Section 6: Domain Interaction Security Services

NOTE: This is an initial definition of these services and requires refinement and reworking to provide consistency.

6.1 Introduction

xxx introduced the concept of layered security services and xxx has described the basic security services in abstract terms, based upon the definitions within the ISO Security Framework. These basic security services require to operate within the context of a set of security information.

This chapter describes the Domain Interaction Security Services, the highest layer, which manage and propagate that security information context and are illustrated in Figure xxx.

Interactions between principals, both individuals and security domains, and a security domain is achieved through the creation of associations between the principal and the security domain. This requires the establishment of the set of security information, the security context, and its propagation with the tree of execution representing the service provision to the principal.

The services described in this section provide for:

- the creation of an association between a principal and a security domain. This is the responsibility of the Sponsor service within a security domain. In the case of an individual as a principal, the sponsor invokes the User Identification and Authentication service. In the case of an IT system component as principal, the sponsor services in both domains invoke a Secure Association Service.
- the management and propagation of the security information that is necessary for interactions both within and between security domains.

The rest of this subsection provides an overview of the domain interaction security services. The following subsections describe the services in more detail.

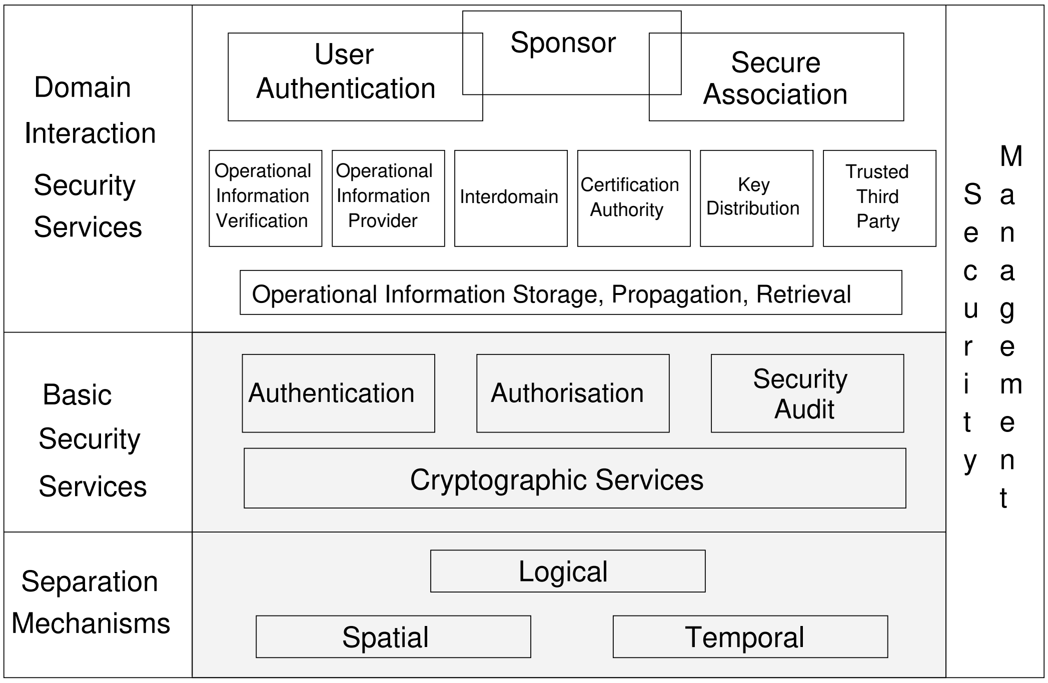

Figure 6-1 – Domain Interaction Security Services

Operational Information Provider Service

This service supports the aquisition of operational security information. The operational security information may include authorisation information (ACI) and audit event discrimination information. This service may provide initiator information, target information and action information. The information may be presented in the form of a security certificate or security token.

NOTE: The Operational Information Provider Service may support the provision of other contextual information in addition to security information, for example cultural information such as locale but this is not considered further within this framework.

Security Information Verification

This service verifies the authenticity of security information recieved by a security domain. In respect of the authorisation service it comprises the verify action ADI function.

Interdomain

In order for security domains to interact then it is necessary for them to exchange security information under the auspices of a secure interaction policy. The semantics and syntax of the information and policy in both domains may differ. An interdomain service provides for the translation of the representation as security information in one domain into a representation as security information in the other domain.

Certification Authority

The component services provided by a Certification Authority (CA) are:

• produce certificates (for example, as defined in ISO-9594-8/X.509) for public keys presented to it by bona-fide key holders

• produce revocation lists as requested and according to policy.

• satisfy itself as to the validity of a request before actioning the request.

• certify entities' public keys (which includes the public keys of other CAs, thus enabling hierarchies of CAs to be established)

• maintain and publish a list of revoked certificates.

Key Distribution

The purpose of key distribution is to securely transmit cryptographic keys between entities maybe located on different platform domains.

Trusted Third Party Services

These are digital signature and timestamp services in support of notarisation and non-repudiation requirements.

Operational Information Storage, Propagation and Retrieval

The security service model described in xxx refers to the storage, propagation and retrieval of operational security information, that is, the security context information for each security service. This requires services that support the following:

• the binding of a set of security information representing the security context of a set of operations with the tree of execution supporting the operations.

• support for an operation supported by a tree of execution to retrieve the security context bound to that tree of execution, and extract components of the information therefrom.

Sponsor Services

A Sponsor service promotes a principal within a security domain. Sponsor services are deployed within each security domain. The sponsor service is responsible for managing the formation of associations between its own security domain and other security domains. Another term for the sponsor service within service domains is association management service.

A platform domain that supports direct interaction with users has a sponsor service provided by a dedicated service domain. This service domain is referred to as a User Sponsor service.

User Authentication Services

User authentication services support a range of procedures and mechanisms suitable for the identification and authentication of users. Most of these mechanisms are based on cryptographic techniques.

The user authentication service is used by user sponsor services. The user authentication service may be required to provide a full security context for the user. In this case the operational information provider services are also used.

Secure Association Services

Secure association services are responsible for forming associations between security domains in accordance with the appropriate secure interaction policy. This requires:

- the propagation of the operational security information from the initiating domain to the target domain
- checking the authorisation for the association formation. This may require authentication of the initiating and target platform domains as well is the service domains
- invoking the appropriate interdomain services
- invoking a communication integrity and confidentiality services as required by the secure interaction policy.

6.2 Operational Information Provider Service

This service supports the aquisition of security information. The security information may include access control information and audit event discrimination information for initiators, targets and actions.

NOTE: The Operational Information Provider Service may support the provision of other contextual information in addition to security information, for example cultural information such as locale but this is not considered further within this framework.

6.2.1 Management Services

The management related operational information services comprise:

- Install operational security information
- Modify operational security information
- Revoke operational security information
- List operational security information
- Disable operational security information provider service
- Re-enable operational security information provider service

6.2.2 Operational Services

The operational related operational information services comprise:

- Acquire operational security information

This service provides a set of operational security information such as ACI. The initiator is required to assert its identity and maybe its privileges, for example by presenting exchange AI or ACI, to obtain the service.

If an initiator is requesting ACI appropriate to a target it may also be required to assert the identity of the target.

- Modify operational security information.

This service permits an initiator to modify an existing set of operational security information, for example to select a set of ADI from ACI use with a particular action and target. An example is the selection of a set of access rights to delegate to another principal, a server service domain, which is required to act as proxy for the initaior.

- Release operational security information

This service notifies an operational information provider that a set of operational information previously issued is no longer in use.

6.3 Operational Information Verification

This service verifies the authenticity of operational security information recieved by a security domain. For the authorisation service it comprises the verify action ADI function. This service is invoked to verify ACI before it is submitted as verified ACI to the authorisation service (access decision function ADF).

This service generally maps to the verification of the authenticity of a security certificate or security token. When the security information is stored or propagated by a domain that the target domain trusts to maintain the integrity of the information then this service may map to a null service. An example is when a service domain trusts the platform domain storing security information as process attributes to maintain their integrity.

Operational Services

The operational related initiator attribute services comprise:

- Verify operational security information

6.4 Interdomain

In order for security domains to interact then it is necessary for them to exchange security information under the auspices of a secure interaction policy. There are different cases regarding the interpretation of the security information exchanged:

- The semantics and representation of the information and policy in both domains are identical. In this case translation is unnecessary.

- The semantics of the information and policy are identical, but not their representation. In this case a syntax translation is necessary.

For example two systems may both use uids to identify users and represent their access privileges but a user may be allocated two different uid values on each system, it is then necessary to map a uid value on an initiating system to a uid value on the target system.

- The semantics and the representation of the rules of each of the security domains are different. This means that an agreed set of rules needs to specify how the security information and policy of one domain can be translated into the security information and policy of the other domain because the description method is different and syntax translation is necessary.

A simple example is interactions between a security domain that supports access control service and a security domain that does not. This will require the security domain that supports access control to assign an appropriate set of access control information to all data exchanged with the security domain that does not support access control.

6.4.1 Interdomain Management Related Services

The interdomain management related services include:

- Install interdomain mapping
- Modify interdomain mapping
- Delete interdomain mapping

- Disable interdomain service
- Re-enable interdomain service

6.4.2 Interdomain Operational Related Services

The interdomain operational related services are invoked as part of the secure association service which therefore protects applications from the details of this service.

6.4.3 Special Instances of Interdomain Services

There are two special instances of interdomain services:

- the interaction between service domains and platform domains. A service is required to map the representation of security information within the service domains, for example, as held within a security certificate, to a representation meaningful within the platform domain, that is, as process attributes. This service is invoked by the sponsor service, not by applications directly.
- the conversion of security information from an IT system representation, for example a uid, to a human-readable representation, that is a text string.

This service is used by applications and therefore requires an operational service interface. The management interfaces for this service are provided by the install and modify services appropriate for the particular operational information. Thus the management service that installs the mapping for initiator ACI is the install initiator ACI service.

6.5 Certification Authority

The function of a Certification Authority (CA) is:

- Produce certificates (for example, as defined in ISO-9594-8/X.509) for public keys presented to it by bona-fide key holders
- to produce revocation lists as requested and according to policy.
- to satisfy itself as to the validity of a request before actioning the request containing it.
- to certify entities' public keys (which includes the public keys of other CAs, thus enabling hierarchies of CAs to be established)
- Maintain and publish a list of revoked certificates

There can be many CAs, and one CA may serve several domains. The CA is typically off-line, but a registration authority (RA) component can act as an online front-end to the CA. The function of the RA is to receive requests and dispatch them to the CA for actioning, then return the appropriate response to the initiator

The CA may be used to certify the public keys of on-line security services such as an Operational Information Provider Service and Key Distribution Service. It may be also used to certify the long-term public keys of any other entity, for example an interdomain service, or security-aware application.

A given CA may serve several domains. To allow domains under different CAs to interwork, domains may exchange uncertified public keys. Additionally, or alternatively, a given key may be certified by more than one CA. CA hierarchies and cross-certification may be used as determined by policy.

6.5.1 Certification Authority Services

CA/RA Services

Create-Certification

Create a certificate binding the specified identity and public key.

Revoke-Certification

Revoke the certification, and hence the identity specified by the certificate.

Cross-Certify

Create a certificate binding the specified CA and public key.

6.5.2 Certification Services

Get-Certificate

Retrieve a certificate (locally or from a directory)

Initate-Certification-Path-Construction-Context

Set up a context for constructing a certification path

Construct-Certification-Path

Construct a certification path for the specified domain. If Construct-Certification-Path is called, but it has insufficient information to complete the path, then it returns the name of a key holder or CA that the caller should obtain certificates for.

Terminate-Certification-Path-Construction-Context

Terminate a certification path construction context

The public key management service provider uses the certification path construction functions to construct a certification path. These functions interrogate the trust criteria set up using the trust-path functions when deciding how to construct a path. All these functions work both with a flat certification model, and also a hierarchical certification structure with cross-certificates.

NOTE: This example will probably be moved to an annex.

Consider the following system: - in MEGA CORP, there are CAs called MEGA-CORP, MEGA-ADMIN, and MEGA-HUMAN-RESOURCES - in BIG INC, there are CAs called BIG-INC, and BIG-MANAGEMENT - in LEAN CO, there is one CA called LEAN-CO, and a PAS called LEAN-SALES

The following certificates exist: - BIG-INC certifies BIG-MANAGEMENT - BIG-MANAGEMENT cross-certifies LEAN-CO - LEAN-CO certifies LEAN-SALES (a PAS) - MEGA-CORP certifies MEGA-ADMIN - MEGA-ADMIN cross-certifies LEAN-CO - MEGA-HUMAN-RESOURCES has no cross-certificate links with the others.

Suppose an BIG-INC domain which trusts BIG-MANAGEMENT (but no other CA, unless cross-certified by BIG-MANAGEMENT) calls Get-Public-Key for the PAS called LEAN-SALES. Get-Public-Key would work as follows (not all parameters and details are shown): (1) Set up a certification path construction context with Initate-Certification-Path-Construction-Context, specifying the name of the remote entity (LEAN-SALES) (2) Repeatedly call Construct-Certificate-Path until a path is successfully constructed. The caller then obtains the certificates, and calls Construct-Certification-Path again (3) Terminate the certification path construction context with Terminate-Certification-Path-Construction-Context

In the scenario above, the sequence of calls would work out as follows. Certificates are denoted as [<ca_name>, <owner_name>], e.g. [LEAN-CO,LEAN-SALES] is a certificate for LEAN-SALES signed by LEAN-CO.

Uncertified keys are denoted as ["" , <owner_name>] - i.e. the ca_name is blank. It is assumed that this is the first time a path has ever been constructed by the caller - and hence the structure of the hierarchy has not yet been learned.

Construct-Certificate-Path("") => "LEAN-SALES" Get-Certificate("LEAN-SALES") => [LEAN-CO,LEAN-SALES]

Construct-Certificate-Path([LEAN-CO,LEAN-SALES])
=> "LEAN-CO Get-Certificate("LEAN-CO")
=> [MEGA-ADMIN,LEAN-CO] , [BIG-MANAGEMENT, LEAN-CO]

Construct-Certificate-Path([MEGA-ADMIN,LEAN-CO], [BIG-MANAGEMENT, LEAN-CO])
=> "MEGA-ADMIN" Get-Certificate("MEGA-ADMIN")
=> [MEGA-CORP, MEGA-ADMIN]

Construct-Certificate-Path([MEGA-CORP,MEGA-ADMIN])
=> "BIG-MANAGEMENT" Get-Certificate("BIG-MANAGEMENT")

=> ["" , BIG-MANAGEMENT]

Construct-Certificate-Path(["" , BIG-MANAGEMENT])
=> PKM_CPC_COMPLETE and the final path is:
[LEAN-CO, LEAN-SALES] [BIG-MANAGEMENT, LEAN-CO] ["", BIG-MANAGEMENT].

A public key management service provider caller may repeat this process twice, the first pass draws certificates from local storage, the second pass draws from the "freshest" source of information (e.g.: the directory). A second pass is only performed if the first pass doesn't succeed in forming a path. (The second pass is shown above).

6.6 Key Distribution

The purpose of key distribution is to securely transmit cryptographic keys between entities maybe located on different end-systems.

For situations where cryptographic techniques must be utilised in order to set up and maintain secure communication, a key distribution mechanism is involved as part of the process of establishing of a secure association between communicating peers.

Different mechanisms for distributing keys exist. These include:

— symmetric

— asymmetric

— manual

Key distribution service providers will typically utilise the underlying services of the cryptographic support and public key managemt facilities.

The operational and management services defined for the secure association service insulate the users of key distribution services from the details of the mechanism.

6.7 Operational Information Storage, Propagation and Retrieval

The security service model described in xxx refers to the storage, propagation and retrieval of security context information for the security service. This requires services that support the following:

• the binding of a set of operational security information representing the security context of the operation with the tree of execution supporting the operation.

• the provision of a capability for a component of the tree of execution to retrieve the operational security context, or a handle to the operational security context, bound to that tree of execution to use directly as part of an operation or to extract component information therefrom.

Within a platform domain such support requires the use of the platform domain services. Between service domains, the service domains themselves may provide for such propagation using the secure association service.

6.7.1 Management Related Services

There are no management related aspects of this service.

6.7.2 Operational Related Services

The operational related services include:

Bind Operational Information This service binds operational security information to an execution tree.

Retrieve Operational Information This service retrieves operational security information that has been bound to an execution tree.

Extract Operational Information This service extracts particular security attributes from a set of operational security information.

6.7.3 Implementation

Within a platform domain this service is typically supported by storing operational security information as process attributes. These process attributes are propagated to new processes by inheritance from the parent process.

It is possible for the retrieve and extract services to be combined, as in the process attribute example above with a retrieve operation for each security attribute type, as in the system calls getuid, getgid.

In the case when service domain operational information is added to a system, for which no support is provided by the platform domain, an indirect method of support for operational information propagation is used. As an example, the service domain operational information may be held in a file which is associated with a process attribute, typically a uid. Access to the file is protected by the normal platform domain authorisation services.

This method of propagation may not guarantee the uniqueness of the binding of the operational information to a particular execution tree as other execution trees may possess access rights to the file. In addition, any execution tree with the capability to assume resposibility for platform domain access control policy, for example administrative processes, are able to access such a file.

6.8 Sponsor Services

NOTE: This subsection needs further thought and work.

A Sponsor service promotes a principal within a security domain. Sponsor services are deployed within each security domain. The sponsor service is responsible for managing the formation of associations between its own security domain and other security domains. Another term for the sponsor service within service domains is Association Management Service.

A platform domain that supports services for individuals has a sponsor service provided by a dedicated service domain. This service domain is referred to as a User Sponsor service.

Sponsor services may provide top level control capability exercising control and selection of the use of services within the domain. For example, the top level control capability in a database server within some distributed application. Here, the sponsor service's principals are the application's client components.

Sponsor services are responsible for:

• The initial identification and authentication of the principal, for this purpose the Sponsor uses the appropriate Authentication service. In the case of the User Sponsor this would be the User Authentication service.

• Establishing one or more security contexts for the principal - The security contexts contain security attributes to be used in subsequent security operations; typically these attributes are: principal identification, audit identification and access control information. The Sponsor services use the Security Information Provider Service to acquire the relevant security information based on the principal's identity.

This may include establishing a platform domain security context represented by set of process attributes.

• Facilitating interactions between the principal and the other services within the security domain - In certain cases the Sponsor may be assigned responsibility to mediate access to these services; in this respect it operates as an Access Control Enforcement Function.

The Sponsor is often responsible for the switching of security contexts on behalf of the principal in order to support different operations. Where these operations result in a request to propagate the tree of execution to another security domain the Secure Association service is invoked to form the necessary secure association and pass the security context to that domain. An example is a secure X Window system that permits a user to select the initiator ADI (such as uid, gid and security label) to be used to invoke an application.

6.9 User Authentication

6.9.1 Introduction

Users are a type of entity that require access to an IT system but are physically distinct from it. In order to utilise the services of an IT system a user must create an association between himself as a principal and the IT system. In order to create such an association a user must successfully complete the user authentication process, specifically identify himself to the system and have that identity authenticated. The process of user authentication may include the invocation of other security services such as authorisation in that the success of the authentication process may depend upon the context of user interaction such as time of day, location of terminal or workstation.

On successful authentication the user sponsor service is presented with a set of exchange AI (also commonly referred to as credentials) with which the user's identity may be asserted within the system. The credentials may include additional information such as period of validity. In the extended model of user authentication, described in xxx, the credentials may include additional operational security information such as ACI and audit identity and audit discrimination information.

NOTE: Note that the User Authentication services may be required to provide support for the mutual exchange of authentication credentials. That is, the user requires the system to authenticate itself to him. This can be considered to be a very user-visible implementation of a trusted path.

6.9.2 Basic User Authentication Service Model

Figure xxx illustrates the basic user authentication service model followed by an explanation of the components of the user authentication process.

Platform domains, through which users interact with an IT system, are required to direct all initial user contact with the system to a user sponsor service domain. The system security policy may require that this interconnection is by a trusted path.

The purpose of the trusted path is to provide assurance of the integrity and confidentiality of the communication between the user and trusted components of the system. An authentication trusted path is a platform domain supported mechanism that provides the user with assurance that communication is only with the user sponsor. It also provides the user sponsor with assurance that it is communicating directly with a user I/O device.

The user sponsor service is responsible for promoting the user to the authentication service and, if successfully authenticated, to promote the authenticated user to other services of the system.

The user sponsor service solicits claim authentication information from the user and submits this, together with contextual information such as location, if required by the system security policy, to the authentication service domain as

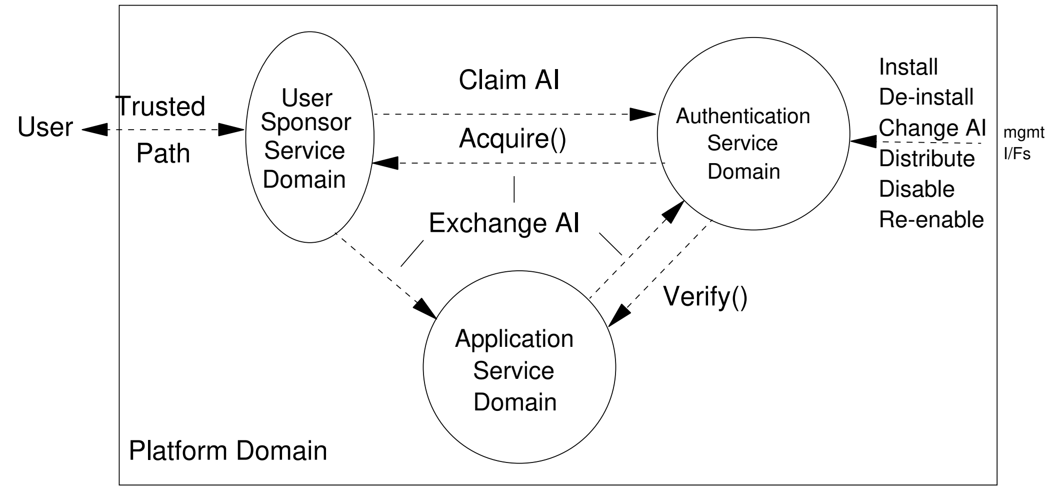

Figure 6-2 – Basic User Authentication Service Model

part of an Acquire AI operation. If user authentication is successful, Exchange Authentication Information, possibly in the form of an authentication certificate, is returned by the authentication service to the user sponsor.

The claim AI used to support human user authentication may include passwords, magnetic stripe card or smart card, and physical characteristics such as finger-print or hand written signature.

The exchange AI, may be represented by an authentication certificate; it can then be submitted by the user sponsor to an application service domain in assertion of the user principal's identity. The application service domain may invoke a verify AI operation to verify the authenticity of the exchange AI submitted by the user sponsor. See

The exchange AI requires binding to the tree of execution initiated on behalf of the authenticated user and requires protection by the user sponsor, and any applica-tions to which it is submitted as it provides assertion of the user principal's iden-tity. This binding of the exchange AI is achieved using the operational information store, propagate and retrieve services and depends upon support from the plat-form domain.

6.9.3 Extended Service Model

The security policy may also require a user to be assigned operational security information, such as a set of initiator ACI to provide authorisation to access services within the system and initiator audit information to support the security audit service. This assignment may be combined with the authentication process or invoked separately.

The authentication service and operational information provider services may be collocated and under a single security authority or may be under different security authorities.

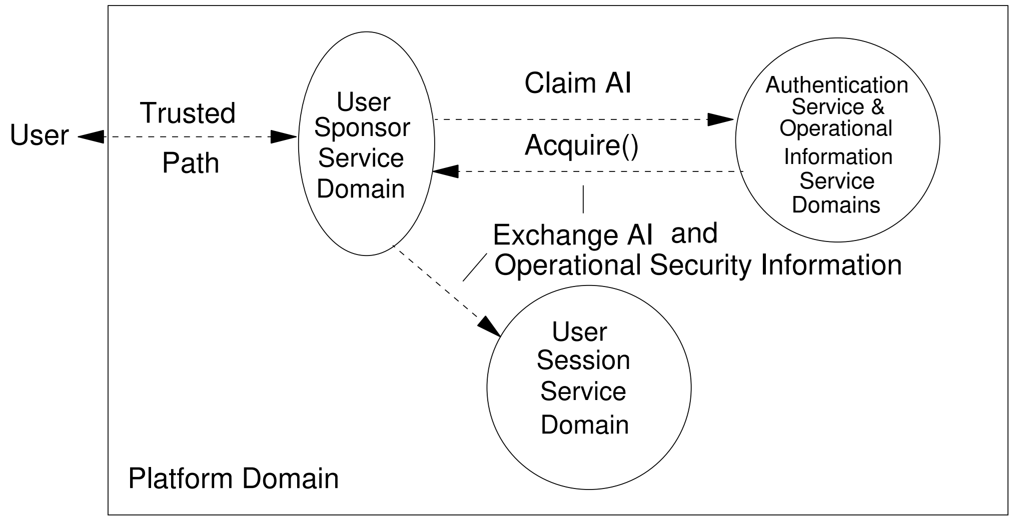

Figure 6-3 – Extended User Authentication Service Model

In the traditional local platform user authentication model the exchange AI is returned as an authenticated identity together with a set operational security information ,initiator ACI and audit control information, if the security policy requires, as a set of process attribute values. The user sponsor invokes a user session service domain to which the returned process attributes are applied to the process group leader of the user session domain and subsequently inherited by all processes invoked within the user session service domain. That is, the authenticated control information is bound to the entity that represents the user within a user session service domain (the tree of execution within the session) and is propagated by inheritance as process attributes.

6.9.4 Management Services

The management related services include:

- Install User, which may comprise enrollment, testify, and validate
- De-install User, which may comprise invalidate, notify, unenroll
- Modify User AI
- Distribute User AI
- Disable and Re-enable User
- List Users, installed, disabled or active.

These services require both APIs and HCIs to be defined.

These management services will also support the interdomain service providing a mapping between the internal representation of a user and a human-readable name.

6.9.5 Operational Services

The operational related services include:

- Solicit User Claim AI
- Generate Exchange AI
- Verify Exchange AI.

6.10 Secure Association Service

NOTE: This section has been partially reworked in the context of the Domain Interaction Services added since it was originally drafted. This reworking is incomplete.

6.10.1 Introduction

An essential part of the operation of an IT system is the formation of associations. The section on User I&A described the secure formation of associations between Users as principals and the IT system. This section deals with the formation of secure associations between peer entities within the IT system, these entities are the sponsors within security domains.

The creation of a secure association is subject to the secure interaction policy configured for associations between the specific security domains by prior management action using the management related secure association services. The operational-related secure association services actually create the association between the security domains. The establishment of a secure association depends upon several other security services:

• Authentication and operational information provider services to provide a set of initiator operational security information in the form of initiator credentials.

• Operational information provider services to generate operational security information in the form of a secure association context to be exchanged between the entities.

• Communication security services, if available, to establish a communication channel for the association that meets the requirements of the interdomain policy with respect to communication confidentiality and integrity protection.

• Authorisation services to confirm that the requested association is permitted under the interdomain policy.

• Interdomain service to map the semantics and syntax of security attributes if the association is between services located in security domains with different security attribute semantics and syntax.

The creation of an association between one set of entities within an IT system of necessity requires the formation of an association between entities that contain the primary associating entities. Thus an association between service domains also requires the formation of an association between platform domains (unless collocated within a single platform domain). The creation of the association is subject to the secure interaction policies applicable to each of the constituent associations required. This equates to associations being formed, and secure interaction policy requirements applying to different communication service layers (for example layer 7 and layer 4 of the OSI model).

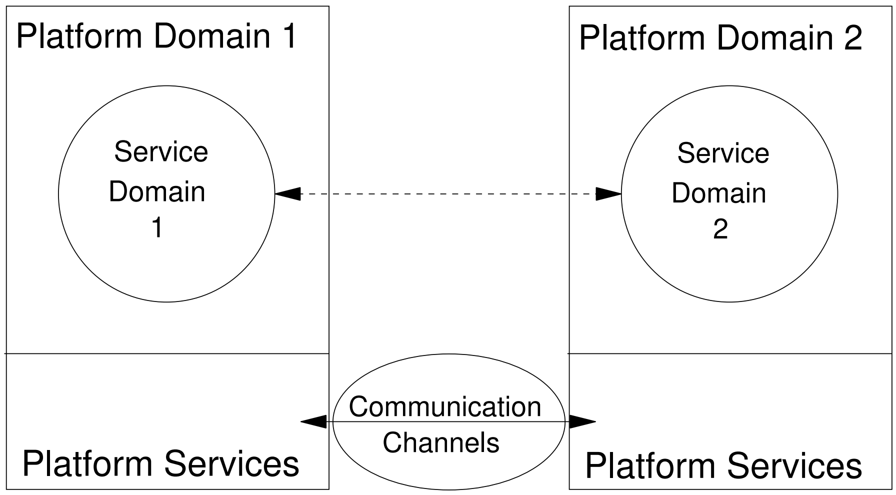

Figure 6-4 – Layered Nature of Associations Between Security Domains

6.10.2 Basic Service Model

The stages in the creation of a secure association are illustrated in the following figure.

1. Establish Secure Interaction Policy

   An association may only be created within the bounds of a secure interaction policy established for the formation of a particular association (or set of associations). The detailed rules of the secure interaction policy must be interpreted into a set of criteria which need to be configured within the SMIBs of the interacting security domains by management action. This includes any requirements for an interdomain service to map the syntax and semantics of security attributes between their representations within each security domain, or to a common interchange format.

2. Initiator Credentials

   A sponsor of a service domain initiating a secure association is required to possess credentials. This is:

- operational security information such as exchange AI or initiator ACI appropriate to the principal to whom the service domain is providing service,

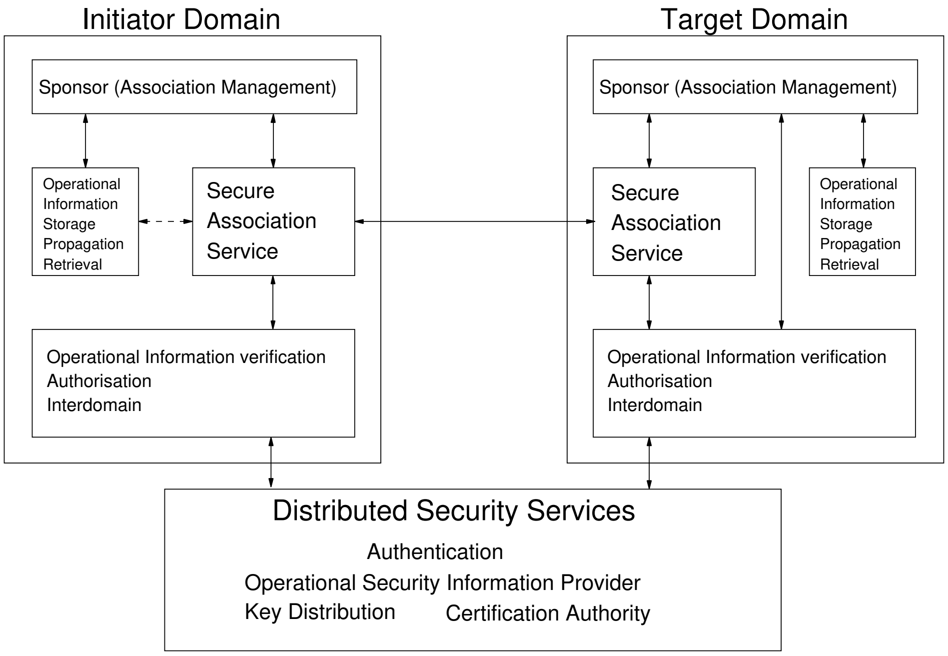

Figure 6-5 – Basic Secure Association Service Model

- operational security information such as exchange AI or initiator ACI appropriate to the service domain itself as a principal,
- may be both.

Operational security information appropriate to a user as principal is derived by the user sponsor service as part of the user authentication process and propagated securely within the user session service domain operating on behalf of that user principal. Security information appropriate to a service domain itself as a principal is established when the service domain is created from initial information associated with that service domain by the platform domain (for example, service domain identity, cryptographic key or security certificate).

A service domain, providing services on behalf of many principals may possess more than one set of initiator security information and may select which of the sets of initiator security information is to be used for the creation of a particular association.

The default credentials associated with the tree of execution of the initiating security domain may be used, or the initiator may request to modify the credentials, for instance to support delegation of some of the initiator's access rights to the target.

3. Generate Association Security Context

   The initiator invokes the generate service of the secure association service to generate the operational security context of the association. The initiator may specify particular aspects of the security context, or may accept, or have imposed, specified defaults under the secure interaction policy. This includes specification of the Cryptographic Quality of Service (confidentiality and integrity Services) and the strength of authentication mechanisms to be used.

   The operational security context for the association is returned to the initiating sponsor as a security token.

4. Initial Security Information Exchange

   If the generation of an association security context is successful, the initiator sends the security token representing the requested security context for the association to the sponsor within the target service domain.

5. Verify Association Security Context

   The target service domain sponsor invokes the verify security context service of the secure association service, with the security token received from the initiator as a parameter. The verify security context service:

   - verifies the authenticity of the security token by invoking the operational information verification service, this may in turn require the invocation of certification authority services if a certification chain has to be verified (see certification authority example).
   - if necessary, identifies the interdomain service appropriate to the association.
   - establishes the communication security services required by the association security context.

   and returns an association security context to the target sponsor.

6. Authorise Association

   The sponsor, having verified the authenticity of the association security context:

   - verifies the identity of the initiator,
   - verifies the authorisation for the target to form an association with the initiator with the requested security context. This is based upon operational security information included within the association security context and security information possessed by the target. Verification of authorisation may include verification of the chain of delegation used to request this association.

7. Responding Security Information Exchange

   If the association is authorised, the target sends the security token generated by the target verify security context operation to the initiator. This conveys security information regarding the acceptance or otherwise of the originally specified security context and levels of service to be used within the secure association.

8. Verify Association Security Context

   If required, the initiator sponsor invokes the generate security context service of the secure association service with the security token returned by the target service domain. This service performs the same functions as the verify association security context service in the target domain but for the association security context returned by the target domain sponsor.

9. Association Security Context Negotiation

   In some circumstances it may be necessary for the initiator and target to negotiate over some aspects of the security context establishment. In this case further calls to the operational related services of the secure association service and further exchanges of security tokens may occur.

10. Extract Security Information From Association Context

    In order to enforce security policy within its own security domain the target sponsor extracts the operational security information, such as access control information and audit identity and audit discrimination information, from the association security context. The target sponsor utilises the operational information storage, propagation, and retreival service to bind that operational security information with the tree of execution within the target domain. This may include mapping the operational security information to platform domain process attributes.

6.10.3 Management Services

Install Association

This service installs a permitted initiator/target pairing together with associated permitted security context as defined by the secure interaction policy. This includes the specification of aspects such as the cryptographic quality of service to be used within the association and the strength of authentication mechanisms to be employed. It may also include the configuration of an interdomain service to map the semantics (and maybe the syntax) of a set of security attributes within another security domain into the semantics (and syntax) of the security authority's own security domain.

Modify Association

This service modifies the details of a permitted association.

Uninstall Association

This service deletes a permitted association.

Revoke

This service revokes an existing association. It may be invoked if ACI on which authorisation for the association is based is itself revoked.

NOTE: Is this an appropriate service?

Disable

This service sets an association state such that it is unavailable for use.

Re-enable

This service terminates the disabled state of an association.

6.10.4 Operational Services

Generate Association Security Context

An initiator uses this service to request operational security information to be generated for use in creating an association with a specified target, or to verify a operational security information returned by a target. It requires input, either specifically or as default, of the initiating principal’s credentials. These credentials may include the delegation of some of the principals access rights to the target service domain for use in forming further associations to obtain service from further service domains.

Verify Association Security Context

A target uses this service to verify the authenticity of the association security context provided by an initiator.

Release Association Security Context

This service releases and deletes a security context created by a generate or verify service on termination of an association.

Extract Security Information

This service permits an initiator or target to extract security information from an association security context (for example security token) for use by other security services, for example AI, ACI, Audit Information.

6.10.5 Services Used Within An Association

Bind ACI to Message (Data)

An association security context may permit the transfer of data with varying ACI. This service permits an entity to specify the ACI to be bound to data to be transferred within an association.

Message Protection Services

These services invoke confidentiality and integrity services for specific messages and data to provide protection during transmission within an association. The specific cryptographic mechanisms used to provide these services are determined as part of the security context established for the association. (See Cryptographic Operations Services.)

The concept of cryptographic quality of service applied to operations within associations represents a service to support a trade off of performance against strength of security mechanism.

6.10.6 Impact of Secure Association Service on Primary Service APIs

Security Enforcing API / Security Unaware Caller

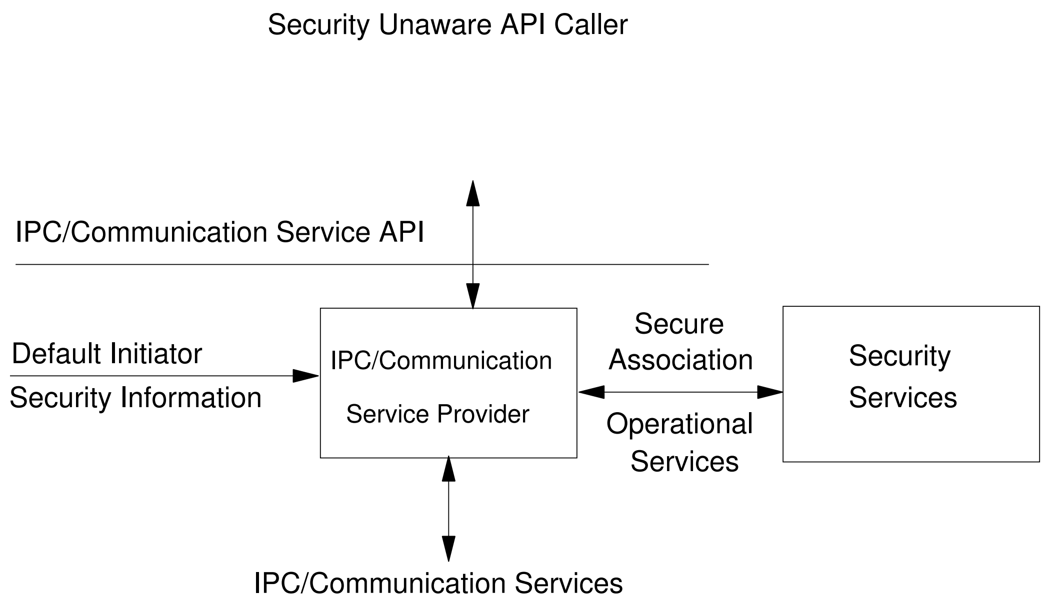

Figure 6-6 – Security Enforcing API / Security Unaware Caller

Security enforcing primary service APIs may provide no support for the caller of the interface to assume responsibility for any aspect of security association policy enforcement. The security policy is enforced entirely by the primary service provider. It is therefore suitable for supporting Security Unaware Callers.

A security enforcing API requires that the default operational security context (initiator's credentials) within which the primary service is invoked has been previously established, that is, the initiator ACI has been generated and made available to the primary service provider either by inheritance from a previous process or from previous actions of the current process. In addition, the Cryptographic Quality of Service has been previously defined, either by management action as a default or by use of a security service operational API.

Cryptographic Quality of Service Supporting API /Simple Security Selecting Caller

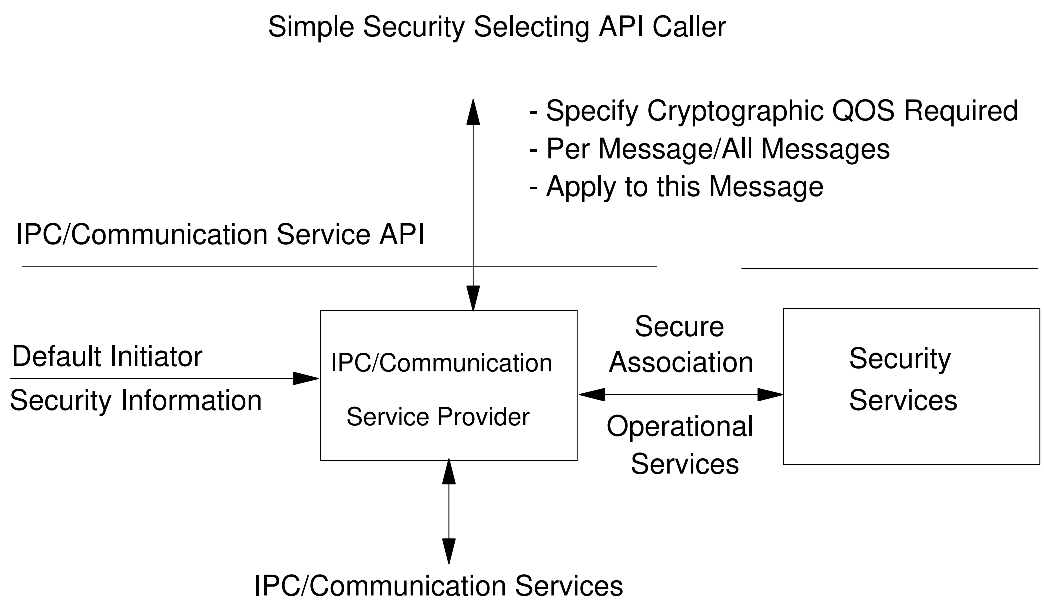

Figure 6-7 – Cryptographic QOS Supporting API / Simple Security Selecting Caller

Cryptographic Quality of Service Supporting APIs provides support for the caller of the primary service interface to select the strength of mechanism (Cryptographic Quality of Service) to be applied to information exchanged via an association.

The specification of the Cryptographic Quality of Service requires provision within the primary service APIs that create associations. This may include an indication of whether this applies to all messages or only messages for which the service is specified.

If Cryptographic Quality of Service is to be specified on a per message basis then a parameter specifying this needs to be included in each API that transmits and receives a message.

Security Context Supporting API / Security Selecting Caller

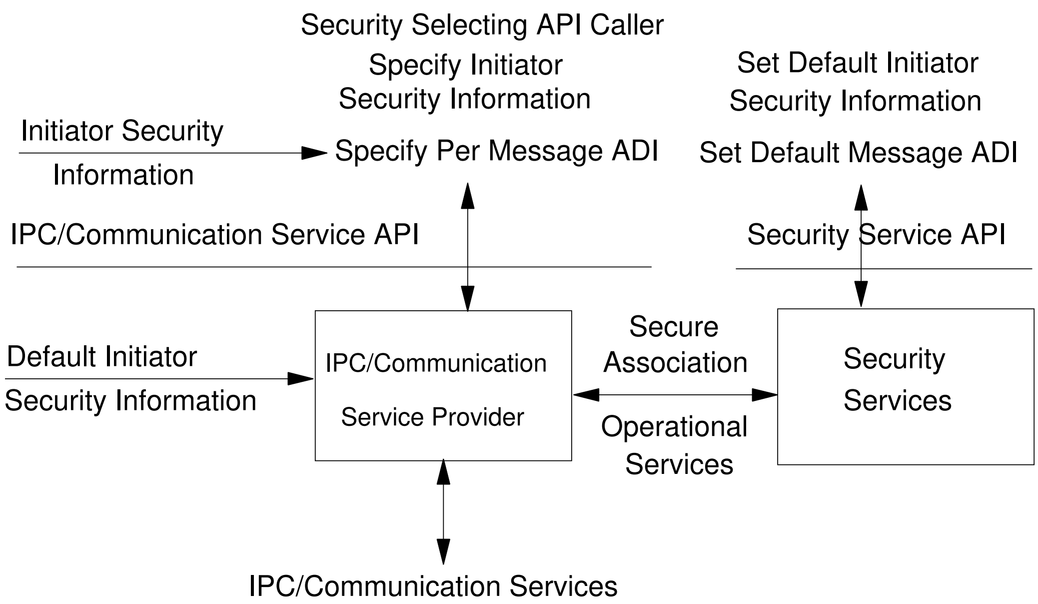

Figure 6-8 – Security Context Supporting API / Security Selecting

Security context supporting APIs specify the security context for the creation of an association or the binding of security information to information exchanged within an association. The caller of a Security Context Supporting API is responsible for manipulating security information. That is, it is responsible for manipulating the initiator credentials to be used in the establishment of the security context of a secure association or for the specification of the ACI to be bound with data exchanged within the association.

The specification of the operational security information may be supported in band, that is as parameters to the primary service API, or out of band, that is as separate interfaces that set default values to be applied to subsequent primary service API invocations.

Security Non-enforcing API / Security integrating Caller

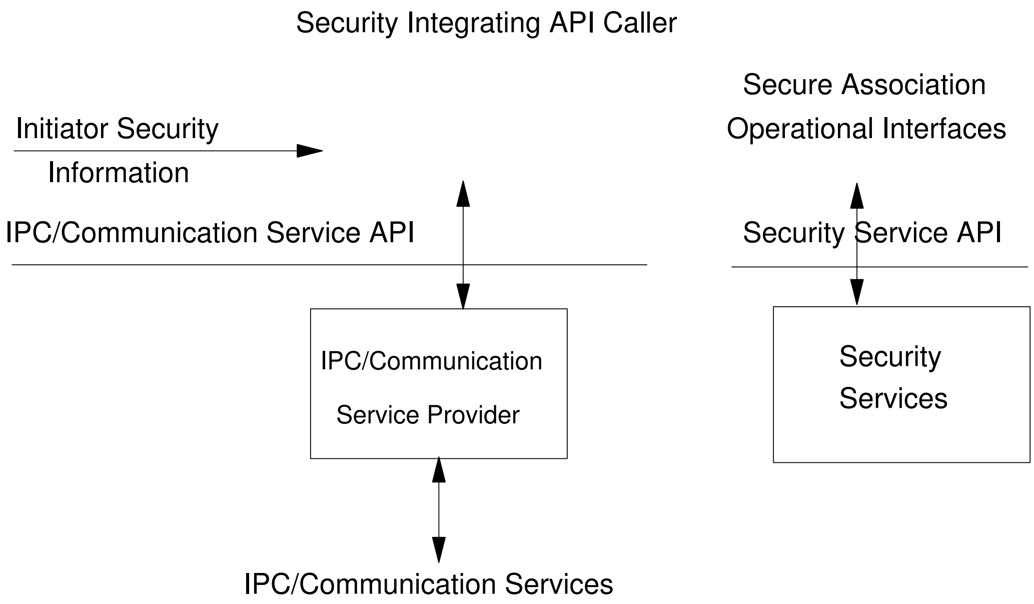

Figure 6-9 – Security Non-enforcing API / Security Integrating Caller

A primary service provider presenting Security Non-enforcing APIs provides no support for secure association security services. It is therefore the responsibility of the caller of such APIs to implement the Secure Association Services.

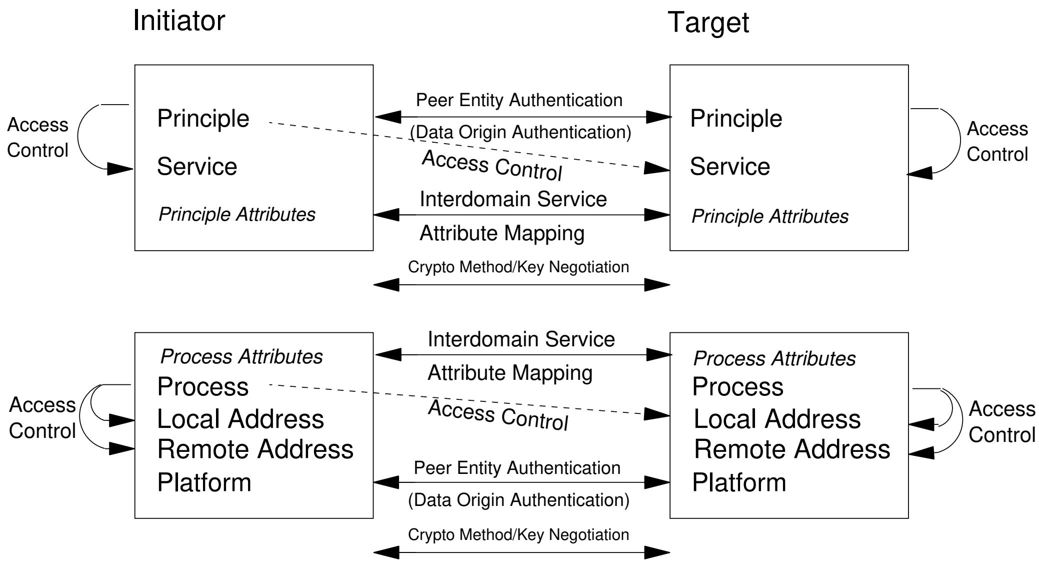

Figure 6-10 – Example Disposition of Security Services in Association Establishment

The figure above illustrates how various security services within different security domains may be deployed in supporting a secure association service.

NOTE: Text to support this diagram has still to be added.

6.11 Trusted Third Party Services

NOTE: This section is here as a placeholder. The following text is very tentatve.

The non-repudiation service involves the generation, verification and recording of evidence, and the subsequent retrieval and re-verification of this evidence should proof be required.

The purpose of the non-repudiation service described in this framework is to provide proof about a particular event or action.

6.11.1 Basic Service Model

Non-repudiation can be divided into four phases:

- Evidence generation - production of a record of a security event
- Evidence transfer, storage and retrieval - subsequent handling and management of such evidential records
- Evidence verification - verification of the occurence of a security event
- Dispute resolution - subsequent adjudication between parties on the authenticity of evidential records

To support non-repudiation of an event it is necessary to establish a trust relationship between the originator of an event and the recipient of an event. Such a trust relationship may be established either through the use of assymmetric cryptographic techniques, trusted communication channels or through the intervention of a trusted third party or parties.

NOTE: This will be a diagram

Adjudicator

Non repudiation Evidence user service requestor

Evidence generator Evidence verifier

Trusted third party

-evidence recording
-monitoring
-certificate generation
-signature verification
-delivery authority

-time stamping
-certification
-signature generation
-notarization

6.11.2 Operational Services

Generate evidence

Generate evidence will generate evidence of the occurence of an event, such evidence may be based on the:

- authenticated identity of the originator of the event,
- authenticated identity of the requestor of the non-repudiation service,
- authenticated identity of any intermediaries in the formation of the trust relationship leading to the occurence of the event,
- authenticated identify of any intermediaries in the formation of the trust relationship leading to the propagation of the evidence to the requestor state of the

system at the time of the event, including a certified timestamp

- information on the nature of the event itself

Validate evidence

Validate evidence will accept evidence generated by the above service and will return an indication of the validity of such evidence given the expected state of the event and the environment within which such an event occurs.

Assure evidence

Assure evidence is used to provide additional assurance in by requesting that a trusted third party provide an evidential statement regarding an event, or that such a third party endorse an existing evidential statement.

Deposit evidence

Deposit evidence is used to deposit an evidential statement with a trusted third party for later retrieval during arbitration.

Retrieve evidence

Retrieve evidence is used to retrive an evidential statement which has been previously deposited with a third party.

6.11.3 Management Services

Management information for the non-repudiation service consists of those certificates, keys and trust dependencies which are required in order to support the operation of the non-repudiation service.

Install

Install management information

Modify

Modify management information

Delete

Delete management information

List

List management information

The non-repudiation services may require support from a time service to ensure the application of appropriate timestamp information in an assured manner, and from directory/certificate and key management services.