8.7 Security Association

Intent

Define a structure which provides each participant in a Secure Communication with the information it will use to protect messages to be transmitted to the other party, and with the information which it will use to understand and verify the protection applied to messages received from the other party.

Also Known As

None known.

Motivation

Instantiating the Secure Communication pattern to protect messages in a communications channel is expensive and often slow, because it requires cryptographic operations to authenticate partners and exchange keys, and it often requires negotiating which protection services need to be applied to the channel. When two parties want to communicate securely they often want to send more than one message, but the cost of creating an instance of Secure Communication for each message would be prohibitive. Therefore it is desirable to enable an instance of Secure Communication to protect more than one message. Doing this requires storing a variety of security-related state information at each end of the communications channel. The Security Association pattern defines what state information needs to be stored, and how it is created during the establishment of an instance of the Secure Communication pattern.

Applicability

Use this pattern when:

- The Secure Communication pattern is used to protect messages in a communications channel.
- Some security parameters of the Secure Communication pattern are established by negotiation each time communication is initiated, rather than being pre-configured at each endpoint of the communication link out-of-band.
- It is desirable to send multiple messages over a secure communications channel without re-negotiating the security parameters of the channel for each message.

Structure

A Security Association may contain some or all of the following information:

- Association Identifier

  Used to distinguish this instance of the Security Association pattern from other instances.

- Partner Identifier

  Used to identify the entity with which this instance of the Security Association pattern enables communication.

- Association Expiration

  The time after which the instance of the Security Association pattern is no longer valid and must not be used to protect messages.

- Cryptographic Keys

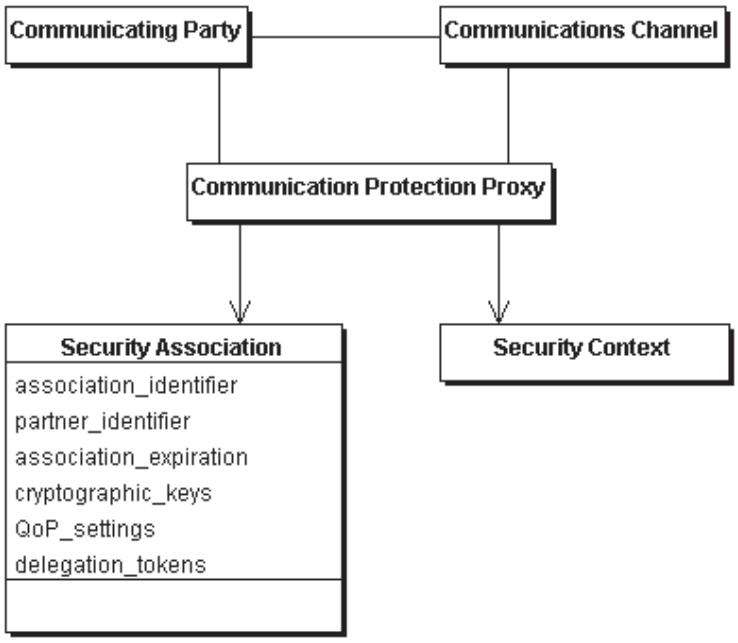
  Used by the Secure Communication pattern owning this instance of Security Association to protect messages.

- Quality of Protection (QoP) Settings

  Used by the Secure Communication pattern to determine which security services need to be applied to messages.

- Delegation Tokens

  Used by the Secure Communication pattern to implement delegation functionality.



Participants

- Protection Proxy

  Creates Security Associations and protects messages using information in Security Associations.

- Security Association

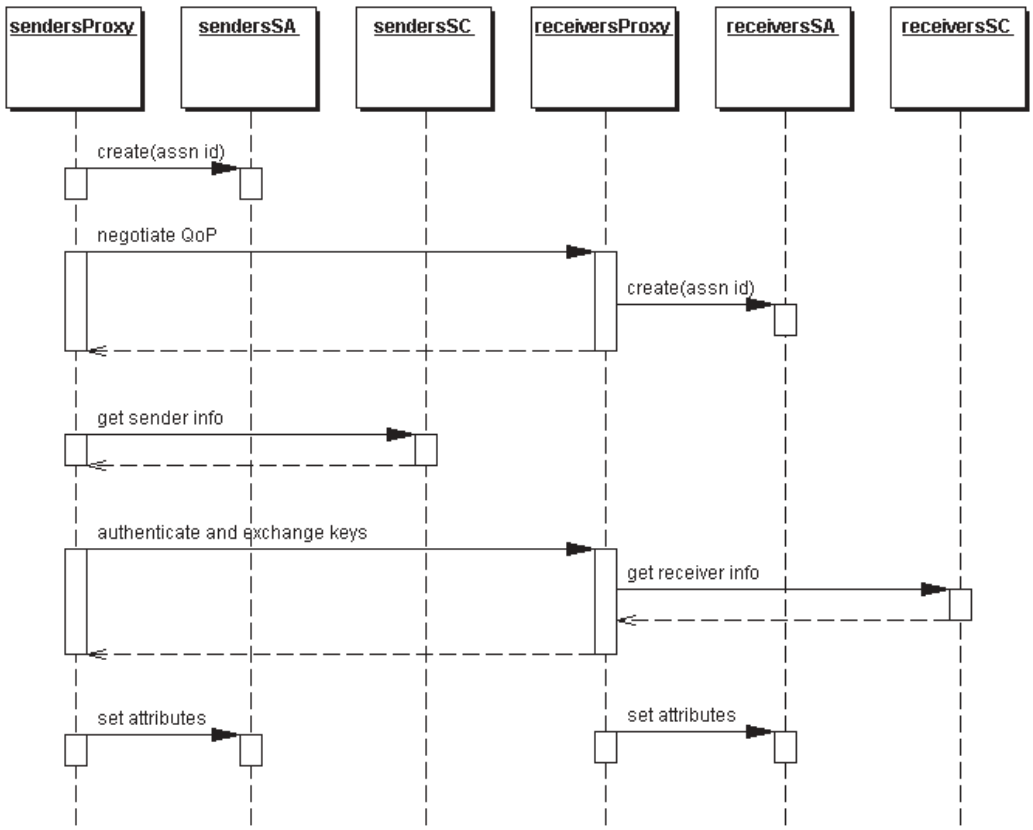
  Defines parameters used to protect messages.

- Security Context

  Contains information used to set up Security Association.

Collaborations

- Each Protection Proxy creates an instance of Security Association and assigns it a unique Association Identifier.
- The Protection Proxies determine the required QoP by reading configuration information or by negotiation with one another.
- If necessary, the Protection Proxies authenticate partner identifiers.
- If necessary, the Protection Proxies exchange session keys.
- Each Protection Proxy determines an expiration time for its Security Association (this will typically be a pre-configured interval, though it might be limited by a variety of factors including remaining key lifetimes).
- The sender's Protection Proxy transmits delegation tokens to the receiver's Protection Proxy, if appropriate.



Consequences

Use of the Secure Association pattern:

- Permits re-use of a single instance of Secure Communication to protect more than one message.
- Reduces the time required to set up Secure Communications by eliminating the need to re-negotiate protection parameters and cryptographic keys.
- Creates a data structure which stores cryptographic key material; this structure needs to be strongly protected against disclosure of keys and against modification of identity information associated with keys.

Implementation

Security Association can be used to protect both session-oriented and store-and-forward message traffic, but the negotiation and key distribution mechanisms differ for the two types of messaging environments. In general, Security Association instance information can be developed via online, real-time negotiations in session-oriented protocol contexts, whereas they typically need to be derived from configuration information, target object reference information, or information in a directory or other repository in non-session-oriented protocol contexts.

Known Uses

Generalized Security Service (GSS-API) [IETF RFC 1508 and others]; the Security Association instances are called ‘‘Security Contexts’’.

OMG CORBASecurity; Security Association instances are called ‘‘Security Contexts’’.

Related Patterns

Secure Communication [TG_SDP] uses Security Association to store information used to protect message traffic.

Security Context [TG_SDP] contains information used by Secure Communication to create Security Association instances.