XSPA
Cross-Enterprise Security and Privacy Authorization

# SAML v2.0 Interop

## Fine Grain Access Control Validation

*Get Medical Record Request – Permissions Enforced, Patient Consent Directives Enforced*

**Security Domain 1 – Service User**

•Dr. Bob performs login to XSPA application

•Dr. Bob perform patient search for Bambi Smith and sets context to her medical record

•Dr. Bob then navigates to Clinical Notes menu option and sees current available notes For viewing

•Dr. Bob clicks on the "XSPA" search button to obtain listing of available C32 documents For Bambi Smith.

•Application asserts "purpose of use" and unique patient identifier and makes cross-enterprise request

•Request is logged locally – view authentication and assertion information

**Security Domain 2 – Service Provider**

•Local Policy is reviewed and connection authorization is obtained (Network ACD)

•Request is logged at service provider

•Purpose of use, patient identifier are exacted through Assertion Query

•Service performs attribute lookup for patient directive and required permissions based on purpose of use

•PIP request is logged

•XACML Request is formed and sent to PDP from PEP

•PEP enforces access control decision

•Application ACD is logged on Service Provider

**Security Domain 1 – Service User**

•If patient directive in Security Domain 2 results in "Permit" a C32 will be delivered and viewed within Clinical notes area

•If "Deny" no results are returned.

Blues indicates areas where message viewing is possible

HITSP

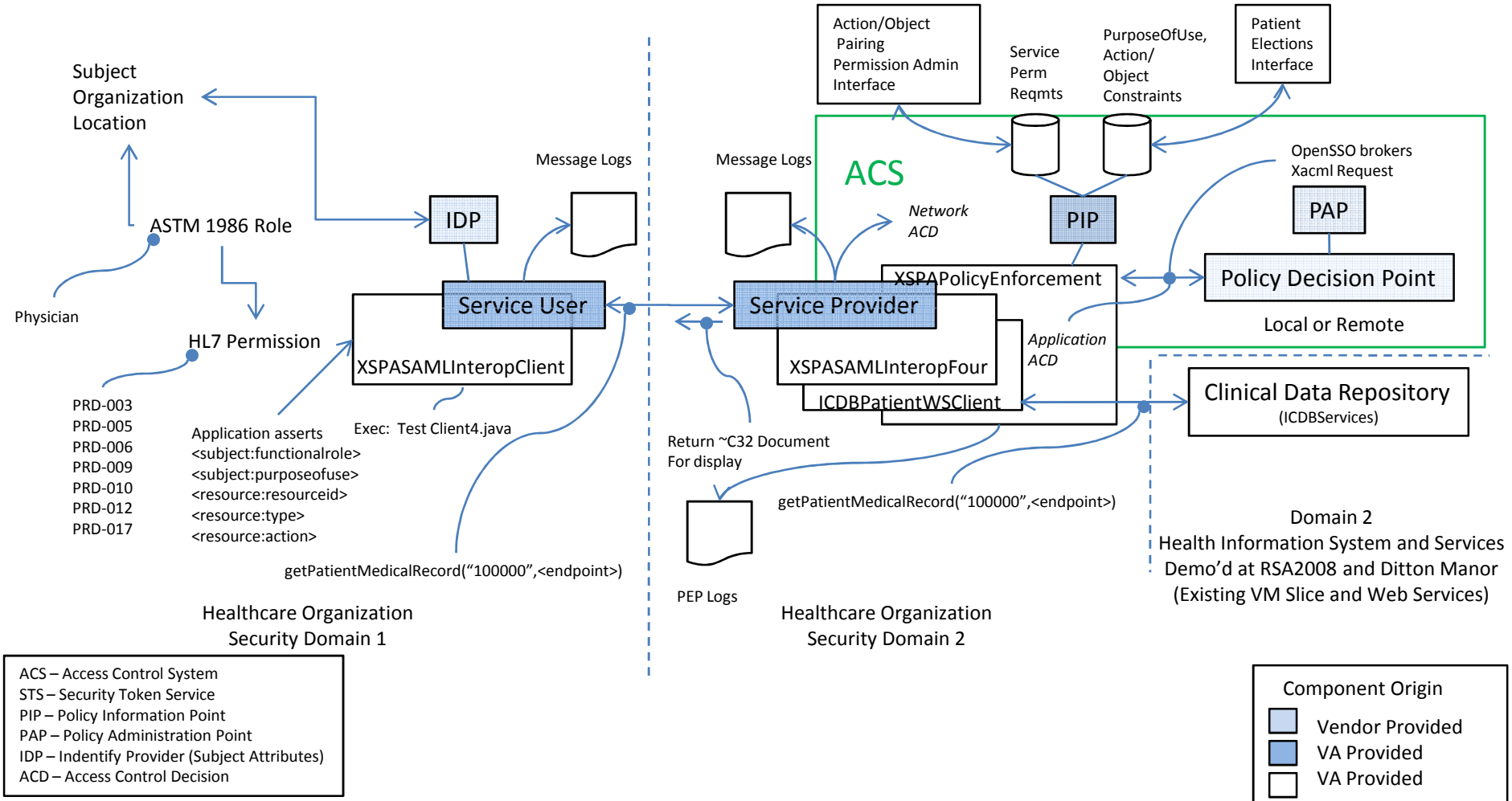
OASIS

XSPA
Cross-Enterprise Security and Privacy Authorization

# SAML v2.0 Interop

## Fine Grain Access Control Validation

*Get Medical Record Request – Permissions Enforced, Patient Consent Directives Enforced*




ACS – Access Control System
STS – Security Token Service
PIP – Policy Information Point
PAP – Policy Administration Point
IDP – Indentify Provider (Subject Attributes)
ACD – Access Control Decision

Component Origin
- Vendor Provided
- VA Provided
- VA Provided

HITSP

OASIS