

International Telecommunication Union

**ITU-T**

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

**X.1162**

(05/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM  
COMMUNICATIONS AND SECURITY

Telecommunication security

---

**Security architecture and operations for  
peer-to-peer networks**

Recommendation ITU-T X.1162



ITU-T X-SERIES RECOMMENDATIONS  
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

<b>PUBLIC DATA NETWORKS</b>	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
<b>OPEN SYSTEMS INTERCONNECTION</b>	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
<b>INTERWORKING BETWEEN NETWORKS</b>	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
<b>MESSAGE HANDLING SYSTEMS</b>	X.400–X.499
<b>DIRECTORY</b>	X.500–X.599
<b>OSI NETWORKING AND SYSTEM ASPECTS</b>	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
<b>OSI MANAGEMENT</b>	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
<b>SECURITY</b>	X.800–X.849
<b>OSI APPLICATIONS</b>	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
<b>OPEN DISTRIBUTED PROCESSING</b>	X.900–X.999
<b>TELECOMMUNICATION SECURITY</b>	<b>X.1000–</b>

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

## **Recommendation ITU-T X.1162**

### **Security architecture and operations for peer-to-peer networks**

#### **Summary**

Recommendation ITU-T X.1162 describes a general security-related architectural model which can be applied in various peer-to-peer (P2P) networks. Based on the architectural model, this Recommendation identifies primitive operations for generic P2P networks. Non-generic and application-dependent operations are not described in this Recommendation. For each primitive operation, the relationship between the security requirements and operations is described. In addition, the relationship between the security functions and operations is described.

#### **Source**

Recommendation ITU-T X.1162 was approved on 29 May 2008 by ITU-T Study Group 17 (2005-2008) under Recommendation ITU-T A.8 procedure.

## 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/>.

© ITU 2008

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

## CONTENTS

	<b>Page</b>
1 Scope .....	1
2 References.....	1
3 Definitions .....	1
3.1 Terms defined elsewhere .....	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms .....	2
5 Conventions .....	3
6 Conceptual architecture of overlay network.....	3
7 Security architecture of the peer-to-peer network .....	4
7.1 Peer-to-peer architectural reference model .....	4
7.2 Relationship between the P2P overlay stratum and transportation stratum ...	5
8 Primitive operations of the peer-to-peer network.....	6
8.1 Join .....	6
8.2 Leave .....	6
8.3 Search .....	6
8.4 Chat.....	6
8.5 Routing .....	6
8.6 Insertion and Retrieval .....	7
8.7 Update and Delete .....	7
8.8 Multicasting.....	7
8.9 Relationship between security requirements and operations.....	7
8.10 Relationship between security functions and operations.....	12
Annex A – Structures of peer-to-peer networks .....	13
A.1 Centralized peer-to-peer networks .....	13
A.2 Pure (distributed) peer-to-peer networks.....	14
A.3 Hybrid peer-to-peer networks.....	14
A.4 DHT (distributed hash table)-based peer-to-peer networks [b-ES05].....	14
Bibliography.....	15



# Recommendation ITU-T X.1162

## Security architecture and operations for peer-to-peer networks

### 1 Scope

This Recommendation describes a general and common security-related architectural model and operations that can be applied to various peer-to-peer (P2P) networks, and only covers the generic security issues that are common to most P2P networks. The security issues are described on the basis of the operations. The complete set of security requirements is defined in [ITU-T X.1161]. According to the requirements, the peer-to-peer architectural reference model and primitive operations are proposed. For each primitive operation, the relations among the security requirements, security functions, and operations are described for the development guidelines.

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

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 access control** [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

**3.1.2 authentication** [b-ITU-T X.800]: See data origin authentication defined in clause 3.1.8, and peer entity authentication defined in clause 3.1.12.

**3.1.3 authorization** [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

**3.1.4 availability** [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

**3.1.5 confidentiality** [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

**3.1.6 cryptography** [b-ITU-T X.800]: The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

**3.1.7 data integrity** [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

**3.1.8 data origin authentication** [b-ITU-T X.800]: The corroboration that the source of data received is as claimed.

**3.1.9 integrity** [b-ITU-T X.800]: See data integrity.

**3.1.10 key** [b-ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

**3.1.11 key management** [b-ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy

**3.1.12 peer entity authentication** [b-ITU-T X.800]: The corroboration that a peer entity in an association is the one claimed.

**3.1.13 privacy** [b-ITU-T X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

**3.1.14 peer** [ITU-T X.1161]: Communication node on P2P network that functions simultaneously as both "client" and "server" to the other nodes on the network.

**3.1.15 repudiation** [b-ITU-T X.800]: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

## **3.2 Terms defined in this Recommendation**

This Recommendation defines the following terms:

**3.2.1 overlay network:** An overlay network is a virtual network that runs on top of another network. Like any other network, the overlay network comprises a set of nodes and links between them. Because the links are logical ones, they may correspond to many physical links of the underlying network.

**3.2.2 peer user:** A peer user is one who uses a computer system to access the P2P network. A peer user in a P2P network is similar to a user in the Internet, with slight differences. Specifically, peer users in the P2P network have a different operational context including personal interests, resource plans, security considerations, etc.

**3.2.3 security domain administrator:** A security domain administrator is a party with the authority to manage a specific P2P network. An administrative body may have a security policy and the appropriate enforcement mechanism to ensure the security of the P2P network under its management. Such policy and enforcement mechanism are completely application-dependent.

**3.2.4 super-peer:** A super-peer is a node in a P2P network to help routing and connectivity of nodes distributed in the Internet. The super-peer is less powerful than ordinary servers, but it is strong enough (in terms of, for example, computing power and storage) to act as a server of route resolution and connection request.

## **4 Abbreviations and acronyms**

This Recommendation uses the following abbreviations and acronyms:

DHT	Distributed Hash Table
DoS	Denial of Service
HTTP	HyperText Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
ID	Identifier
P2P	Peer-to-Peer
QoS	Quality of Service

TCP	Transmission Control Protocol
TLS	Transport Layer Security

## **5 Conventions**

None.

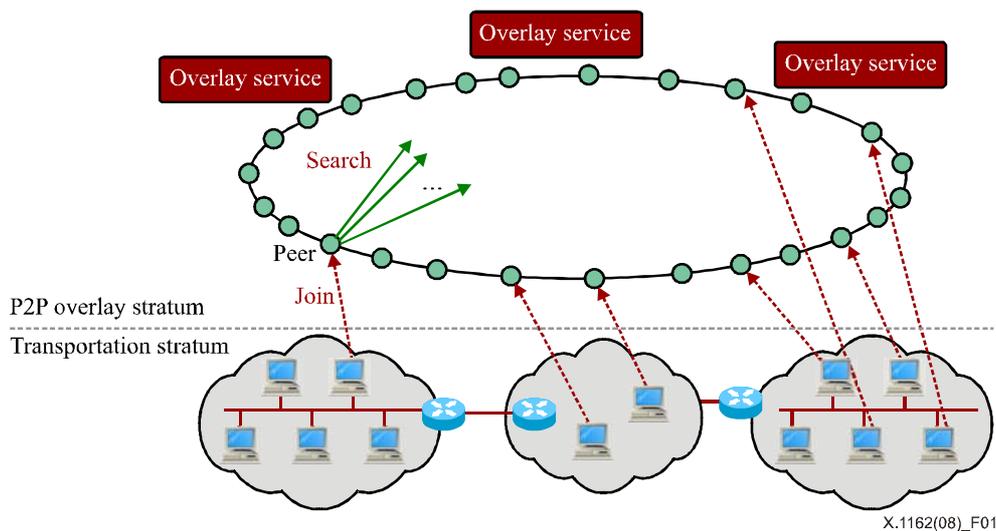
## **6 Conceptual architecture of overlay network**

While addressing, routing, and QoS management are main issues of the overlay network, this Recommendation focuses on the security of a specific type of overlay network, namely a "peer-to-peer (P2P)" network.

The P2P network is an overlay network on top of the Telecommunication and Internet. The P2P 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 a service that is not available in the Internet. With the rapid advancement of the Telecommunication Internet and computing technology, much more aggregate information and computing resources are available from distributed nodes than from a limited number of centralized servers.

Overlay networks have the following characteristics:

- 1) Overlay networks allow both networking developers and application users to design and implement their own communication environment and protocols on top of the Telecommunication and Internet, e.g., data routing and file sharing management.
- 2) Data routing in overlay networks can be very flexible, quickly detecting and avoiding network congestions by adaptively selecting paths based on different metrics, such as probed latency.
- 3) The end-nodes in overlay networks are closely connected to each other due to flexible routing. As long as the physical network connections exist, one end-node can always communicate to another end-node via overlay networks. Thus, scalability and robustness in overlay networks are two attractive features.
- 4) The high connectivity of end-nodes to join overlay networks enables the effective sharing of a huge amount of information and resources available in the Internet.
- 5) Since overlay networks are open to all kinds of Internet users, the security and privacy issues can be quite serious.
- 6) Overlay networks are highly decentralized; hence the possibly weak ability for resource coordination.



**Figure 1 – Conceptual architecture of the overlay network [b-ES05]**

As a kind of overlay networks, P2P (peer-to-peer) networks are typically used for connecting nodes via ad hoc connections. Such networks are useful for many purposes. Sharing data files containing audio, video, text, or anything in digital format is very common; real-time data, such as telephony traffic, also exploits P2P technology.

## 7 Security architecture of the peer-to-peer network

### 7.1 Peer-to-peer architectural reference model

Figure 2 shows the physical and logical P2P network architecture. In the physical P2P network, a user can join the P2P services through a device. Generally the term "peer" is used to represent a user or a device owned by the user. The connection types between the entities in a P2P network can be categorized into three cases as follows:

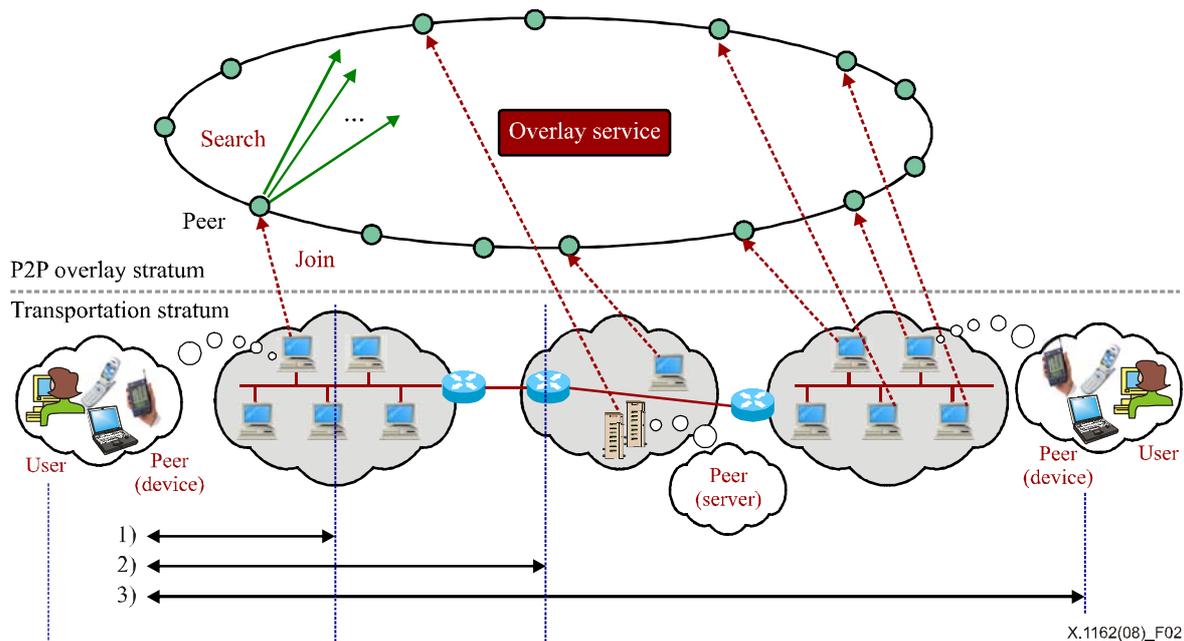
- 1) connection with an intra-domain peer (this is eventually separated into two cases: one is between a peer and a service provider peer, and the other is between peers of the same intra-domain);
- 2) connection with a service provider peer located in other network domain; and
- 3) connection with an inter-domain peer.

Peers communicate with each other by searching, sharing, etc. In the categorization, the role of the service provider peer may be treated as the role of the super-peer according to its function and/or as the role of the security domain administrator.

In the presence of a security domain administrator in the network, the role of the administrator is described as follows: in the absence of a security domain administrator in the network, the security of a P2P network depends only on the service provider. In a secure P2P network without a security domain administrator, the role of the security domain administrator may be interpreted as the role of the service provider. Therefore, the service provider should provide the P2P network with adequate security mechanisms.

Figure 2 also shows the logical P2P network architecture as a virtual network over the transportation stratum. The operation of each peer is assumed not to be limited by the physical network architecture and a peer can communicate with each peer regardless of their location (through the help of super-peer, if required). The structure of peer-to-peer network is divided into two strata: P2P overlay and transportation. The transportation stratum is responsible for providing

the transfer of packets from/to the upper layer. The overlay stratum is responsible for providing the P2P services.



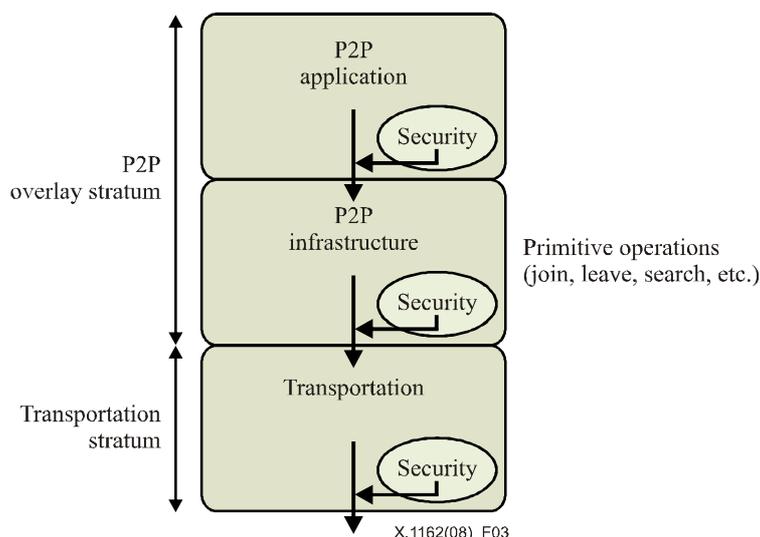
**Figure 2 – Architectural reference model for the P2P network [b-ES05]**

## 7.2 Relationship between the P2P overlay stratum and transportation stratum

For easy reference, a typical structure of a peer node is shown in Figure 3. In the structure, the overlay stratum is divided into two sub-strata: application and infrastructure.

The transportation stratum provides the session service based on the TCP and HTTP. From the viewpoint of security, a P2P provider can use the traditional security mechanisms, such as TLS and HTTPS to ensure trustiness among peers.

The P2P infrastructure sub-stratum provides primitive operations that are generally used for P2P networks, i.e., provides community services among peers: join, leave, search, routing, etc. The P2P application sub-stratum provides non-generic and application-dependent operations that are not described in this Recommendation.



**Figure 3 – Typical structure of a peer functionality**

## 8 Primitive operations of the peer-to-peer network

General operations are reviewed at the point of the infrastructure stratum. All operations should be coordinated by the security functions of [ITU-T X.1161].

### 8.1 Join

A peer user can *join* a group of P2P services by executing the P2P program. After *joining*, peer users can communicate and share resources with each other. There is no limitation in *joining* the group; thus making the P2P network vulnerable.

### 8.2 Leave

A peer user can *leave* a group of P2P services by executing *leave* operation. In P2P networks, a peer user may *leave* the network without notifying the security domain administrator and/or other peer users in case of accidents, e.g., unreliable network condition and power failure. Normally, the P2P network may implement an explicit *leave* operation to ensure the validity of other operations.

### 8.3 Search

A peer user broadcasts a *search* query to the P2P network. If there are some peers who can meet the request, they respond to the query. Some peers who cannot meet the request relay the *search* query to adjacent peers. When the TTL (time-to-live) value of a query reaches 0, the message is not forwarded.

### 8.4 Chat

A peer of a group can select the other peer for communicating with each other. After setting the session between peers, they send and/or receive text or voice messages to/from each other.

### 8.5 Routing

*Routing* is an operation not only on the unstructured P2P network but also on the structured P2P one. If a peer user makes a *search* query to the structured P2P network, the query moves around the network according to the predefined routing mechanism. It is the role of the security domain administrator to define and implement the routing mechanism.

## 8.6 Insertion and Retrieval

*Insertion and retrieval* operations belong to the structured P2P network. For the *inserting* and *retrieving* processes, the routing table of each peer is calculated. In the case of inserting a new resource, the hash value of the peers is computed, and the table of the corresponding peers is retrieved and updated. Finally, the resource is stored on the retrieved peer.

## 8.7 Update and Delete

*Update* is an operation designed to change the contents of the inserted resource; *delete* is an operation designed to *delete* the inserted resource. Since multiple copies of a shared resource may exist in a P2P network, and the peers are dynamic, the network may not guarantee a synchronized *update* or *delete* operation.

## 8.8 Multicasting

On the overlay network, *multicasting* is different from IP multicasting. In general, P2P *multicasting* is realized using the application-level retransmissions at each peer. Peers on the middle paths relay the *multicasting* packets to neighbouring peers. The protocol realization depends on the purpose of the multicast service.

## 8.9 Relationship between security requirements and operations

The primitive operations of the P2P network are closely related to the security requirements listed in [ITU-T X.1161]. The security domain administrator needs to implement the primitive operations using adequate security functions to meet the security requirements. The relationship between the security requirements and operations is shown in Table 1.

In Table 1, the letter "X" in each cell formed by the intersection of the table's columns and rows indicates that the security of a particular primitive operation is related to a particular security requirement. More precisely, the marked security requirement should be supported by the implementation of the marked primitive operation.

**Table 1 – Relationship between security requirements and operations**

Security requirements \ Operations	User authentication	Anonymity	Privacy	Data integrity	Data confidentiality	Access control	Non-repudiation	Usability	Availability	Traceability	Traffic control
Join	X	X	X						X	X	
Leave		X	X								
Search	X	X	X	X	X	X		X	X	X	X
Chat	X	X	X	X	X	X	X	X	X	X	X
Routing	X	X	X	X	X	X	X	X	X	X	X
Insertion & Retrieval	X	X	X	X	X	X	X	X	X	X	X
Update & Delete	X	X	X	X	X	X	X	X	X	X	X
Multicasting	X	X	X	X	X	X	X	X	X	X	X

### **8.9.1 Relationship between security requirements and join operation**

The security domain administrator may require that every joining peer be authenticated. Therefore, the *join* operation should implement a mechanism for providing user authentication.

Anonymity may be provided. An outside observer should not be able to acquire the information of the joining or joined peer. The *join* operation should be able to enforce the security domain administrator's policy, e.g., whether the joined peer can acquire another peer's information or not.

The *join* operation should restrict or minimize the disclosure of the peer user's personal or device-specific information.

The *join* operation should ensure an adequate level of availability for authorized access. Authorized access can be determined by various factors according to the security domain administrator's policy, e.g., whether the peer is authenticated or not.

### **8.9.2 Relationship between security requirements and leave operation**

The *leave* operation should be able to enforce the security domain administrator's policy as to whether or not the leaving peer user's personal or state information is revealed to other peers.

The P2P network may implement an explicit *leave* operation that should restrict or minimize the disclosure of the peer user's personal or device-specific information.

### **8.9.3 Relationship between security requirements and search operation**

The security domain administrator may require that only an authenticated peer be able to *search* the network. Therefore, the *search* operation should implement a mechanism for providing user authentication.

An outside observer should not be able to acquire the information of the sender or responder of the *search* query.

The *search* operation should restrict or minimize the disclosure of the peer user's personal or device-specific information.

The integrity of the *search* query or response message should be ensured to prevent or restrict the malicious manipulation of the messages. Since the *search* mechanism relies only on the peer's response, a maliciously manipulated query may cause attacks such as DoS; a forged response may cause search failure.

An outside observer should not be able to retrieve any sensitive, meaningful information from the *search* query or response message. The security domain administrator's policy may restrict peers other than the responding peer(s) from acquiring any sensitive, meaningful information from the *search* query or response message.

Peers joined in the P2P network in an authorized manner, as described in clause 8.9.1, can send or receive *search* query or response to or from other peers in the same network. The access type and level may be determined by the security domain administrator, who in turn should provide an adequate security mechanism. The access control types are listed in clause 10.6 of [ITU-T X.1161].

The *search* operation should ensure an adequate level of availability for authorized access. Authorized access can be determined by various factors according to the security domain administrator's policy, e.g., whether the peer is authenticated or not.

The *search* operation should be able to enforce the security domain administrator's policy as to whether the *search* query or response message is traceable or not.

The frequency of the *search* query and number of query responses should be limited such that these messages cannot cause heavy network congestion. If it is the security domain administrator's policy to provide any traffic control mechanism, the search operation should conform to it.

#### **8.9.4 Relationship between security requirements and chat operation**

The security domain administrator may require that only an authenticated peer be able to *chat* with other peer(s) in the network. Therefore, the *chat* operation should implement a mechanism for providing user authentication.

An outside observer should not be able to acquire the information of the chatting peers. If it is the security domain administrator's policy, a chatting peer should not be able to acquire the information of the chatting counterpart.

The implementation of the *chat* operation should restrict or minimize the disclosure of the peer user's personal or device-specific information.

The integrity of the *chat* message should be ensured to prevent or restrict the malicious manipulation of such a message.

An outside observer should not be able to retrieve any sensitive, meaningful information from the *chat* message. Other peers who are in the network but who are not participating in the *chat* should not be able to acquire any sensitive, meaningful information from the *chat* messages.

Peers joined in the P2P network in an authorized manner, as described in clause 8.9.1 can *chat* with other peer(s) in the network. The access type and level may be determined by the security domain administrator who, in turn, should provide an adequate security mechanism. The access control types are listed in clause 10.6 of [ITU-T X.1161].

The security domain administrator's policy may enforce the non-repudiation of the origin or delivery of the *chat* message.

The *chat* operation should be available to peers who are authorized to *join* the network. Authorization can be determined by various factors according to the security domain administrator's policy, e.g., whether the peer is authenticated or not.

The *chat* operation should be able to enforce the security domain administrator's policy as to whether the *chat* message is traceable or not. The enforcement may include the identifier of participating peers, chat messages, etc.

Large *chat* messages (e.g., file transfer) may be limited such that they cannot cause heavy network congestion. If it is the security domain administrator's policy to provide any traffic control mechanism, the chat operation should conform to it.

#### **8.9.5 Relationship between security requirements and routing operation**

The security domain administrator may require that only an authenticated peer be able to participate in the *routing* operation. Therefore, the *routing* operation should implement a mechanism for providing user authentication.

An outside observer should not be able to acquire the information of the sender or responder of the *route* query in a structured P2P network.

The *routing* operation should restrict or minimize the disclosure of the peer user's personal or device-specific information.

The integrity of the *route* message should be ensured to prevent or restrict the malicious manipulation of such message. Since the routing mechanism relies on the peer's response, a maliciously manipulated query may cause attacks, such as denial of service; a forged response may cause search failure.

An outside observer should not be able to retrieve any sensitive, meaningful information from the *route* message. The security domain administrator's policy may restrict peers other than the peer(s) who are located in the path from acquiring any sensitive, meaningful information from the *route* message.

Peers joined in the structured P2P network in an authorized manner, as described in clause 8.9.1, can send or receive *route* query or response to or from other peers in the same network. The access type and level may be determined by the security domain administrator, who in turn should provide an adequate security mechanism. The access control types are listed in clause 10.6 of [ITU-T X.1161].

The security domain administrator's policy may enforce the non-repudiation of the origin or delivery of the route message.

The *routing* operation should be available to peers who are authorized to *join* the network. Authorized access can be determined by various factors according to the security domain administrator's policy, e.g., whether the peer is authenticated or not.

The *routing* operation should be able to enforce the security domain administrator's policy as to whether the *route* query or response message is traceable or not.

The frequency of the *route* query and number of query responses should be limited such that these messages cannot cause heavy network congestion in a structured P2P network. If it is the security domain administrator's policy to provide any traffic control mechanism, the *routing* operation should conform to it.

### **8.9.6 Relationship between security requirements and insertion and retrieval operations**

The security domain administrator may require that only an authenticated peer be able to perform the *insert and (or) retrieve* operation. Therefore, the *insert and (or) retrieve* operation should implement a mechanism for providing user authentication.

An outside observer should not be able to acquire the information of the inserting or retrieving peer(s). If it is the security domain administrator's policy, an inserting peer should not be able to acquire information as to where the resource is stored. If it is the security domain administrator's policy, a retrieving peer should not be able to acquire information as to who has inserted the resource or where the resource is retrieved from.

The implementation of the *insertion and retrieval* operations should restrict or minimize the disclosure of the peer user's personal or device-specific information.

The integrity of the *insertion and retrieval* message should be ensured to prevent or restrict the malicious manipulation of such messages.

An outside observer should not be able to retrieve any sensitive, meaningful information from the *insertion and retrieval* message.

The security domain administrator's policy may enforce the non-repudiation of the origin or delivery of the *insertion and retrieval* message.

The *insertion and retrieval* operation should be available to peers who are authorized to join the network. Authorization can be determined by various factors according to the security domain administrator's policy, e.g., whether the peer is authenticated or not.

The *insertion and retrieval* operation should be able to enforce the security domain administrator's policy as to whether these messages are traceable or not. The enforcement may include the identifier of the inserting (retrieving) peers, resource, etc.

Large number and frequent *insertion (retrieval)* may be limited such that the message cannot cause heavy network congestion. If it is the security domain administrator's policy to provide any traffic control mechanism, the insertion and retrieval operation should conform to it.

### **8.9.7 Relationship between security requirements and update and delete operations**

The security domain administrator may require that only an authenticated peer be able to perform the *update and (or) delete* operation. Therefore, the *update and (or) delete* operation should implement a mechanism for providing user authentication.

An outside observer should not be able to *update or delete* shared resources. If it is the security domain administrator's policy, a peer who has inserted a resource should be the only one who can *update or delete* the resource.

The synchronization difficulty of the *updated or deleted* operations onto a resource should not affect data integrity, non-repudiation, and availability of the resource. For example, a newly joined peer may find that a deleted resource is still available in the network.

The security domain administrator's policy may enforce the non-repudiation of the *update and/or delete* operation.

The *update and/or delete* operation should be able to enforce the security domain administrator's policy as to whether these operations are traceable or not. The enforcement may include the identifier of the updating (deleting) peer, resource, etc.

Large number and frequent update may be limited such that the operation cannot cause heavy network congestion. If it is the security domain administrator's policy to provide any traffic control, the update operation should conform to it.

### **8.9.8 Relationship between security requirements and multicasting operation**

The security domain administrator may require that only an authenticated peer be able to participate in the *multicasting* operation. Therefore, the *multicasting* operation should implement a mechanism for providing user authentication.

An outside observer should not be able to acquire the information of peers. If it is the security domain administrator's policy, a multicast source should not be able to acquire the information as to who is receiving the *multicast* message. If it is the security domain administrator's policy, a receiver of the *multicast* message should not be able to acquire the information as to who is the source of the message. If it is the security domain administrator's policy, a peer in the middle path of the multicast tree should not be able to acquire information as to who is sending or receiving the message.

The implementation of the *multicasting* operation should restrict or minimize the disclosure of peer user's personal or device-specific information.

The integrity of the *multicast* control or data message should be ensured to prevent or restrict the malicious manipulation of the message.

An outside observer should not be able to retrieve any sensitive, meaningful information from the *multicast* control or data message.

The security domain administrator's policy may enforce the non-repudiation of the origin or delivery of the *multicast* message.

The *multicast* operation should be available to peers who are authorized to join the network. Authorization can be determined by various factors according to the security domain administrator's policy, e.g., whether the peer is authenticated or not.

The *multicast* operation should be able to enforce the security domain administrator's policy as to whether the message is traceable or not. The enforcement may include the identifier of the sender, receiver, message, etc.

Large number and frequent *multicast* transmission may be limited such that the message cannot cause heavy network congestion. If it is the security domain administrator's policy to provide any traffic control mechanism, the multicast operation should conform to it.

### 8.10 Relationship between security functions and operations

The primitive operations of the P2P network are closely related to the security functions listed in [ITU-T X.1161]. The security domain administrator should implement the primitive operations using adequate security functions to meet the security requirements. The relationship between security functions and operations is shown in Table 2.

In Table 2, the letter "X" in each cell formed by the intersection of the table's columns and rows indicates that the security of a particular primitive operation is related to a particular security function. More precisely, the marked security function should be used in the implementation of the marked primitive operation such that the primitive operation can support the security requirement.

**Table 2 – Relationship between security functions and operations**

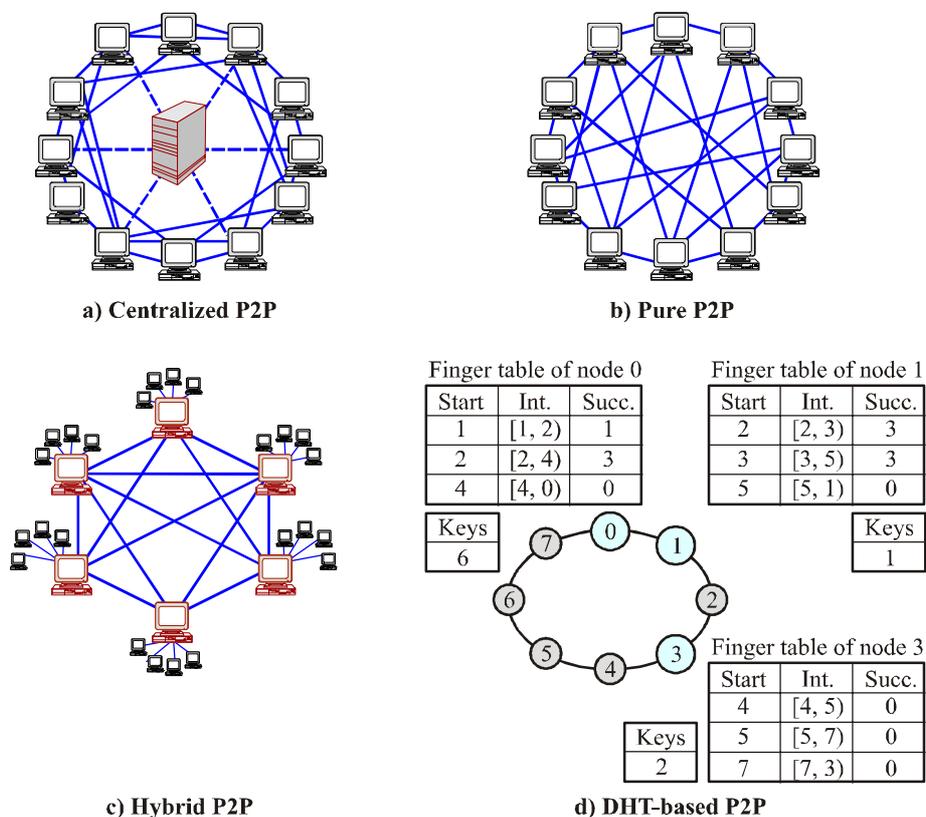
Operations \ Security functions	Security functions										
	Encipherment	Key exchange	Digital signature	Trust management	Access control	Data integrity mechanism	Authentication exchange	Notarization	Secure routing	Traffic control mechanism	ID assignment
Join	X	X	X	X	X		X		X	X	X
Leave	X			X	X		X				
Search	X	X	X	X	X	X	X		X	X	X
Chat	X	X	X	X	X	X	X	X	X	X	X
Routing	X	X	X	X	X	X	X	X	X	X	X
Insertion & Retrieval	X	X	X	X	X	X	X	X	X	X	X
Update & Delete	X	X	X	X	X	X	X	X	X	X	X
Multicasting	X	X	X	X	X	X	X	X	X	X	X

## Annex A

### Structures of peer-to-peer networks

(This annex forms an integral part of this Recommendation)

The P2P network is built over the transportation stratum and categorized as shown in Figure A.1.



**Figure A.1 – Structures of peer-to-peer networks [b-ES05]**

The P2P networks in Figures A.1-a, A.1-b, and A.1-c are generally called "Unstructured" P2P networks, because the content and its location are unrelated; neither do they follow any specific structure. In contrast, the P2P network in Figure A.1-d is a type of "Structured" P2P network, which is a distinct approach to establish a link between the stored content and the location. By far, the most common type of structured P2P network is the distributed hash table (DHT), in which a variant of consistent hashing is used to assign content to the IP address of a particular peer.

#### A.1 Centralized peer-to-peer networks

Peer-to-peer networking started with the centralized concept. In this case, a central server is still available. Unlike the client-server approach, however, this server merely stores the locations (IP addresses) of peers wherein the content is available.

Centralized P2P network is characterized by the fact that it relies on a central look-up server. Therefore, the overlay topology of a centralized P2P network can be described as a star network. Every peer is connected to the centralized look-up server, to which it can issue requests for content matching the keywords stated in the request. If the request can be resolved by the centralized look-up server, it returns the access coordinates of the peer(s) which can offer the requested content.

As depicted in Figure A.1-a, the centralized network can be characterized by its centralized topology. The file searching protocol uses a client-server model with a central index server. Note, however, that the file transfer is done in a true peer-to-peer manner. File exchange occurs directly between the hosts without passing the server.

## **A.2 Pure (distributed) peer-to-peer networks**

These schemes rely on flooding the request message of the desired content onto the P2P network rather than on central facilities. Peers sharing the content will then respond to the requesting peer.

For example, a node explores the network by broadcasting one or more query messages onto the P2P network. Each node in the network duplicates incoming query messages and forwards them to one's neighbour(s). Since the efficiency of such "flooding" depends on the number and lifetime of the duplicated query messages, some mechanisms are required to handle time-to-live (TTL) and multiple reception of the copy of a query message.

Response messages are routed back to the source of the query message. Many nodes in the network may respond to the same query. Therefore, a mechanism may be required to prevent the so-called response explosion.

## **A.3 Hybrid peer-to-peer networks**

The Hybrid P2Ps make use of a node called super-peers to help route request to content. Namely, the super-peers are often able to answer incoming request immediately by providing the resource location. When the location is not available at one super-peer, the request is relayed to other super-peers in the network.

## **A.4 DHT (distributed hash table)-based peer-to-peer networks [b-ES05]**

In DHT-based P2P approaches, the link between the stored content and the location (e.g., the IP address) is managed in a structured way.

A DHT manages data by distributing it across a number of nodes and implementing a routing scheme that allows one to look up efficiently the node on which a specific data item is located.

Each node in a DHT becomes responsible for a particular range of data items. Moreover, each node stores a partial view of the entire distributed system that effectively distributes the routing information. Based on this information, the routing procedure typically traverses several nodes, getting closer to the destination with each hop until the destination node is reached.

Thus, the DHT follows a proactive strategy for data retrieval by structuring the search space and providing a deterministic routing scheme. The DHT introduces new address spaces into which data is mapped, achieving distributed indexing by assigning a contiguous portion of the address space to each participating node. Given a value from the address space, the main operation provided by a DHT system is the look-up function, i.e., to determine the node responsible for this value.

## Bibliography

- [b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [b-ES05] Eberspächer, Jörg, and Schollmeier, Rüdiger (2005), *First and Second Generation of peer-to-peer Systems*, R. Steinmetz and K. Wehrle (Eds.): *P2P Systems and Applications*, LNCS 3485, pp. 35-56, Springer-Verlag Berlin Heidelberg.





## 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	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	Telephone transmission quality, telephone installations, local line networks
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
<b>Series X</b>	<b>Data networks, open system communications and security</b>
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems