



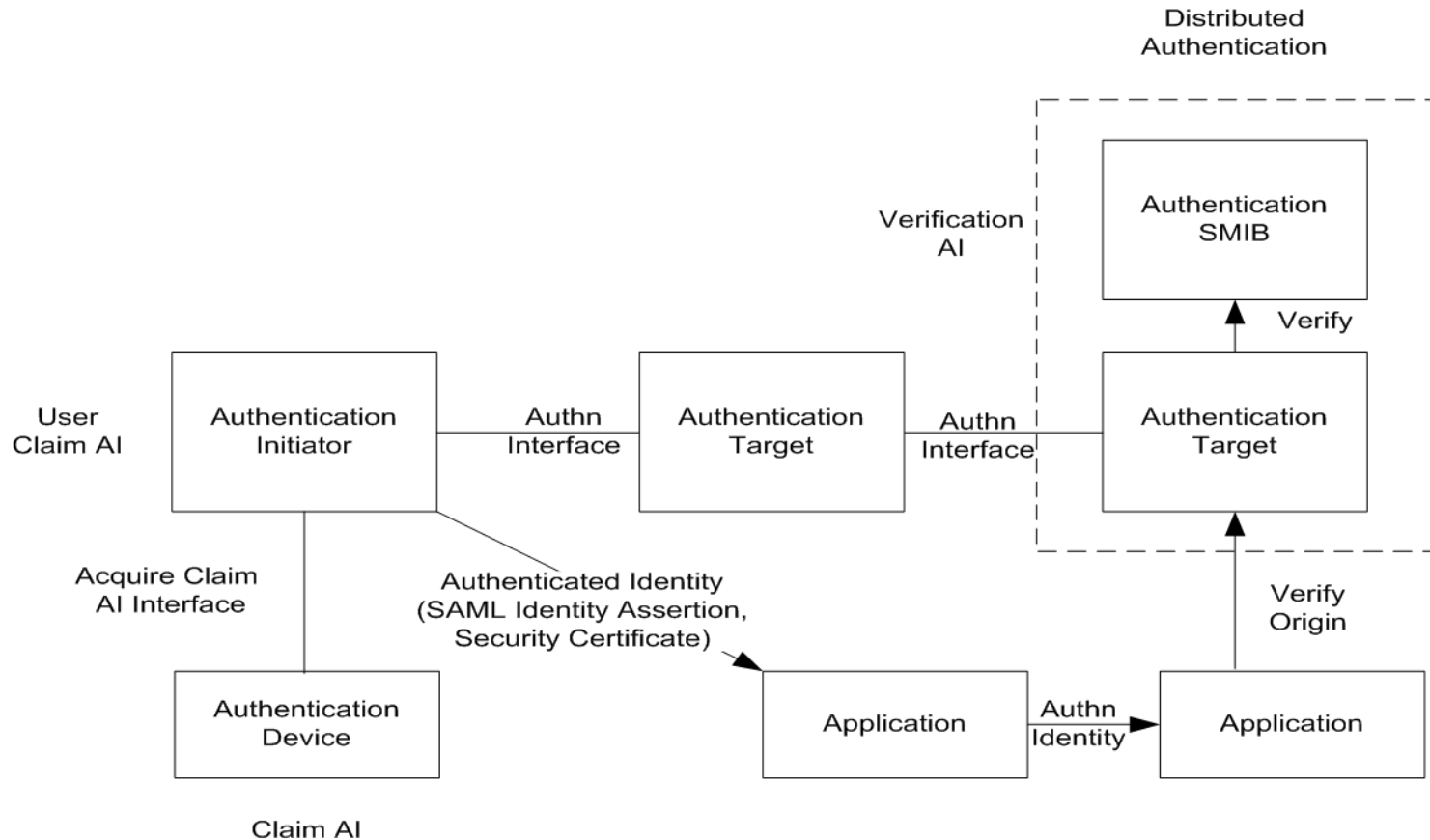
SAML in CCOW Environment OR BETTER CCOW in SAML Environment

Mike Davis

1/8/2009



Authentication SOA



Adapted from ISO 10181-2





CCOW Authentication

(1) User signs-on (e.g., enters logon name and password; swipes security card, etc.).

(2) Application authenticates the user and tells context manager the user's logon name; authentication data is **not** passed on to the context manager.



Application trusted to authenticate users

Context Manager

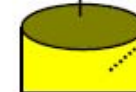
Application YY

(6) Each application gets user's application-specific logon name from the context manager. The application may also get the user's digital certificate from the context manager.

(7a) An application optionally consults internal authentication data repository to get application-specific authentication data for the new user and automatically signs-on the user.

(5) Context manager tells other applications that there is a new user context.

Application ZZ



External Authentication Repository (Optional)

(7b) An application optionally consults external authentication data repository to get application-specific authentication data for the new user and automatically signs-on the user.

(3) Context manager tells mapping agent context change is occurring; mapping agent supplies the context manager with other logon names for the user as known to each application.

User Mapping Agent (Optional)

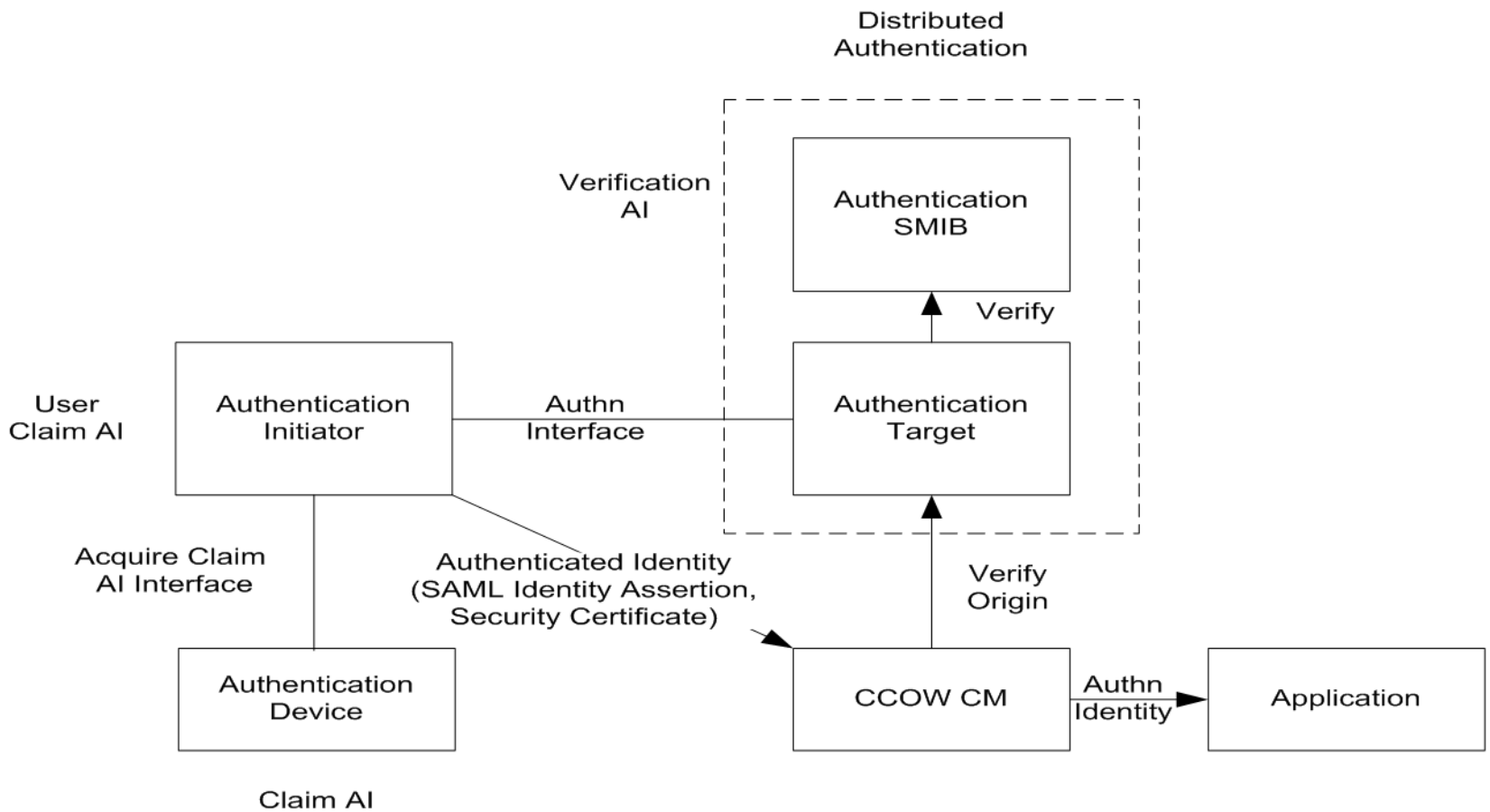
User Certificate Annotation Agent (Optional)

(4) Context manager tells annotation agent context change is occurring; annotation agent supplies the context manager with user's digital certificate.

Chain of Trust

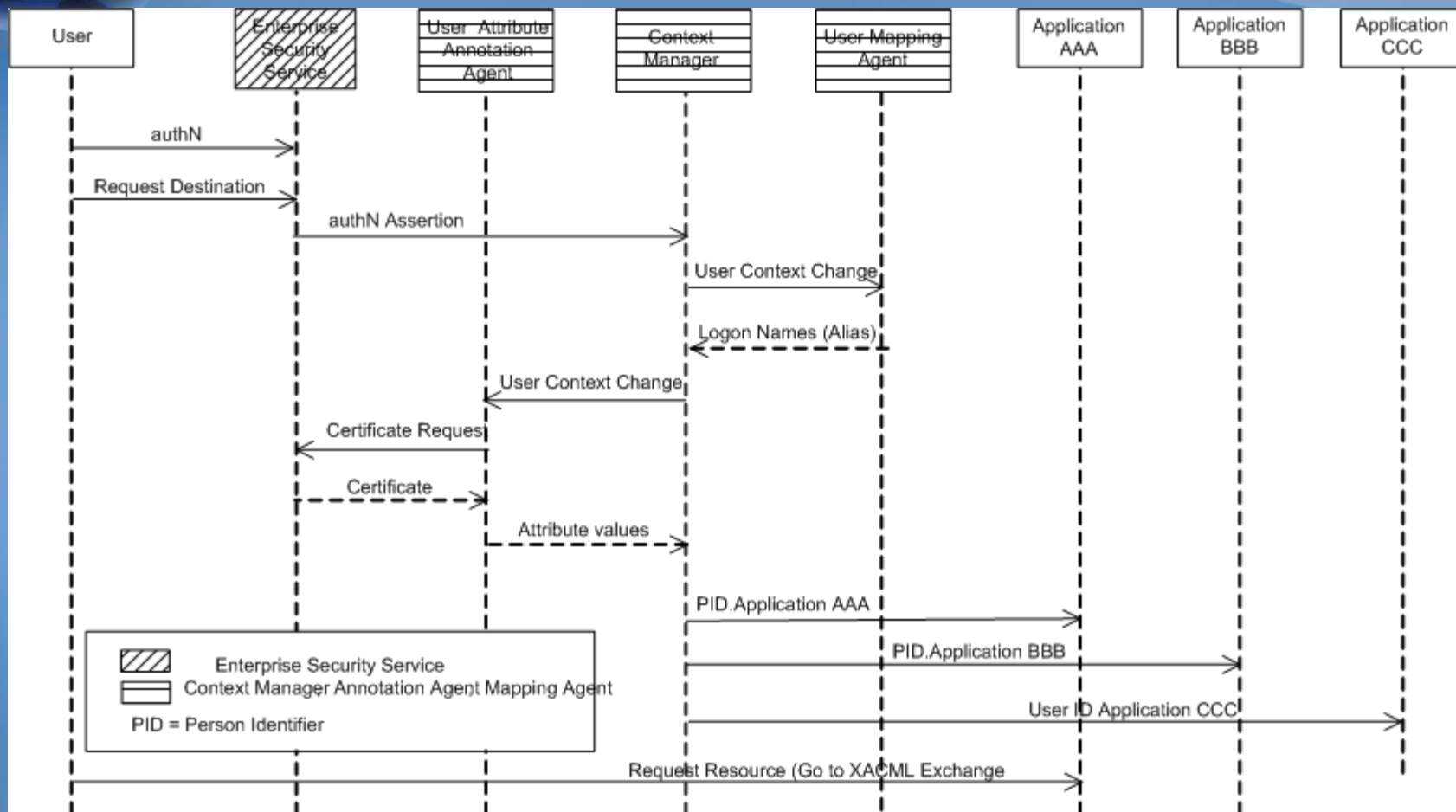


CCOW Authentication SOA



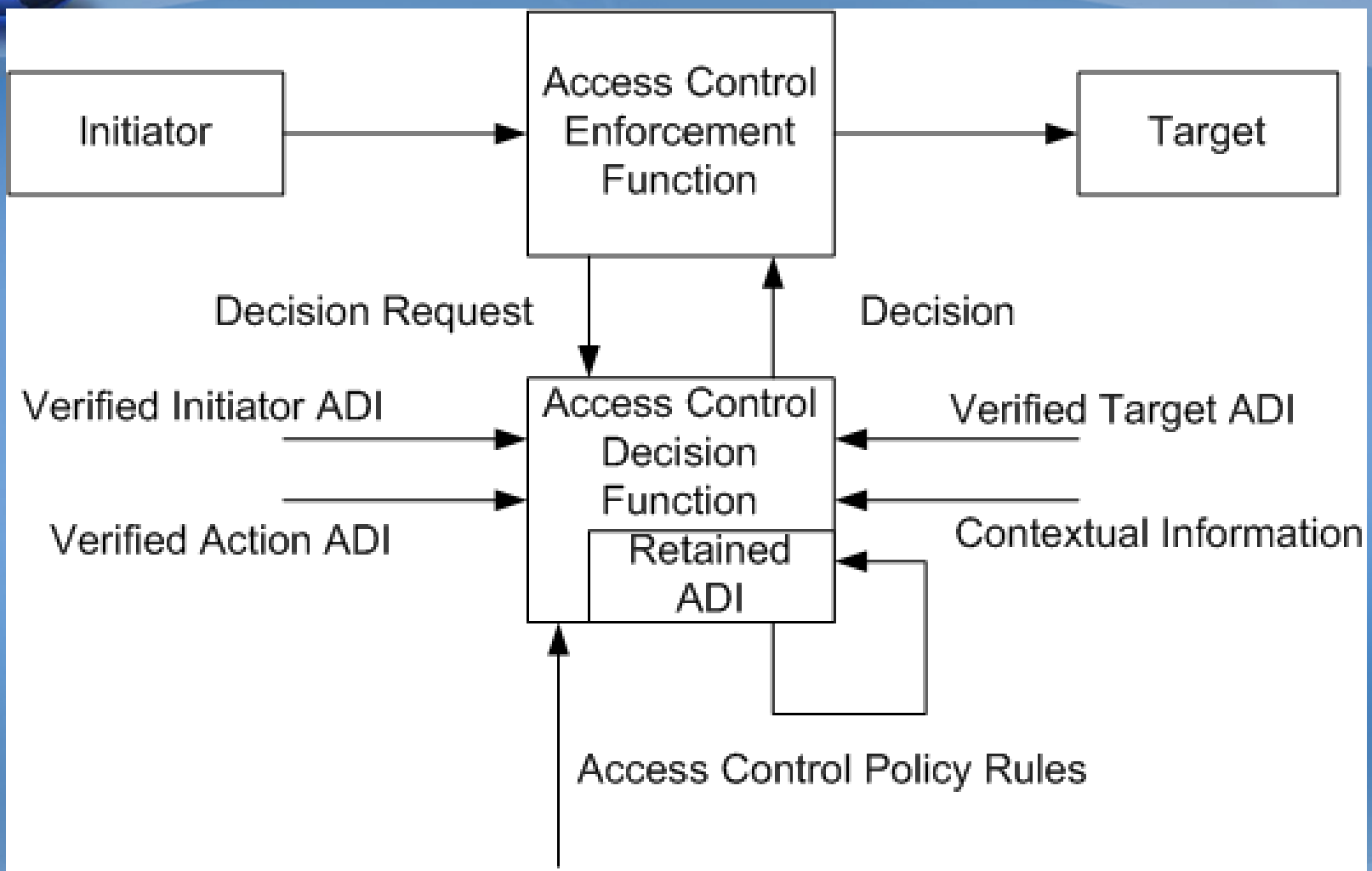


CCOW Interface to SOA



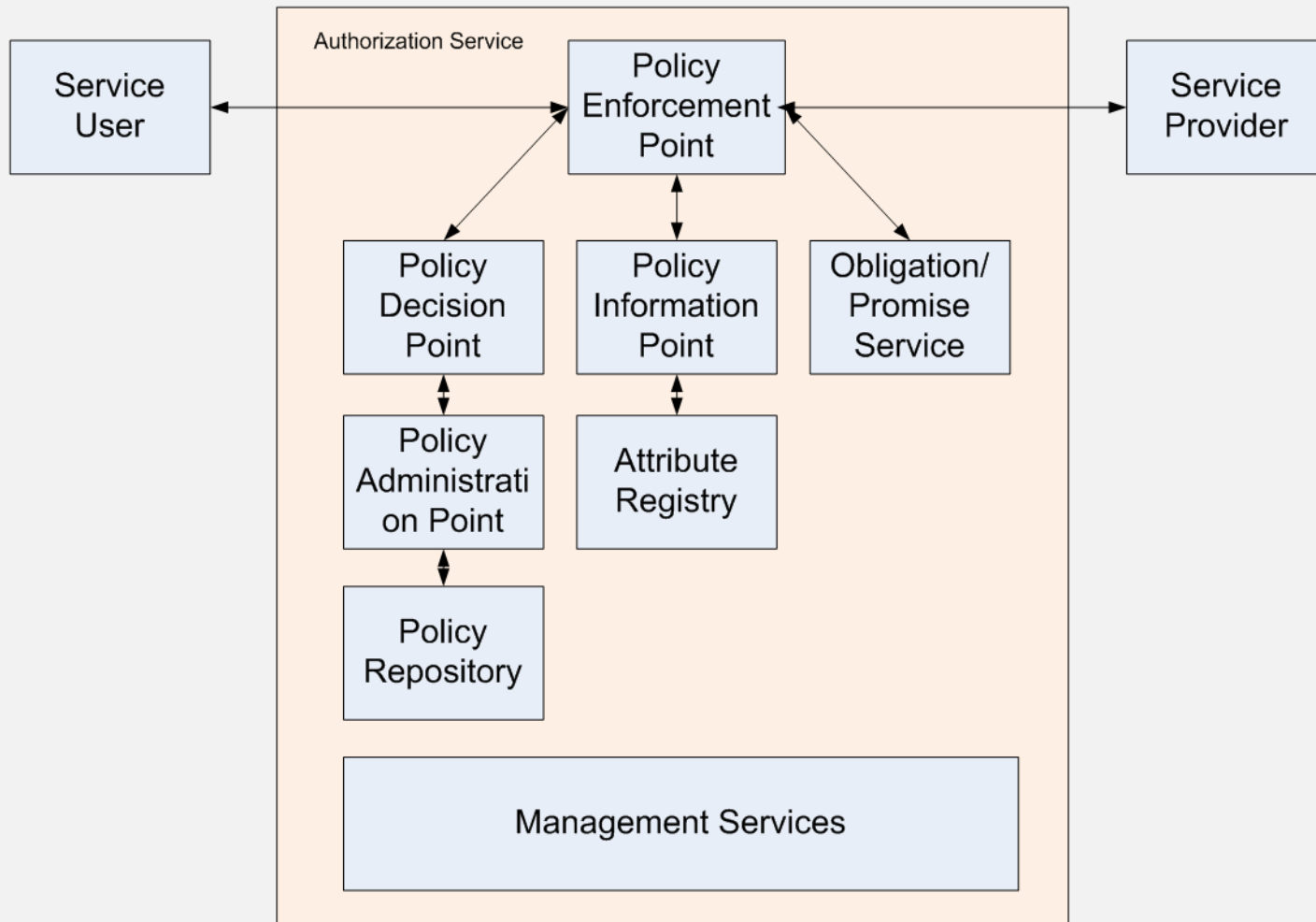


ISO Access Control Model





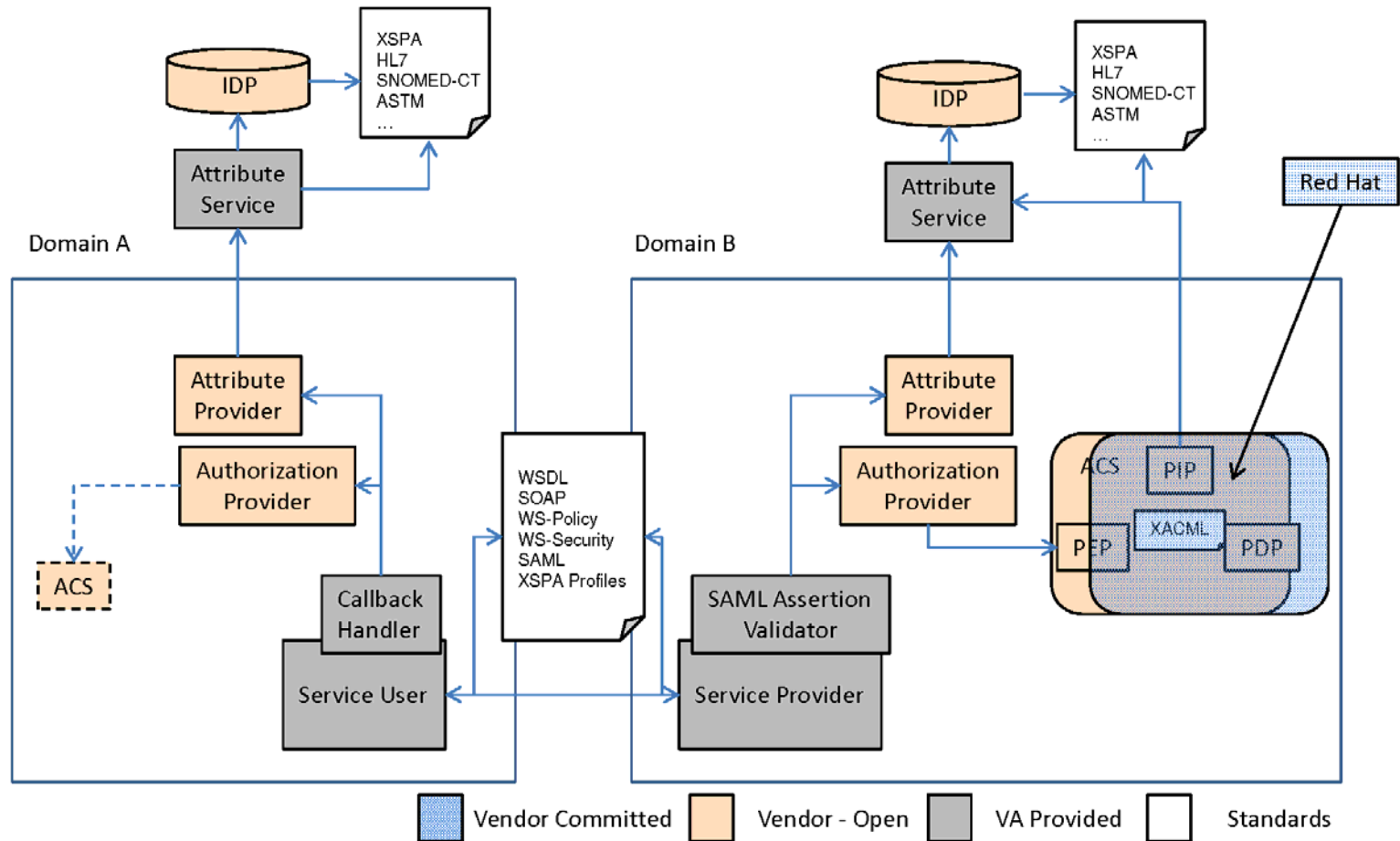
Authorization SOA



HIMSS Interop Scenarios

XSPA Profile of SAML

Vendor Participation





HIPAA Privacy SOA

Privacy Manager

Smith, Jane (321567)

ACCESS RESTRICTION

Some or all of this patient's chart has been sealed as requested by the patient or substitute decision maker.

Selecting a reason and clicking on "OK" will allow access and generate a Privacy/Security Alert.

Select a reason to override the access restriction (required for override)

Select Reason - [v]

Enter additional details below

Select "Cancel" to exit

OK Cancel

For assistance, please call the Privacy Office at extension XXXX

Sample access restriction message



Privacy Manager

user interface

appropriate at the point of service and for all levels of health data exchange, e.g. PHR, CDO, portal, EHR, HIE, RHIO, LHIN (Canada), NHIN (U.S.), PCT (UK)

integrates with application architecture via simple application interface (API) or via HL7 CCOW

issues IHE audit messages (e.g. "break the glass" access) to the Universal Audit

Repository, which generates immediate security alerts as appropriate





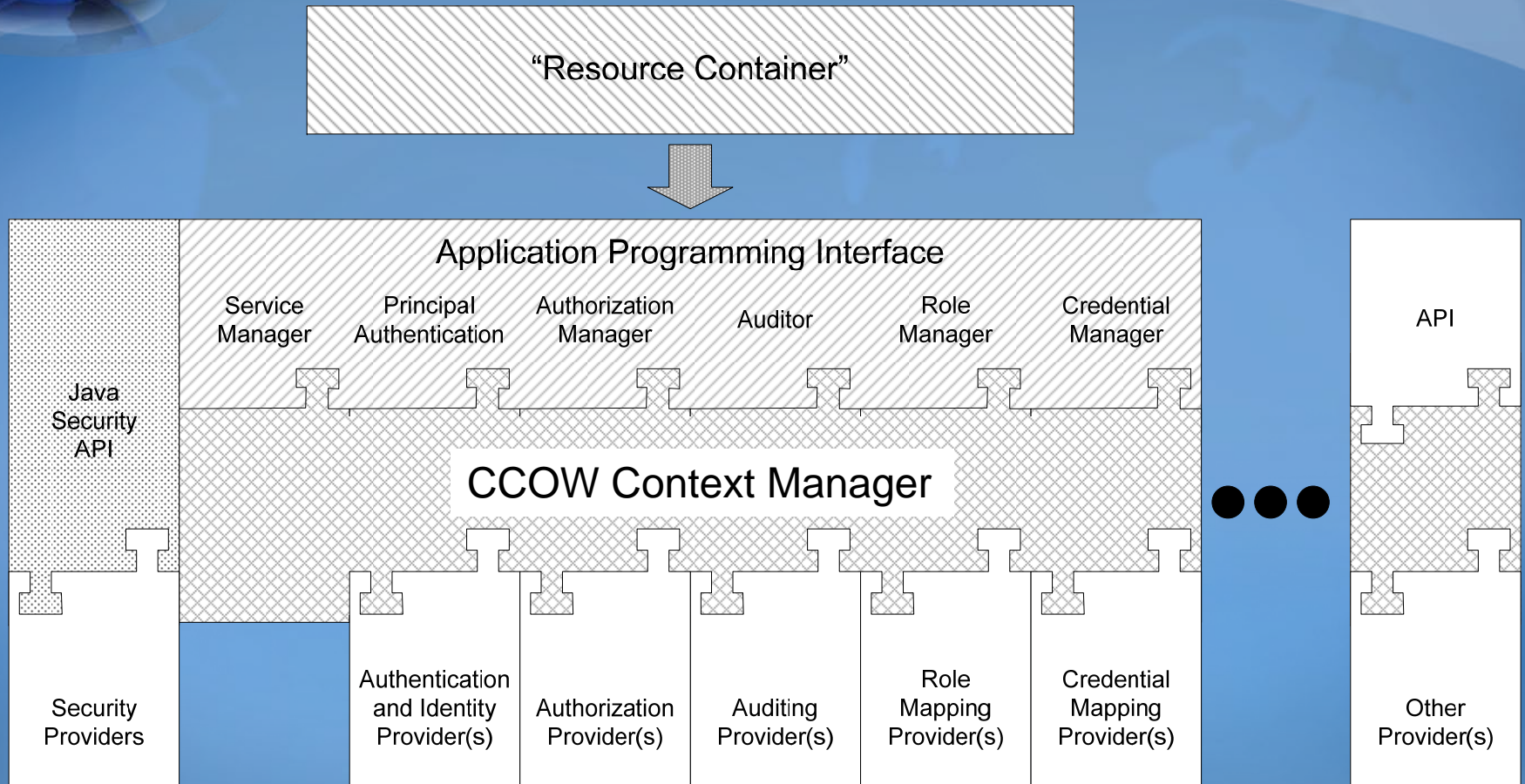
CCOW SOA/BIZ ISSUES

- CCOW is not SOA Aware: Why not follow the distributed authentication model?
- CCOW can pass the user credential to the application...Why not the SAML Assertion?
- CCOW cannot deal with distributed authorization/access control...Why require users to find alternate solutions?
- CCOW cannot deal with privacy...Why require users to find alternate solutions?





CCOW as SOA Middleware



Adapted from: **Building an Application Security Infrastructure, Business Integration Journal, pp. 36-39 (2004)** Permission to use copyright material

