The model contains eight elements:

The Principal is an entity that requires controlled access to resources in a Secondary Domain.

The Primary Domain is an administrative domain in which the Principal can be authenticated without assistance from any other domain.

The Secondary Domain is an administrative domain in which the Principal cannot be authenticated except with assistance from a Primary Domain.

The Principal has at least one name in a namespace sub-tree administered by the Authentication Authority in the Primary Domain. The Authentication Authority binds the Principal's name to an authentication mechanism in a "name assertion".

The Principal may have one or more entitlements in an entitlement-space sub-tree administered by the Authorization Authority in the Primary Domain. The Authorization Authority binds the Principal's name to a name assertion in an "entitlement assertion".

The Principal may have a session state in a session state-space sub-tree administered by the Session Authority. The Session Authority binds the Principal's session state to a name assertion in a "session assertion".

The Policy Enforcement Point authenticates the Principal with the assistance of a Policy Decision Point and controls its access to resources in the Secondary Domain.

The Policy Decision Point authenticates the Principal and determines its eligibility to access resources in the Secondary Domain on the basis of the assertions.

Figure 1 indicates which elements of the model communicate with which other elements.


There are seven authorization data structures: AuthzNotification, AuthzAcknowledgment, AuthzRequest, AuthzResponse,
The process shown above demonstrates the Principal-centered indirect protocol. The Principal communicates with the Secondary Domain over a series of messages, each of which triggers a specific action.

**Protocol Exchanges:**

**Policy-centered Direct Protocol:**

1. The Principal obtains a name assertion from the Authentication Authority in the Primary Domain in an AuthnNotification message. The authentication of the Principal by the Authentication Authority is outside the scope of this specification.
2. The Principal conducts an authentication exchange with the Policy Enforcement Point. However, the Policy Enforcement Point is not capable of completing the authentication process alone.
3. The Principal provides the name assertion in an AuthnNotification message.
4. The Policy Enforcement Point sends the posited name, the authenticator and the name assertion to the Policy Decision Point in an AuthnQuery message.
5. The Policy Decision Point authenticates the Principal using the posited name, authenticator and name assertion provided in step 4 and returns the result to the Policy Enforcement Point.

**Policy-centered Indirect Protocol:**

This protocol may be used when the Principal is capable of relaying messages between the Primary Domain and the Secondary Domain, and the Secondary Domain is capable of completing the authentication process. The steps in which the Principal communicates with the Secondary Domain are as follows:

1. The Principal obtains a name assertion from an Authentication Authority in the Primary Domain in an AuthnNotification message. The authentication of the Principal by the Authentication Authority is outside the scope of this specification.
2. The Principal conducts an authentication exchange with the Policy Enforcement Point.
3. The Principal provides the name assertion in an AuthnNotification message.
4. The Policy Enforcement Point sends the posited name, the authenticator and the name assertion to the Policy Decision Point in an AuthnQuery message.
5. The Policy Decision Point authenticates the Principal using the posited name, authenticator and name assertion provided in step 4 and returns the result to the Policy Enforcement Point.

The diagram illustrates the interactions between the Principal, Policy Enforcement Point, and Policy Decision Point in the authentication process.
Figure 3 - Principal-centered indirect protocol

It proceeds by the following steps.

1. The Principal obtains a reference to a name assertion from an Authentication Authority in the Primary Domain in the Ref(AuthnNotification) message. As in the previous protocol, the authentication of the Principal by the Authentication Authority is out of scope.

2. The Principal conducts an authentication exchange with the Policy Enforcement Point. As before, the Policy Enforcement Point is not capable of completing the authentication without the help of the Policy Decision Point.

3. The Principal provides the reference to the name assertion in the Ref(AuthnNotification) message.

4. The Policy Enforcement Point sends the posited name, the authenticator and the reference to the name assertion to the Policy Decision Point in the AuthnQuery message.

5. The Policy Decision Point sends a request for the name assertion to the Authentication Authority in the Primary Domain in the AuthnRequest message.

6. The Authentication Authority sends the name assertion in an AuthnResponse message.

7. The Policy Decision Point authenticates the Principal and returns the result to the Policy Enforcement Point in an AuthnResult message.

Pull protocol

This protocol may be used when the Principal communicates with the Secondary Domain.

Figure 4 shows the pull protocol.

It proceeds by the following steps.

1. The Principal conducts an authentication exchange with the Policy Enforcement Point. As before, the Policy Enforcement Point is not capable of completing the authentication without the help of the Policy Decision Point.

2. The Policy Enforcement Point sends the posited name and the authenticator to the Policy Decision Point in the AuthnQuery message.

3. The Policy Decision Point sends a request for the name assertion to the Authentication Authority in the Primary Domain.

4. The Authentication Authority sends the name assertion in an AuthnResponse message.

5. The Policy Decision Point authenticates the Principal using the posited name and authenticator obtained from the Policy Enforcement Point in step 2 and the name assertion obtained from the Authentication Authority in step 4 and returns the result to the Policy Enforcement Point.

6. The Policy Enforcement Point sends a request for the name assertion to the Authentication Authority.

7. The Authentication Authority sends the name assertion in an AuthnResponse message.

Push protocol

This protocol may be used when the Principal communicates with the Secondary Domain under the direction of the Primary Domain. Because it requires the Policy Decision Point to maintain state between communication sessions with the Secondary Domain, this protocol is less favored than the Principal-centered protocols.

Figure 5 shows the Push protocol.
1. The Authentication Authority sends a name assertion to the Policy Decision Point in the Secondary Domain.

2. The Policy Decision Point issues an authentication message to the Policy Enforcement Point in the Secondary Domain.

3. The Policy Enforcement Point requests an authentication message from the Policy Decision Point.

4. The Policy Decision Point authenticates the Principal using the name assertion and the request and returns the result to the Policy Enforcement Point.

Secondary domain session-close protocol

1. The Principal sends a session notification message to the Authentication Authority.

2. The Authentication Authority sends a session notification message to the Policy Decision Point in the Secondary Domain.

3. The Policy Decision Point sends a session acknowledgment message to the Authentication Authority.

4. The Authentication Authority sends a session notification message to the Policy Enforcement Point.

5. The Policy Enforcement Point confirms the session status of the Principal with the Policy Decision Point before processing each exchange between the Principal and the Policy Enforcement Point.

Secondary domain session-close protocol

1. The Principal sends a session notification message to the Policy Enforcement Point.

2. The Policy Enforcement Point sends a session acknowledgment message to the Policy Decision Point.

3. The Policy Decision Point sends a session notification message to the Authentication Authority.

4. The Authentication Authority sends a session notification message to the Policy Enforcement Point.

Primary domain session-close protocol

1. The Principal sends a session notification message to the Authentication Authority.

2. The Authentication Authority sends a session notification message to the Policy Decision Point in the Secondary Domain.

3. The Policy Decision Point sends a session acknowledgment message to the Authentication Authority.

4. The Authentication Authority sends a session notification message to the Policy Enforcement Point.

5. The Policy Enforcement Point sends a session acknowledgment message to the Policy Decision Point.

6. The Policy Decision Point sends a session notification message to the Authentication Authority.

7. The Authentication Authority sends a session notification message to the Policy Enforcement Point.
Data structures

Note: there are separate data structures for authentication, authorization and session exchanges. If an entity needs information on any combination of name, entitlements and session status, it must conduct separate protocols for each. However, these separate protocols may proceed in parallel.

Schema for the data structures can be found in the Schema section of this specification.

AuthnNotification

The AuthnNotification message is used in the Principal-centered direct authentication protocol to send the name assertion from the Authentication Authority to the Principal and from the Principal to the Policy Decision Point. It contains the following information.

version - this specification version number.
notification-identifier - an identifier assigned by the message originator. It must be unique among all the outstanding AuthnNotification messages.
name-assertion - the name assertion.
sender - the name of the sender, as agreed between the sender and receiver during initialization. It must be unique among all the sender names recognized by the receiver.
to - the recipient name for the intended receiver.
context - the context string, if any.
message - the principal or principal domain name, if any.

AuthnAcknowlegment

The AuthnAcknowlegment message is used in the Push protocol for the Policy Decision Point to acknowledge receipt of the name assertion from the Authentication Authority. It contains the following information.

version - this specification version number.
note - the notification identifier supplied in the corresponding AuthnNotification message.
success-indicator - an indication of whether the receiver was able to process the AuthnNotification message.
error-code - error code.

The following error codes shall be supported.

Unsupported version
Unsupported authentication method

AuthnRequest

The AuthnRequest message is used in the Principal-centered indirect protocol and the Pull protocol for the Policy Decision Point to request the name assertion from the Authentication Authority. It contains the following information.

version - this specification version number.
request-identifier - an identifier assigned by the message originator. It must be unique among all the outstanding AuthnRequest messages.
posited-name - the Primary Domain and Principal names claimed by the Principal. Optional.
reference-to-name-assertion - a reference to the name assertion. Optional, if the posited name is not present, then this field must be present.
sender - the name of the sender, as agreed between the sender and receiver during initialization. It must be unique among all the sender names recognized by the receiver.
to - the name of the intended receiver.
context - the context string, if any.
message - the principal or principal domain name, if any.

AuthnResponse

The AuthnResponse message is used in the Principal-centered indirect protocol and the Pull protocol for the Authentication Authority to return the name assertion to the Policy Decision Point. It contains the following information.

version - this specification version number.
notification-identifier - an identifier assigned by the message originator. It must be unique among all the outstanding AuthnResponse messages.
name-assertion - the name assertion.
error-code - error code.

The following error codes shall be supported.

Unsupported version
Unsupported authentication method

Data structures
**AuthnRequest**

- **name-assertion** - the name assertion.
- **success indicator** - an error code.
- **error code** - an error code.

**AuthnQuery**

This protocol is used in the Principal-centered direct and indirect protocols and the Pull and Push protocols for the Policy Decision Point to request the Policy Enforcement Point to perform the authentication of the Principal.

- **version** - the specification version number.
- **request-identifier** - an identifier assigned by the message originator. It must be unique among all the outstanding AuthnQuery messages.
- **name-assertion** - the name assertion.
- **posited name** - the name claimed by the Principal.
- **authenticator** - the data used in the authentication exchange between the Policy Enforcement Point and the Principal. This may be a user-name/password combination, a symmetric-key challenge/response combination, an asymmetric-key challenge response combination or a document/signature combination.

**AuthnResult**

This protocol is used in the Principal-centered direct and indirect protocols and the Pull and Push protocols for the Policy Decision Point to return the result of the authentication of the Principal to the Policy Enforcement Point.

- **version** - the specification version number.
- **request-identifier** - the request identifier from the corresponding AuthnQuery message.
- **success indicator** - an error code.

**AuthzNotification**

The AuthzNotification message is used in the Principal-centered direct authorization protocol to send the entitlement assertion from the Authorization Authority to the Principal and from the Principal to the Policy Decision Point. It contains the following information.

- **version** - the specification version number.
- **notification-identifier** - an identifier assigned by the message originator. It must be unique among all the outstanding AuthzNotification messages.
- **entitlement-assertion** - the entitlement assertion.
- **sender** - the name of the sender, as agreed between the sender and receiver during initialization. It must be unique among all the sender names recognized by the receiver.
- **intended-receiver** - the name of the receiver, as agreed between the sender and receiver during initialization. It must be unique among all the receiver names recognized by the sender.

Note: The entitlement assertion contains an identifier for the Authorization Authority and a reference to the associated Principal name-assertion. It also contains validity dates.

**AuthzAcknowledge**

The AuthzAcknowledge message is used in the Push protocol for the Policy Decision Point to acknowledge receipt of the entitlement assertion from the Authorization Authority. It contains the following information.

- **version** - the specification version number.
- **notification-identifier** - the notification identifier supplied in the corresponding AuthzNotification message.
- **success indicator** - an indication of whether the receiver was able to process the AuthzNotification message.
- **error code** - an error code.

**AuthzRequest**

The AuthzRequest message is used in the Principal-centered indirect protocol and the Pull protocol for the Policy Decision Point to request the entitlement assertion from the Authorization Authority. It contains the following information.

- **version** - the specification version number.
- **notification-identifier** - the notification identifier supplied in the corresponding AuthzNotification message.
- **success indicator** - an indication of whether the receiver was able to process the AuthzRequest message.
- **error code** - an error code.
version - this specification version number.

request-identifier - an identifier assigned by the message originator. It must be unique among all the outstanding AuthzRequest messages.

posited name - the posited name of the Principal. Optional. reference to entitlement assertion - reference to an entitlement assertion. Optional. If the posited name is absent, then this field must be present.

sender - the name of the sender, as agreed between the sender and receiver during initialization. It must be unique among all the sender names recognized by the receiver.

intended-receiver - the name of the receiver, as agreed between the sender and receiver during initialization. It must be unique among all the receiver names recognized by the sender.

Note: the Authorization Authority receives no evidence that the Principal correctly authenticated to the Policy Enforcement Point. In the Pull protocol, all suitable entitlement assertions are requested.

AuthzResponse

The AuthzResponse message is used in the Principal-centered indirect protocol and the Pull protocol for the Authorization Authority to return the entitlement assertion to the Policy Decision Point. It contains the following information.

version - this specification version number.

request-identifier - the request identifier supplied in the corresponding AuthzRequest message.

entitlement assertion - the entitlement assertion.

success indicator

error code

AuthzQuery

This protocol is used in the Principal-centered direct and indirect protocols and the Pull and Push protocols for the Policy Enforcement Point to request the Policy Decision Point to confirm the authorization of the Principal.

version - this specification version number.

request-identifier - an identifier assigned by the message originator. It must be unique among all the outstanding AuthzQuery messages.

action - a compound variable comprising the name of the object method and a sensitivity value for the object that the Principal is attempting to access.

principal name - the authenticated or claimed name of the Principal. Optional. Must be identical to the posited name in any accompanying AuthnQuery message.

entitlement-assertion - the entitlement assertion. Optional. reference to the entitlement assertion - a reference to the entitlement assertion. Optional. It should be present if the entitlement assertion is present. Optional. At least one of "principal name", "entitlement-assertion" or "reference to entitlement-assertion" must be present.

AuthzResult

This protocol is used in the Principal-centered direct and indirect protocols and the Pull and Push protocols for the Policy Decision Point to return the result of the authorization of the Principal to the Policy Enforcement Point.

version - this specification version number.

request-identifier - the request identifier supplied in the corresponding AuthzRequest message.

success indicator

error code

SessionNotification

The SessionNotification message is used in the Principal-centered direct session protocol to send the session assertion from the Session Authority to the Principal and from the Principal to the Policy Enforcement Point. It is also used in the Pull and Push protocols to indicate that the session with the Principal has been closed. It contains the following information.

version - this specification version number.

notification-identifier - an identifier assigned by the message originator. It must be unique among all the outstanding SessionNotification messages.

session-assertion - the session assertion.
sender - the name of the sender, as agreed between the sender and receiver during initialization. It must be unique among all the sender names recognized by the receiver.

intended-receiver - the name of the receiver, as agreed between the sender and receiver during initialization. It must be unique among all the receiver names recognized by the sender.

Note: the session assertion identifies the Principal either directly or by reference to a name assertion. It also contains an indication of the Principal's session state (e.g., "session closed").

Session Acknowledgment

The Session Acknowledgment message is used in the Push protocol for the Policy Decision Point to acknowledge receipt of the session assertion from the Session Authority. It is also used in the Primary Domain escalation protocols to acknowledge that the session with the Principal has been closed. It contains the following information.

- version - this specification version number.
- notification-identifier - the notification identifier supplied in the corresponding Session Notification message.
- success-indicator - an indication of whether the receiver was able to process the Session Notification message.
- error-code - error code.

The following error codes shall be supported.

- Unsupported version

Session Request

The Session Request message is used in the Principal-centered indirect protocol and the Pull protocol for the Policy Decision Point to request the session assertion from the Session Authority. It contains the following information.

- version - this specification version number.
- request-identifier - an identifier assigned by the message originator. It must be unique among all the outstanding Session Request messages.
- principal-name - the name of the Principal. Optional.
- reference-to-session-assertion - reference to the session assertion. Optional; if the principal-name field is absent, then this field must be present.
- sender - the name of the sender, as agreed between the sender and receiver during initialization. Optional; if the principal-name field is absent, then this field must be present.

Note: the Session Authority receives no evidence that the Principal correctly authenticated to the Policy Enforcement Point.

Session Response

The Session Response message is used in the Principal-centered indirect protocol and the Pull protocol for the Session Authority to return the session assertion to the Policy Decision Point. It contains the following information.

- version - this specification version number.
- request-identifier - the notification identifier supplied in the corresponding Session Request message.
- session-assertion - the session assertion.
- success-indication.
- error-code.

Session Query

This protocol is used in the Principal-centered direct and indirect protocols and the Pull and Push protocols for the Policy Enforcement Point to request the Policy Decision Point to confirm the session status of the Principal.

- version - this specification version number.
- request-identifier - an identifier assigned by the message originator. It must be unique among all the outstanding Session Query messages.
- principal-name - the authenticated or claimed name of the Principal. Optional. Must be identical to the posited name in any associated Authn Query message.
- session-assertion - a session assertion. Optional.

Note: the session assertion identifies the Principal either directly or by reference to a name assertion. It also contains an indication of the Principal's session state (e.g., "session closed").
14 Feb 2001

17

reference to session assertion - a reference to a session assertion. Optional, at
least one of "principal name", "session assertion" or "reference to session
assertion" must be present.

SessionResult

This protocol is used in the Principal-centered direct and indirect protocols and the Pull
and Push protocols for the Policy Decision Point to return the result of the state-
evaluation of the Principal to the Policy Enforcement Point.

version - this specification version number.request-identifier - the identifier from the corresponding SessionQuery message.session assertion:success indicatorerror code

Note: the session assertion returned in the SessionResult message may be integrity-
protected by means other than XML Digital Signature. Alternatively, it may be protected by
the XML Digital Signature mechanism, signed by the Policy Decision Point.

Security considerations

With the exception of the session assertion in the SessionResult message all assertions
must be protected for integrity and authenticity using the XML Digital Signature
mechanism. All protocol messages must be integrity-
protected for integrity and authenticity. Mechanisms other than XML Digital Signature may be used for this latter
purpose.

The exchange of Authority keys, certificates and certificate status information between
domains is out of scope for this specification.