerations are not addressed in these two Recommendations.
Content	• The security requirements of the P2P-based telecommunication network are analysed. • The security mechanisms of the network and some service use cases are defined.	• In [b-ITU-T Y.2206], the DSN capabilities including routing, numbering, and load are defined. • In [ITU-T Y.2080], the DSN architectural functions and reference points are defined.

I.2 Mapping with DSN functional architecture in [ITU-T Y.2080]

Figure I.1 shows the DSN functional architecture (which is Figure 7-1 in [ITU-T Y.2080]).

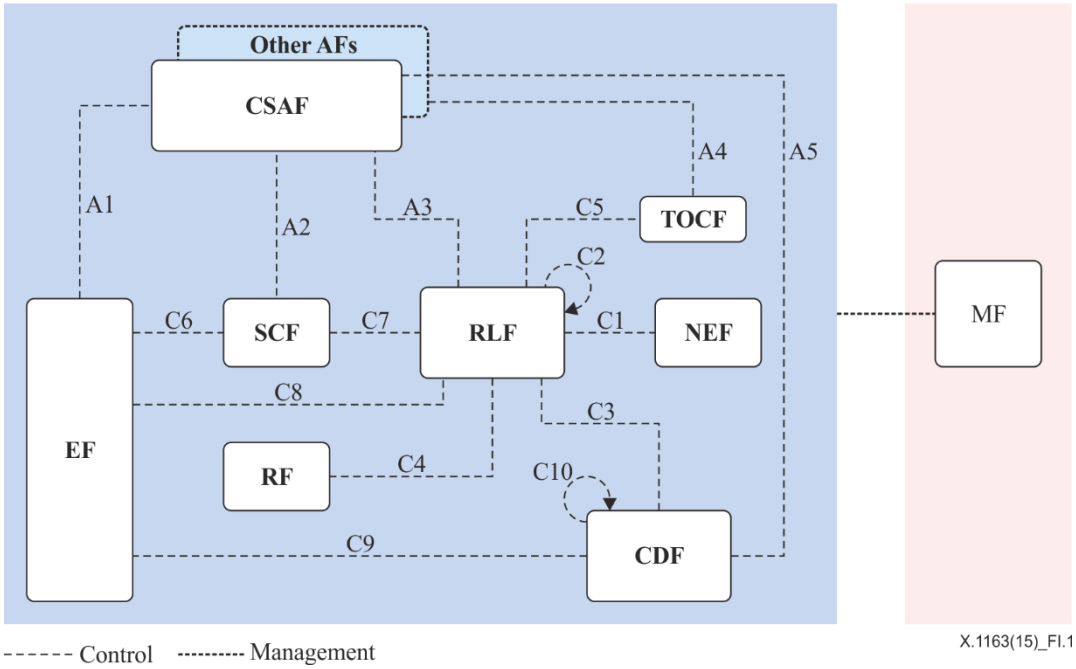

Figure I.1 – DSN functional architecture

In the context of the DSN functional architecture, "functions" are defined as a functional group composed of functional entities. The DSN functional architecture consists of several functions that interwork to provide DSN-related services and capabilities. These functions include:

– Node enrolment functions (NEFs): In the DHT-based DSN network, NEF checks the validity of the enrolling DSN node, provides initial configuration information for the DSN node and tracks the registered DSN node.

– Resource location functions (RLFs): RLF maintains resource-related information and finds the required resources when enquired.

– Relay functions (RFs): RF relays particular application traffic for the DSN nodes to achieve network address translation (NAT)/firewall traversal and quality of service (QoS) improvement.

– Content delivery functions (CDFs): CDF stores, processes and delivers content to DSN nodes or user equipment (UE).

– Traffic optimization control functions (TOCFs): TOCF makes the delivery and distribution of application traffic in the DSN network more efficient and cost effective.

– Service control functions (SCFs): SCF defined in the NGN architecture [b-ITU-T Y.2012] is reused for service control.

– End-user functions (EFs): EF is a function of the DSN UE, which supports access to a DSN network and service.

– Management functions (MFs): MF performs functions including fault management, configuration management, accounting management, performance management, and security management.

– Application functions (AFs): This Recommendation only specifies the content service application functions (CSAFs), which is one kind of AF. CSAF is an application function responsible in the DSN functional architecture for the provision of content-related services to EF.

In order to define the security requirements and mechanisms of a P2P-based telecommunication network, two kinds of entities are identified in Figure 6-1: the user nodes and the core nodes. According to the definitions of functions in [ITU-T Y.2080], they each belong to two kinds of functions: the user nodes belong to the "end-user functions (EFs)", and the core nodes belong to the "service control functions (SCFs)".

Bibliography

[b-ITU-T X.1161] Recommendation ITU-T X.1161 (2008), *Framework for secure peer-to-peer communications*.

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[b-ITU-T Y.2206] Recommendation ITU-T Y.2206 (2010), *Requirements for distributed service networking capabilities.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015