

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X
Supplement 20
(04/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

**ITU-T X.1205 – Supplement on framework of
security information sharing negotiation**

ITU-T X-series Recommendations – Supplement 20



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
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

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

Supplement 20 to ITU-T X-series Recommendations

ITU-T X.1205 – Supplement on framework of security information sharing negotiation

Summary

This Supplement to Recommendation ITU-T X.1205 provides a framework for negotiating agreement on security information sharing between cybersecurity entities such as information requester and information provider. This Supplement defines functional capabilities and a reference model for security information sharing negotiation, conceptual data modelling of security information sharing agreement (SSA), security information sharing policy (SSP) and the SSA negotiation process.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X Suppl. 20	2013-04-26	17

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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 2013

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

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Supplement	1
4 Abbreviations and acronyms	1
5 Conventions	2
6 Introduction	2
6.1 Concept of security information sharing negotiation	2
6.2 Relationship with other CYBEX Recommendations	3
7 Functional capabilities for security information sharing negotiation	4
7.1 Negotiation capabilities	4
7.2 Agreement capabilities	4
7.3 Security capabilities.....	4
8 Reference model of security information negotiation	5
9 Life cycle and data model of SSA	6
9.1 Life cycle of SSA	6
9.2 Structure of SSA.....	7
10 Process of SSA negotiation	8
10.1 SSA negotiating messages.....	8
10.2 SSA negotiating scenarios.....	9
Appendix I – The example of security information sharing negotiation	14
I.1 Negotiation between the security management server and security agent	14
Bibliography.....	16

Supplement 20 to ITU-T X-series Recommendations

ITU-T X.1205 – Supplement on framework of security information sharing negotiation

1 Scope

This Supplement provides a framework for security information sharing negotiation to develop cybersecurity information exchange contracts between entities. The scope of the negotiation framework includes the functional capabilities and reference model for security information sharing negotiation, conceptual data modelling of a security information sharing agreement (SSA), security information sharing policy (SSP) and a SSA negotiation process.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following term defined elsewhere:

3.1.1 cybersecurity [b-ITU-T X.1205]: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise Availability, Integrity (which may include authenticity and non-repudiation) and Confidentiality.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 security information sharing agreement (SSA): A service contract on security information sharing between entities. SSA is translated into a security information sharing policy (SSP) to be applied to the corresponding cybersecurity entities.

3.2.2 security information sharing policy (SSP): A policy for cybersecurity entities to observe when sharing security information with each other. The SSP is made based on an SSA.

3.2.3 SSA negotiation: Interaction for entities to negotiate SSA before starting cybersecurity information sharing.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

CYBEX	Cybersecurity Information Exchange
EMS	Enterprise Management System
IDMEF	Intrusion Detection Message Exchange Format
IODEF	Incident Object Description and Exchange Format

SSA	Security information Sharing Agreement
SSP	Security information Sharing Policy
TMS	Threat Management System

5 Conventions

None.

6 Introduction

6.1 Concept of security information sharing negotiation

[b-ITU-T X.1500] defines a cybersecurity information exchange (CYBEX) model and techniques that can be used to facilitate the exchange of cybersecurity information between entities. An entity in the context of this Supplement is an information requester or information provider. Entities may be an independent organization or person, and as such, they have individual requirements on cybersecurity information sharing.

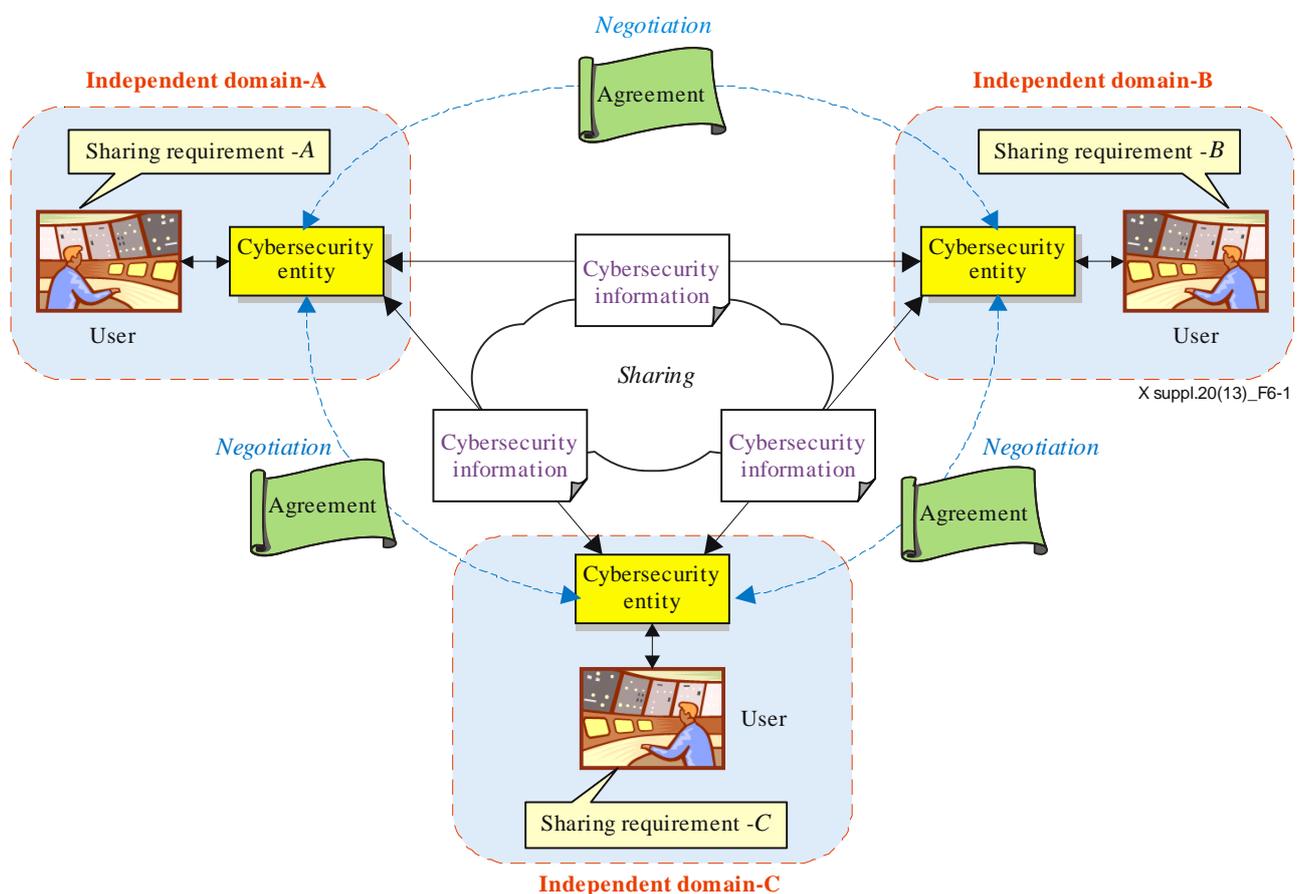


Figure 6-1 – Basic concept of security information sharing negotiation

Examples of requirements and restrictions on cybersecurity information sharing include:

- when to start and stop cybersecurity information sharing;
- what cybersecurity information to share (e.g., DoS detection log, botnet alert, black list, computer security incident, network traffic);
- what sharing level is appropriate (e.g., raw data sharing or statistical data sharing);

- appropriate protection requirements for information at different sensitivity levels (storage and transfer);
- appropriate protection requirements for regulated data;
- who the data may be shared with or disseminated to;
- liabilities in the event of a security incident or mishandling of information; and
- minimum requirements on technical standards for the secure exchange of data using CYBEX techniques, etc.

Therefore entities that participate in cybersecurity information sharing need to negotiate an agreement with each other before they begin exchanging cybersecurity information.

This Supplement describes a framework for security information sharing negotiation of a cybersecurity information exchange contract between entities. The negotiation framework focuses on functional capabilities and a reference model for security information sharing negotiation, conceptual data modelling of security information sharing agreement (SSA), security information sharing policy (SSP) and the SSA negotiation process.

6.2 Relationship with other CYBEX Recommendations

A cybersecurity information sharing procedure basically involves three entities: an information requester (referred to as 'retriever' in [b-ITU-T X.1570]), an information provider (referred to as 'source' in [b-ITU-T X.1570]) and a directory. An information requester requests information and the information provider provides the requested information to the information requester. The directory registers the metadata of the information provider's information and helps the information requester find a proper information provider. If the information requester and information provider have an existing relationship, the directory may only be used to validate information about the other entity.

The typical process for cybersecurity information sharing consists of three phases: Discovery (information provider discovery), Negotiation (information sharing negotiation), and Exchange (information exchange). The first phase is Discovery, where the information requester finds the list of information providers that can provide the desired information. The second phase is Negotiation, where the information requester negotiates the service level for information sharing with the information provider selected through the Discovery phase. Finally the information provider provides the information requester with information according to the service contract developed in the Negotiation phase. Next follows the Exchange phase.

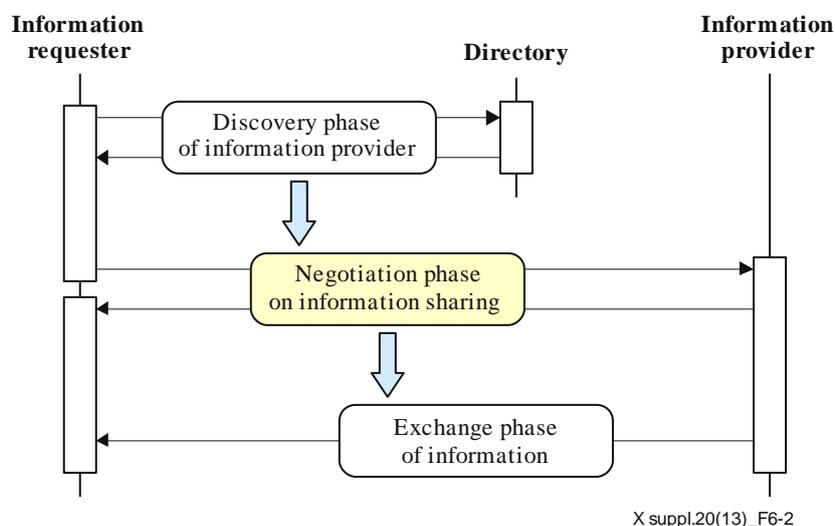


Figure 6-2 – Three phases of cybersecurity information sharing

The Discovery phase and Exchange phase are handled by [b-ITU-T X.1570] and [b-ITU-T X.1500], respectively. This Supplement focuses on the Negotiation phase.

7 Functional capabilities for security information sharing negotiation

The functional capability for security information sharing negotiation between entities is divided into three categories: negotiation capabilities, agreement capabilities and security capabilities. The capabilities below are essential unless indicated as optional.

7.1 Negotiation capabilities

In this clause, the capabilities for security information sharing negotiation are elaborated from the negotiation aspect.

- 1) **Primary negotiation capability:** The requirement for negotiating and establishing an agreement on security information sharing dynamically is as follows:
 - a) Information requester may be able to specify and request new service for security information sharing with its information provider.
 - b) Information provider may be able to communicate its acceptance or rejection of a requested service with the information requester.
 - c) Information requester may be able to accept or reject a security information sharing service proposed by the information provider.
 - d) Information requester and information provider may be able to modify the accepted service and re-negotiate with the corresponding entity. (*optional*)
- 2) **Agreement enforcement capability:** The information provider may be able to provide the information requester with a security information sharing service according to the agreement negotiated between the information requester and the information provider.
- 3) **Agreement monitoring capability:** The information requester and the information provider may be able to monitor the agreement negotiated between them to confirm if the information sharing service is fulfilled according to the agreement.

7.2 Agreement capabilities

In this clause, the capabilities for security information sharing negotiation are elaborated from the agreement aspect.

- 1) **Extendibility:** The protocol format for agreement on security information sharing may have extensibility to meet the various kinds of requirements on security information sharing service for each entity.
- 2) **Concreteness:** Agreement on security information sharing may contain concrete information about the security information sharing contract, such as when to start and stop information sharing, with whom to exchange information, what information to share, what service level to provide, how to share, etc.
- 3) **Translatability:** Agreement on security information sharing may be easily translated into policy to be enforced by entities which share cybersecurity information.

7.3 Security capabilities

Agreement on security information sharing may be handled and managed carefully as it is very sensitive information defining a contract between an information requester and an information provider. Security capabilities for secure negotiation between an information requester and an information provider are as follows:

- 1) **Confidentiality:** It provides confidentiality of the agreement for security information sharing exchanged between an information requester and an information provider.
- 2) **Integrity:** It provides integrity of the agreement on security information sharing exchanged between an information requester and an information provider.
- 3) **Mutual authentication:** It provides mutual authentication between an information requester and an information provider before performing the negotiation for an agreement on security information sharing.
- 4) **Non-repudiation:** It provides non-repudiation when each entity authorizes the agreement on security information sharing negotiated between an information requester and an information provider.

8 Reference model of security information negotiation

Figure 8-1 shows the reference model for security information sharing negotiation. An entity takes charge of the exchange of cybersecurity information between entities. An entity includes the negotiation application, which performs the security information sharing negotiation.

The negotiation application establishes SSA for the entity of a domain through negotiation with other entities. The negotiation application manages the SSP on security information sharing to fulfil the SSA effectively, and monitors the state of security information sharing to confirm if information sharing is performed properly according to the SSP.

The SSA is a service contract for security information sharing between entities. The SSA includes information such as identifier, contact information, when to share, what to share, how to share, etc. The SSA is translated into an SSP to be applied to the corresponding entities.

SSP is a policy for entities to observe when they share security information. An entity acting as an information provider uses SSP to refine raw information to transmit to an entity acting as an information requester. On the other hand, an entity acting as an information requester uses SSP to confirm if the security information sharing service is provided according to the SSA established through negotiation with the peer entity.

The framework of security information sharing negotiation consists of three kinds of components specified as follows:

- **SSA negotiation point:** It provides negotiation of the SSA between entities that participate in cybersecurity information sharing. If the SSA negotiation is successful, the negotiation is passed from the SSA negotiation point to SSA management point.
- **SSA management point:** It manages the SSA negotiation with the peer entity by translating the SSA into the SSP, with enforcement occurring at the SSP enforcement point. The SSA management point checks the quality of service (QoS) of the SSA through monitoring of the current information sharing service.
- **SSP enforcement point:** It processes cybersecurity information based on the SSP, which is enforced by the SSA management point. It receives raw cybersecurity information and returns refined cybersecurity information to be used for information sharing.

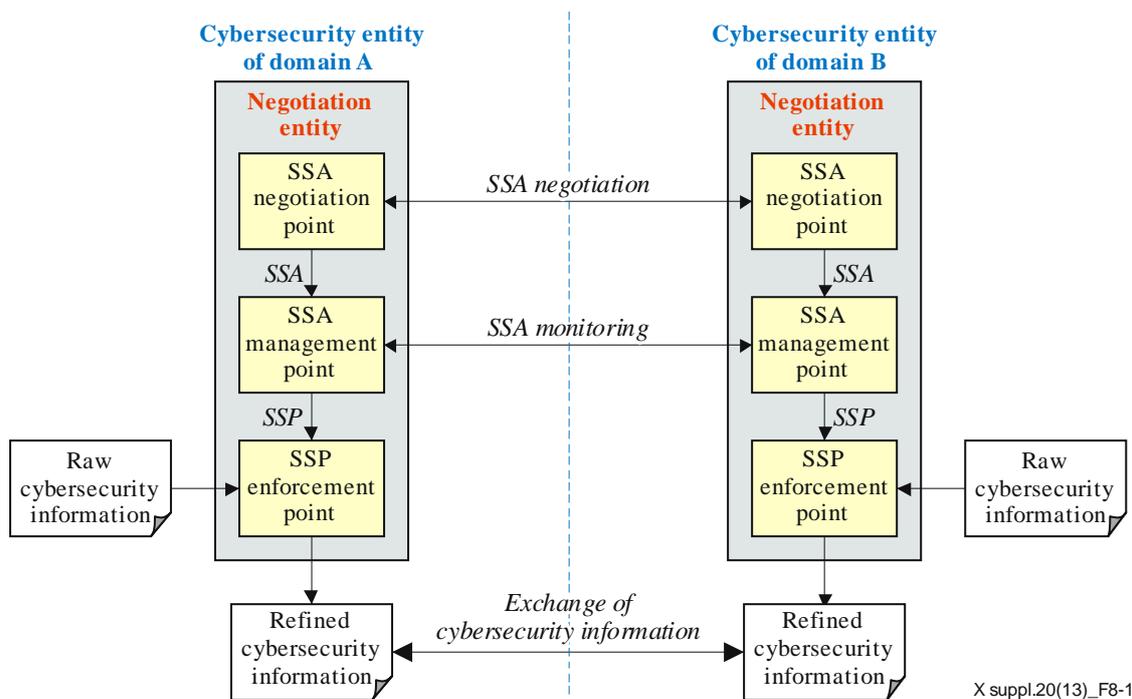


Figure 8-1 – Reference model of security information sharing negotiation

The framework of security information sharing negotiation defines two kinds of interactions between negotiating entities as follows:

- **SSA negotiation:** an interaction for negotiation entities to negotiate SSA before they start cybersecurity information sharing.
- **SSA monitoring:** an interaction for negotiation entities to monitor the fulfilment state of the SSA.

9 Life cycle and data model of SSA

9.1 Life cycle of SSA

SSA is a service contract on security information sharing between the entities exchanging information. The SSA has a life cycle consisting of five steps: template development, negotiation, implementation, execution and assessment.

- Template development: SSA templates are developed.
- Negotiation: SSA negotiation is started and the contract (i.e., SSA) is agreed upon.
- Implementation: The environment for carrying out the contract is constructed.
- Execution: the contract is performed, maintained and monitored.
- Assessment: the SSA performance is evaluated.

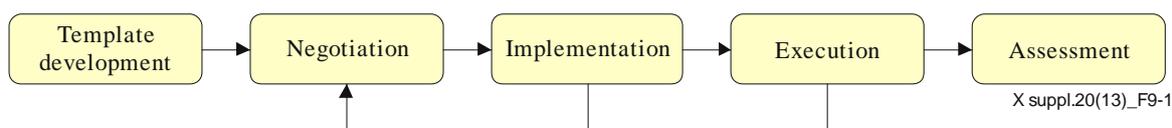


Figure 9-1 – SSA life cycle

In a normal case, each step of the SSA life cycle is performed in a linear sequence. For SSA re-negotiation, there can be additional transitions from the implementation or the execution step back to the negotiation step.

The relationship between the reference model for security information sharing agreement negotiation and SSA life cycle is as follows:

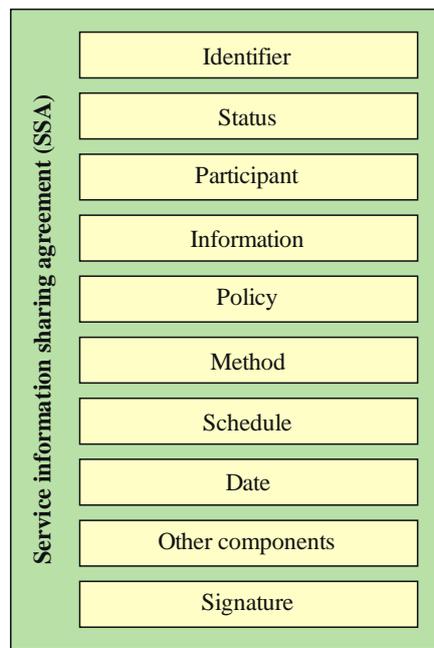
- SSA negotiation point: It performs the template development and the negotiation step.
- SSA management point: It performs the implementation and the assessment step.
- SSA enforcement point: It performs the execution step.

9.2 Structure of SSA

SSA consists of the following components. They are considered essential unless indicated as optional.

- 1) Identifier: It is used by information requesters and information providers to identify a negotiating or negotiated SSA.
- 2) Status: It indicates the status of the SSA. The status value can be 'proposal', 'approval', or 'annulment'. The 'proposal' means that it is the proposed SSA. The 'approval' means that it is the accepted SSA, that all the negotiating entities have approved the SSA. Finally, the 'annulment' means that the SSA may no longer be used.
- 3) Participant: It provides contact information about the negotiating entities. It includes information such as affiliation, name, email, address, etc. The participant has two kinds of information as follows:
 - Requester: It indicates that the participant belongs to the information requester.
 - Provider: It indicates that the participant belongs to the information provider.
- 4) Information: It indicates the name, the type, and the format of the security information to be exchanged between the entities.
 - Information name: It indicates the name of the security information to be exchanged.
 - Information type: It indicates the type of the security information to be exchanged. Examples include black lists, cybersecurity incidents, attack detection logs, etc.
 - Information format: It indicates the data format for exchanging the security information. Examples include IDMEF, IODEF, syslog, etc.
- 5) Policy (optional): It indicates the policy that information providers apply to security information that is supposed to be exchanged. There are four kinds of policies as follows:
 - Masking policy: It is used to hide the personal identifier included in the exchanged security information. An example of such a policy is "a rule to hide all the public IP addresses within the exchanging security information by using 8-bit masking".
 - Filtering policy: It is used when the entities exchanging information want to share only a subset of information. An example instance of a filtering policy is "a rule to provide the information requester with only data where the IP address of the attacking system is 1.1.1.1 out of security log data".
 - Summarization policy: It is used when the exchanging cybersecurity entities want to share not primitive information, but statistical information. An example of such policy is "a rule to provide the information requester with statistical information on the IP addresses of the attacking system that rank in top 10 in the traffic volume".
 - Handling policy: It is used to indicate how widely the exchanging information can be circulated beyond the immediate information requester, and when it is expired. A typical example of such a policy is traffic light protocol.

- 6) Method: It indicates the information delivery method between information requesters and information providers. The method component has three kinds of information as follows:
 - Delivery protocol: It indicates the delivery protocol for delivering security information between the exchanging cybersecurity entities. Examples include SOAP, SNMP, FTP, TCP, UDP, etc.
 - Delivery security: It indicates security requirements to follow during the security information delivery. An example of the delivery security is message encryption.
 - Access: It indicates communication access information for the exchanging cybersecurity entities. This information is used when information requesters connect with information providers or the information provider verifies the information requesters who ask for a connection. The examples of the access information include IP address, port number, URI, etc.
- 7) Schedule: It indicates the start and the end time of the negotiated information sharing service.
- 8) Date: It indicates the contract date of the SSA.
- 9) Other components (optional): It can be added if necessary.
- 10) Signature: It is the value of digital signature for the SSA. It is used for the SSA verification.



X suppl.20(13)_F9-2

Figure 9-2 – Structure of SSA

10 Process of SSA negotiation

The negotiation of SSA is an iterative process, whereby it is done to establish new SSAs, and modify and remove the established SSAs between information requesters and information providers.

10.1 SSA negotiating messages

This clause defines seven types of messages that can be used for SSA negotiation between the negotiating parties (cybersecurity entities). Those messages are as follows:

- 1) SSA request: It is sent by information requesters to ask information providers for a new SSA negotiation. This message includes the SSA which an information requester proposes.

- 2) SSA proposal: It is sent by information providers in response to the SSA request message. This message includes the SSA that an information provider proposes.
- 3) SSA acceptance: It is sent by the information requester in positive response to the SSA proposal message. This message includes the SSA which regards as valid responses to the message sent from the information provider.
- 4) SSA rejection: It is sent by either information providers or information requesters in negative response to the SSA request or SSA proposal message. This message includes the SSA with which the negotiating parties reject the negotiation process.
- 5) SSA cancellation: It is initiated by either information requesters or information providers to cancel an already established SSA. This message includes the SSA which the negotiating parties wish to cancel.
- 6) SSA revision: It is initiated by either information requesters or information providers to modify an already established SSA. This message includes the SSA which the negotiating parties wish to modify.
- 7) SSA confirmation: It is sent by either information requesters or information providers in confirmative response to the SSA acceptance or the SSA cancellation message. This message includes the SSA with which the negotiating parties respond by calling for an agreement.

10.2 SSA negotiating scenarios

In the SSA negotiating process, there are four kinds of scenarios: the successful negotiation of SSA, the unsuccessful negotiation of SSA, the cancellation of the established SSA and the modification of the established SSA.

10.2.1 The successful negotiation of SSA

The successful negotiation of SSA is initiated by an information requester.

Figure 10-1 depicts the exchange of SSA negotiation messages.

- 1) An information requester makes a SSA which includes its own requirements on the issues under negotiation and transmits it to the information provider using the SSA request message.
- 2) If the information provider receives the SSA request message from the information requester, it decides whether it can support the SSA or not. If yes, the information provider makes a SSA which describes its capability that satisfies the received SSA and sends it back to the information requester using the SSA proposal message.
- 3) If the information requester receives the SSA proposal message, it makes a final SSA by considering the SSA proposed by the information provider and sends it back to the information provider using the SSA acceptance message.
- 4) If the information provider receives the SSA acceptance message, it makes a SSA confirmation message that consists of the same contract terms as the received SSA and transmits it to the information requester.

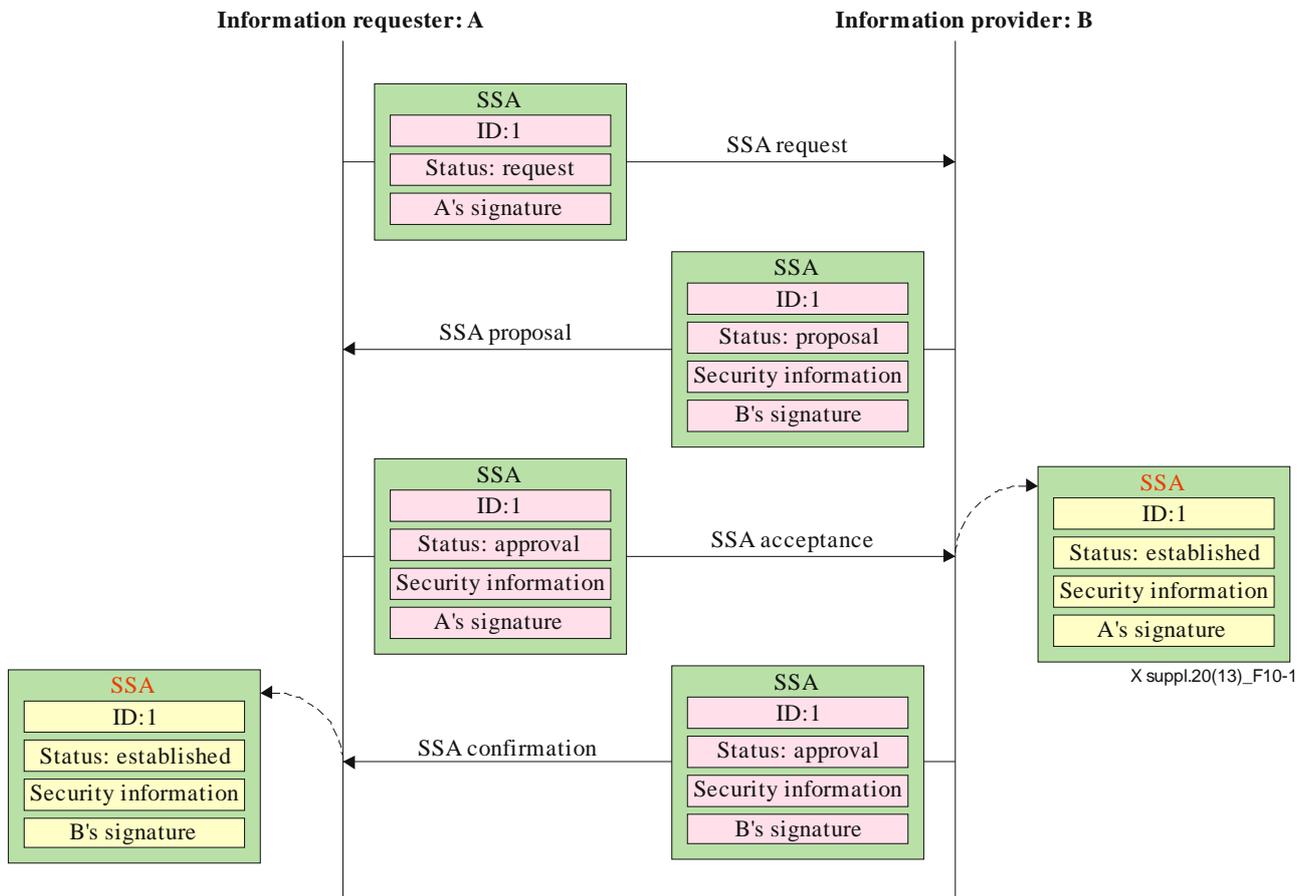


Figure 10-1 – Scenario for the successful negotiation of SSA

10.2.2 The unsuccessful negotiation of SSA

The unsuccessful negotiation of SSA is initiated by either an information requester or an information provider.

Figure 10-2 depicts the exchange of SSA negotiation messages by rejecting the SSA request.

- 1) An information requester transmits a SSA to an information provider using a SSA request message.
- 2) If the information provider decides that it cannot support the received SSA, it sends back a SSA rejection message that includes the identifier of the SSA to reject.

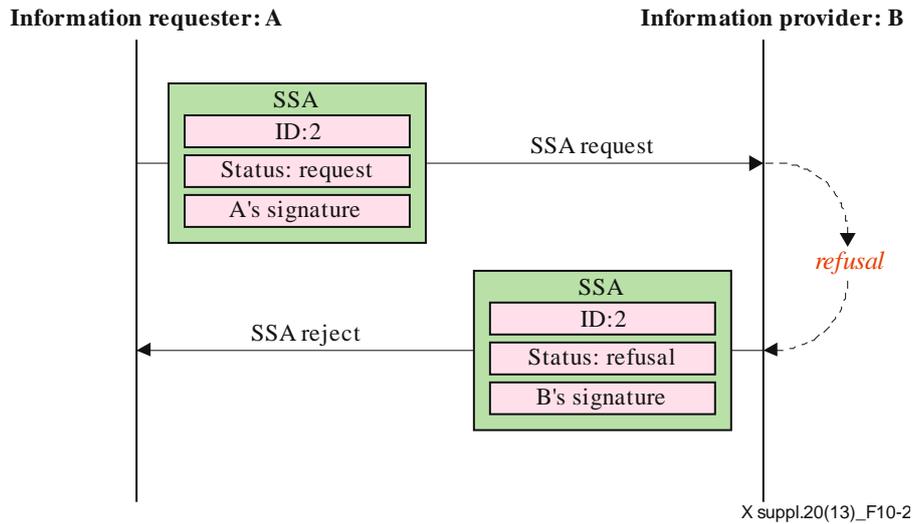


Figure 10-2 – Scenario for the unsuccessful negotiation of SSA by rejecting the SSA request

Figure 10-3 depicts the exchange of SSA negotiation messages by rejecting the SSA proposal.

- 1) An information requester transmits a SSA to an information provider using a SSA request message.
- 2) The information provider makes a SSA that can satisfy the requirements of the information requester and then sends it back the information requester using a SSA proposal message.
- 3) If the information requester cannot accept the SSA that the information provider has sent, it makes the SSA rejection message that includes the identifier of the SSA to reject and transmits it to the information provider.

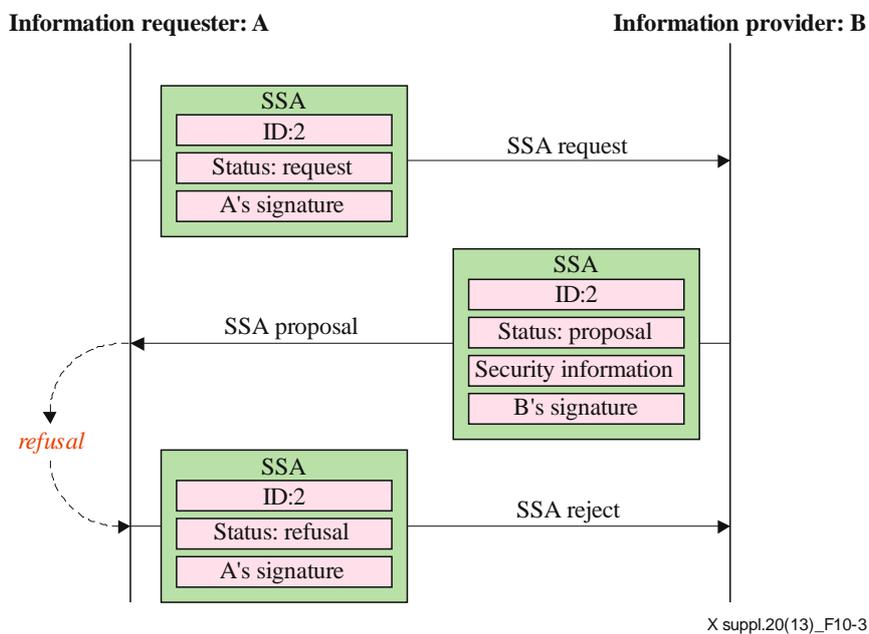


Figure 10-3 – Scenario for the unsuccessful negotiation of SSA by rejecting the SSA proposal

10.2.3 The cancellation of the established SSA

The cancellation of the established SSA can be initiated by either an information requester or an information provider.

Figure 10-4 depicts the exchange of SSA negotiation messages.

- 1) If one negotiating party wants to cancel an already established SSA, it makes the SSA cancellation message that includes the identifier of the SSA to cancel and transmits it to the other negotiating party.
- 2) If the negotiating party receives the SSA cancellation message, it deletes the SSA with the identifier that was specified in the received message and then sends back the SSA confirmation message.

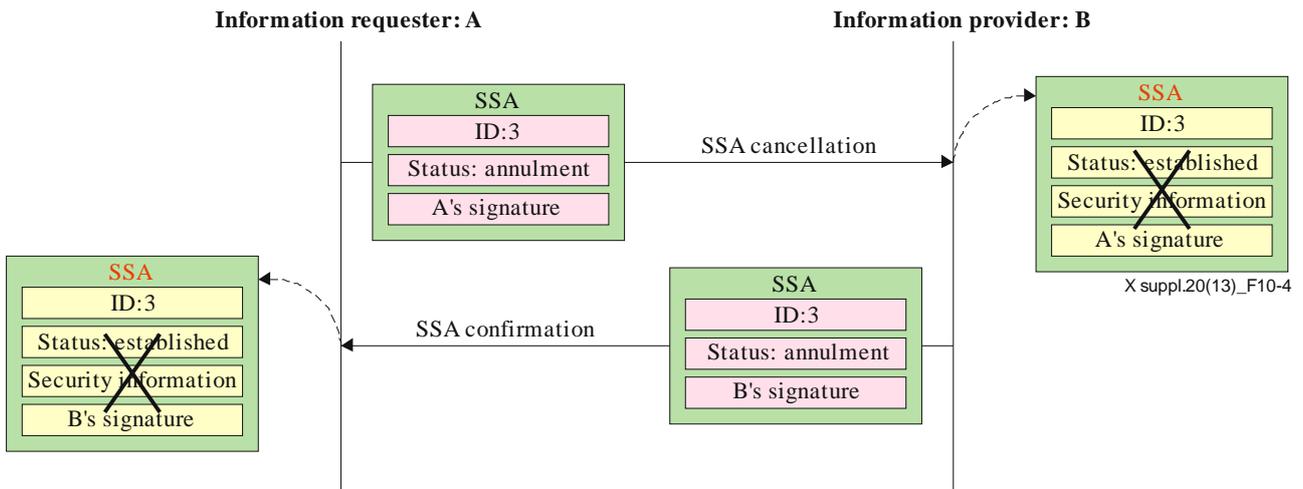


Figure 10-4 – Scenario for the cancellation of the established SSA

10.2.4 The modification of the established SSA

The modification of the established SSA can be initiated by either an information requester or an information provider.

Figure 10-5 depicts the exchange of SSA negotiation messages.

- 1) If one negotiating party wants to modify an already established SSA, it makes the SSA revision message that includes the identifier of the SSA to modify and transmits it to the other negotiating party.
- 2) If the negotiating party receives the SSA revision message, it modifies the SSA with the identifier that was specified in the received message and then sends back the SSA confirmation message.

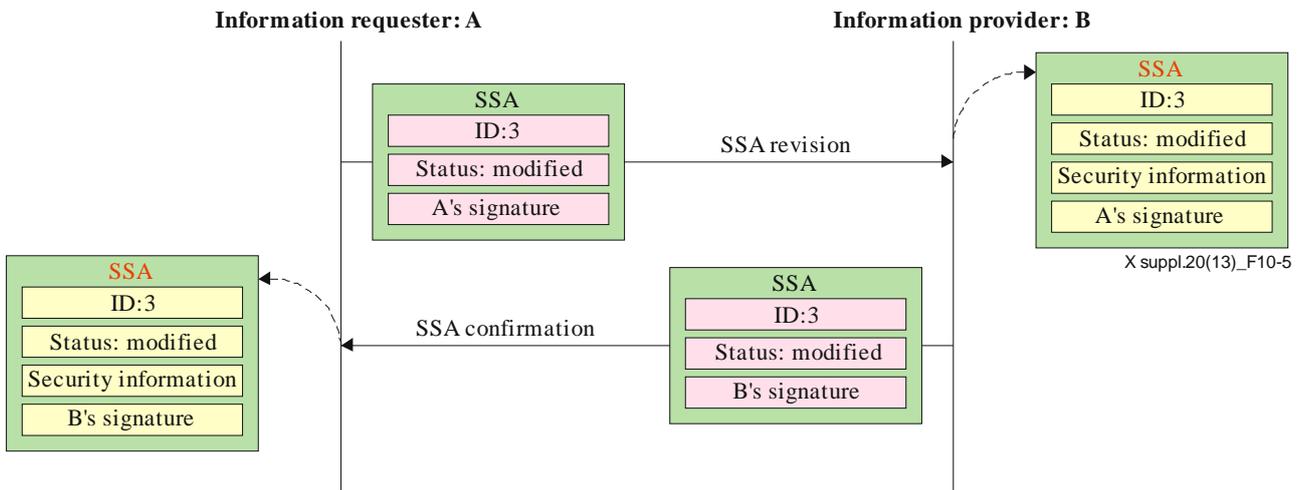


Figure 10-5 – Scenario for the modification of the established SSA

Appendix I

The example of security information sharing negotiation

I.1 Negotiation between the security management server and security agent

An example of security information sharing negotiation between cybersecurity entities is a negotiation between the security management server and security agent.

The security management server corresponds to the information requester. Its purpose is to globally monitor and control the network security situation by analysing cybersecurity information collected from security agents of other domains. The security agent corresponds to the information provider. Examples include the threat management system (TMS) and enterprise management system (EMS). It takes charge of detecting and managing cybersecurity attacks that occur within its domain.

Figure I.1 describes a scenario for security information sharing negotiation between the security management system and security agent. This scenario does not include the Discovery phase where the management system finds the security agent that can provide the information it wants.

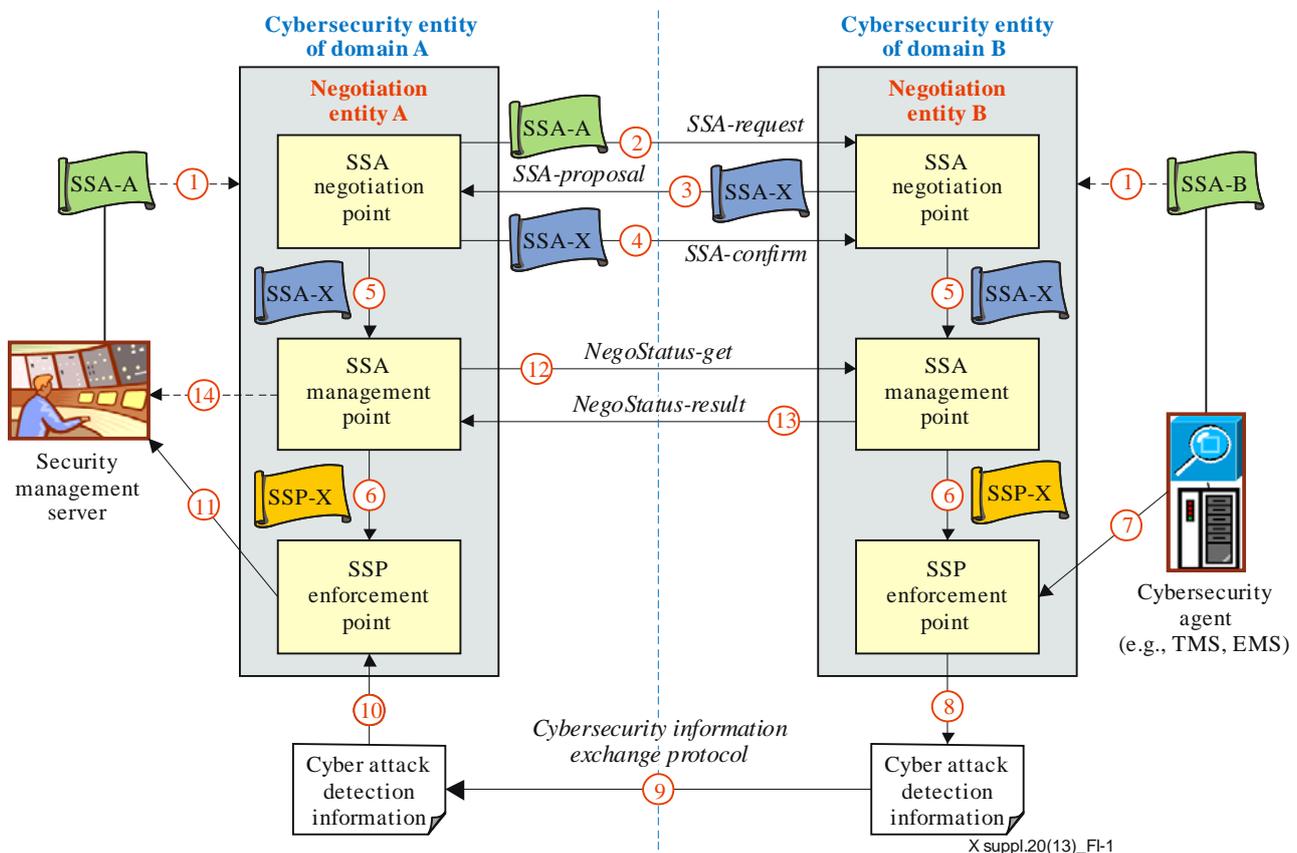


Figure I.1 – Negotiation between the security management server and security agent

The security information sharing negotiation between the security management system and security agent is as follows:

- SSA Negotiation Point-A defines SSA-A as requirements for security information sharing. SSA Negotiation Point-B defines SSA-B as requirements for security information sharing.
- SSA Negotiation Point-A sends a SSA request message with its own SSA (i.e., SSA-A) to the SSA Negotiation Point-B to initiate SSA negotiation.

- ③ If SSA Negotiation Point-B receives SSA-A from SSA Negotiation Point-A, it finds out and sends back a new SSA (i.e., SSA-X) that meets all the requirements of both SSA-A and SSA-B.
- ④ If SSA Negotiation Point-A accepts the SSA-X sent by SSA Negotiation Point-B, it replies with a SSA confirmation message.
- ⑤ SSA Negotiation Point-A gives the SSA-X to SSP Management Point-A. SSA Negotiation Point-B gives SSA-X to SSP Management Point-B.
- ⑥ SSP Management Point-A translates the SSA (i.e., SSA-X) into SSP (i.e., SSP-X) and provides SSP Enforcement Point-A with it. SSP Management Point-B translates the SSA (i.e., SSA-X) into SSP (i.e., SSP-X) and provides SSP Enforcement Point-B with it.
- ⑦ Cybersecurity agent (e.g., TMS, EMS) provides SSP Enforcement Point-B with cybersecurity information (e.g., cyber-attack detection information) whenever it detects a cyber attack.
- ⑧ SSP Enforcement Point-B processes the cybersecurity information received from the cybersecurity agent according to the SSP-X to generate information to provide to Cybersecurity Entity-A.
- ⑨ The information (e.g., cyber-attack detection information) generated by SSP Enforcement Point-B is delivered to Cybersecurity Entity-A using a cybersecurity information exchange protocol such as IDMEF or IODEF.
- ⑩ The information received from Cybersecurity Entity-B is forwarded to SSP Enforcement Point-A.
- ⑪ SSP Enforcement Point-A forwards the received information received to the security management server.
- ⑫ SSA Management Point-A requests information on the fulfilment state of SSA-X from SSA Management Point-B.
- ⑬ SSA Management Point-B replies to SSA Management Point-A.
- ⑭ SSA Management Point-A provides the security management server with information on the fulfilment state of SSA-X from SSA Management Point-B.

Bibliography

- [b-ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity*.
- [b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.
- [b-ITU-T X.1570] Recommendation ITU-T X.1570 (2011), *Discovery mechanisms in the exchange of cybersecurity information*.

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	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