XSPA

Cross-Enterprise Security and Privacy Authorization

HITSP

OASIS

Interop

Goal:

•Demonstrate WS-Trust aspects of HITSP TP-20
•Demonstrate SAML aspects of HITSP TP-20
•Satisfy XSPA Use Cases
•Produce real-time outputs of request/responses

Assumptions:

•Access control decision in consumer security domain is black boxed
•Single XACML Policy Decision Point is made available to all participants for testing
•Code is made available to vendors to create on-site test beds
•Clinical data repository and services available in San Diego

Vendor Participation:

•Slides identify components and vendor points to plug-in
•Vendors can chose to host all with exception of clinical repository and services

VA Delivered Components:

•Test clients and services
•Security Admin console – Patient Consent Directives, Object/Action pairings, required Permissions, and purpose of use
•Lite Electronic Health Record Application
•Simplistic tests to validate configurations
•Use Cases
•XACML Policies

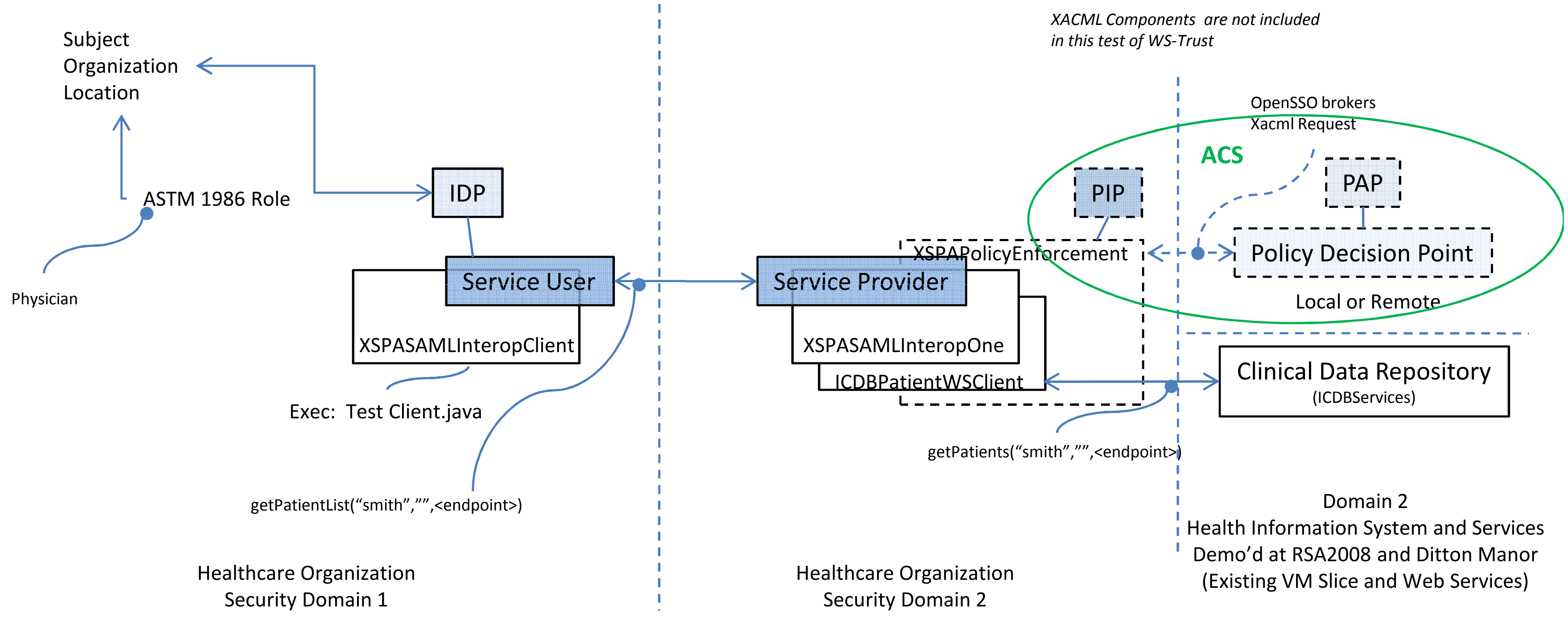
SAML v2.0

XSPA
Cross-Enterprise Security and Privacy Authorization

SAML v2.0 Interop

Coarse Grain Access Control Validation

Simple Patient Lookup – Only ASTM 1986 Role is Required



XACML Components are not included in this test of WS-Trust

Subject
Organization
Location

ASTM 1986 Role

Physician

IDP

Service User

XSPASAMLInteropClient

Exec: Test Client.java

getPatientList(“smith”,””,<endpoint>)

Healthcare Organization
Security Domain 1

Service Provider

XSPASAMLInteropOne

ICDBPatientWSClient

XSPAPolicyEnforcement

getPatients(“smith”,””,<endpoint>)

Healthcare Organization
Security Domain 2

OpenSSO brokers
Xacml Request

ACS

PIP

PAP

Policy Decision Point

Local or Remote

Clinical Data Repository
(ICDBServices)

Domain 2
Health Information System and Services
Demo’d at RSA2008 and Ditton Manor
(Existing VM Slice and Web Services)

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

Component Origin

▨ Vendor Provided
🟦 VA Provided
□ VA Provided

HITSP

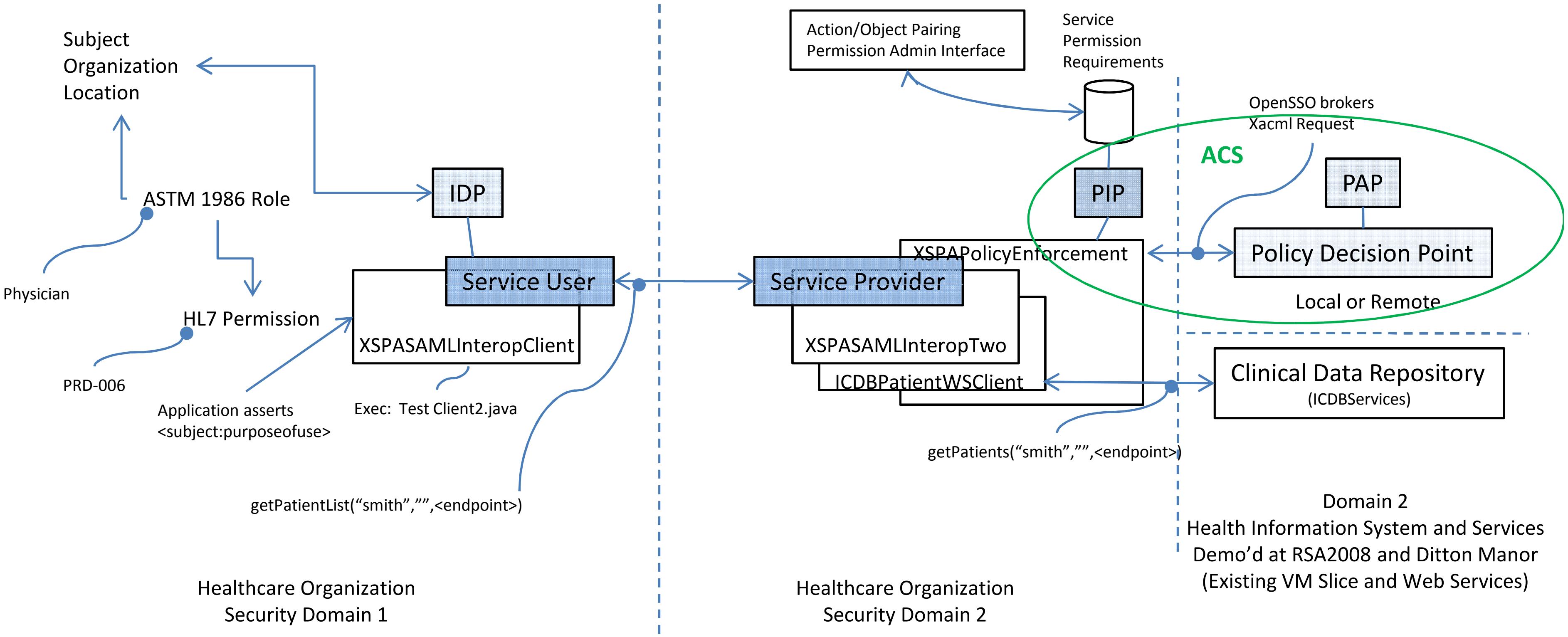
OASIS

XSPA
Cross-Enterprise Security and Privacy Authorization

SAML v2.0 Interop

Fine Grain Access Control Validation

Simple Patient Lookup – Permission Requirements Enforced



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

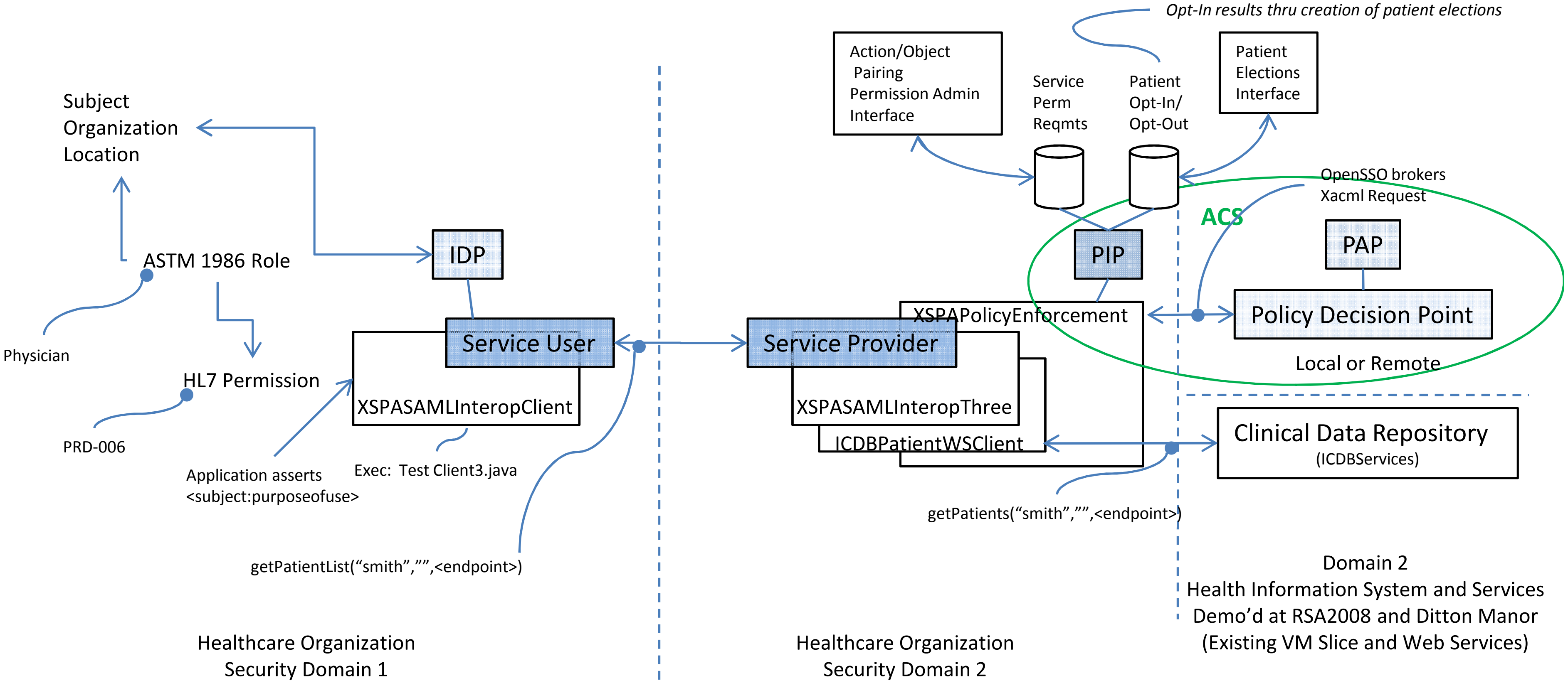
Component Origin

- ▢ Vendor Provided
- 🟦 VA Provided
- □ VA Provided

XSPA
Cross-Enterprise Security and Privacy Authorization

SAML v2.0 Interop
Fine Grain Access Control Validation

Simple Patient Lookup – Permissions Enforced, Patient Consent Directives Enforced
(SAML Version of simplistic Patient Authorization)



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

Component Origin

░ Vendor Provided
▓ VA Provided
□ VA Provided

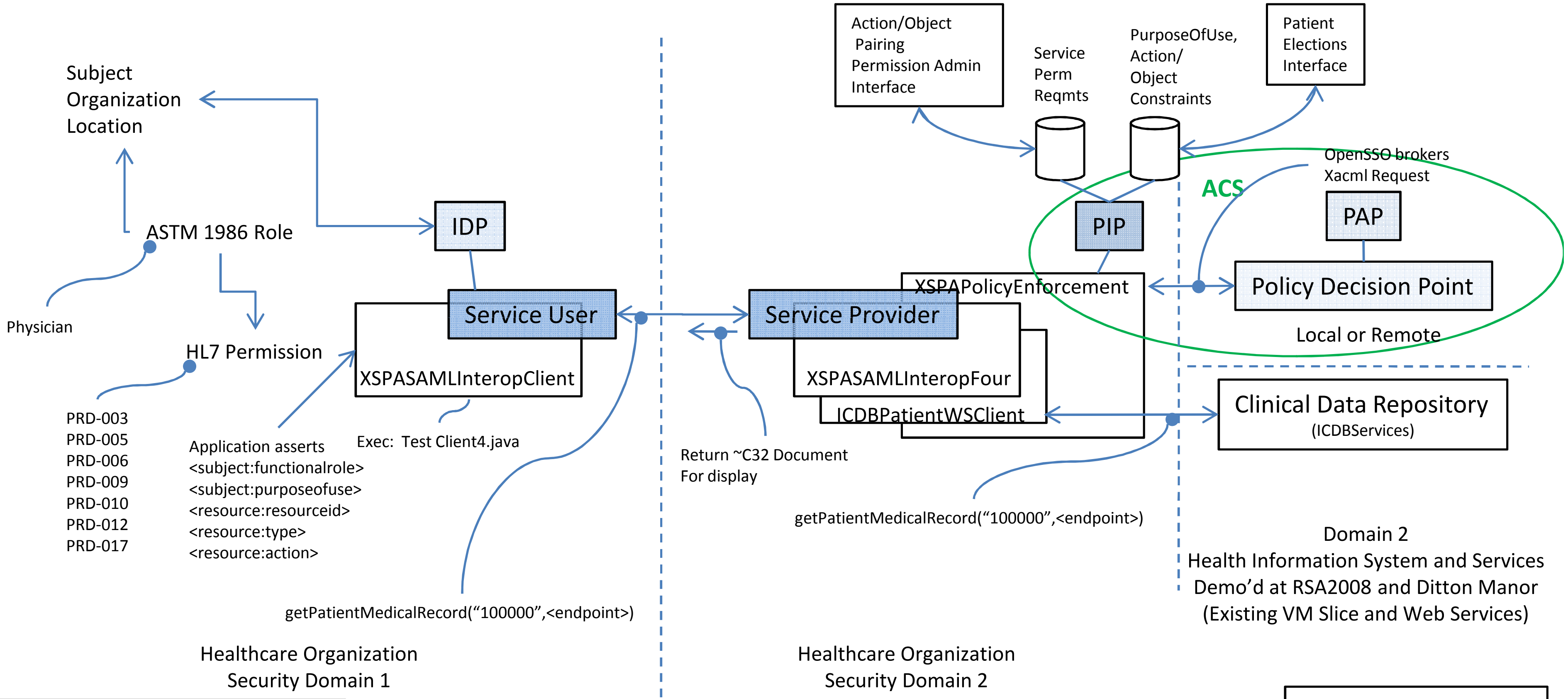
XSPA

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



Subject
Organization
Location

ASTM 1986 Role

Physician

HL7 Permission

PRD-003
PRD-005
PRD-006
PRD-009
PRD-010
PRD-012
PRD-017

IDP

Service User

XSPASAMLInteropClient

Application asserts
<subject:functionalrole>
<subject:purposeofuse>
<resource:resourceid>
<resource:type>
<resource:action>

Exec: Test Client4.java

getPatientMedicalRecord(“100000”,<endpoint>)

Healthcare Organization
Security Domain 1

Action/Object
Pairing
Permission Admin
Interface

Service
Perm
Reqmts

PurposeOfUse,
Action/
Object
Constraints

Patient
Elections
Interface

OpenSSO brokers
Xacml Request

ACS

PIP

PAP

Policy Decision Point

Local or Remote

Service Provider

XSPAPolicyEnforcement

XSPASAMLInteropFour

ICDBPatientWSClient

Return ~C32 Document
For display

getPatientMedicalRecord(“100000”,<endpoint>)

Clinical Data Repository
(ICDBServices)

Domain 2
Health Information System and Services
Demo’d at RSA2008 and Ditton Manor
(Existing VM Slice and Web Services)

Healthcare Organization
Security Domain 2

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

Component Origin

- □ Vendor Provided
- ▨ VA Provided
- □ VA Provided

HITSP

OASIS

WS-Trust

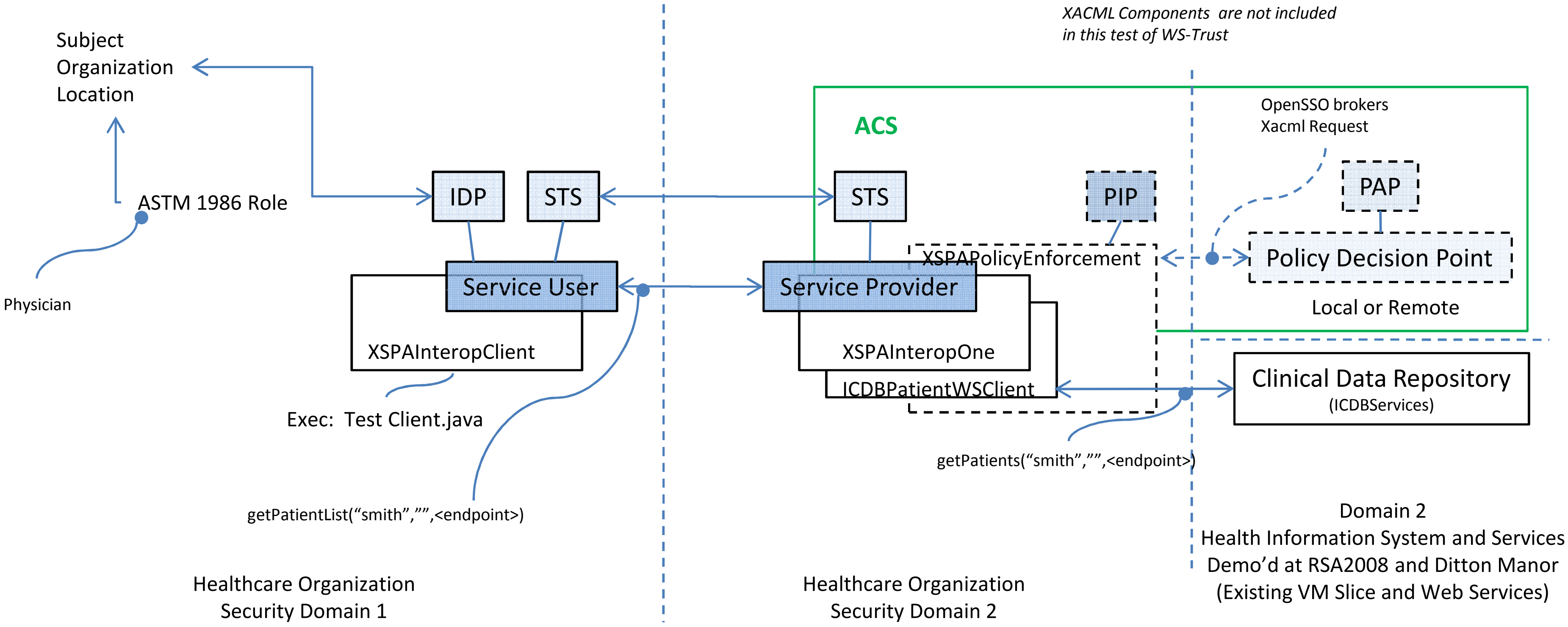
XSPA

Cross-Enterprise Security and Privacy Authorization

WS-Trust Interop

Coarse Grain Access Control Validation

Simple Patient Lookup – Only ASTM 1986 Role is Required



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

Component Origin

▨	Vendor Provided
■	VA Provided
□	VA Provided

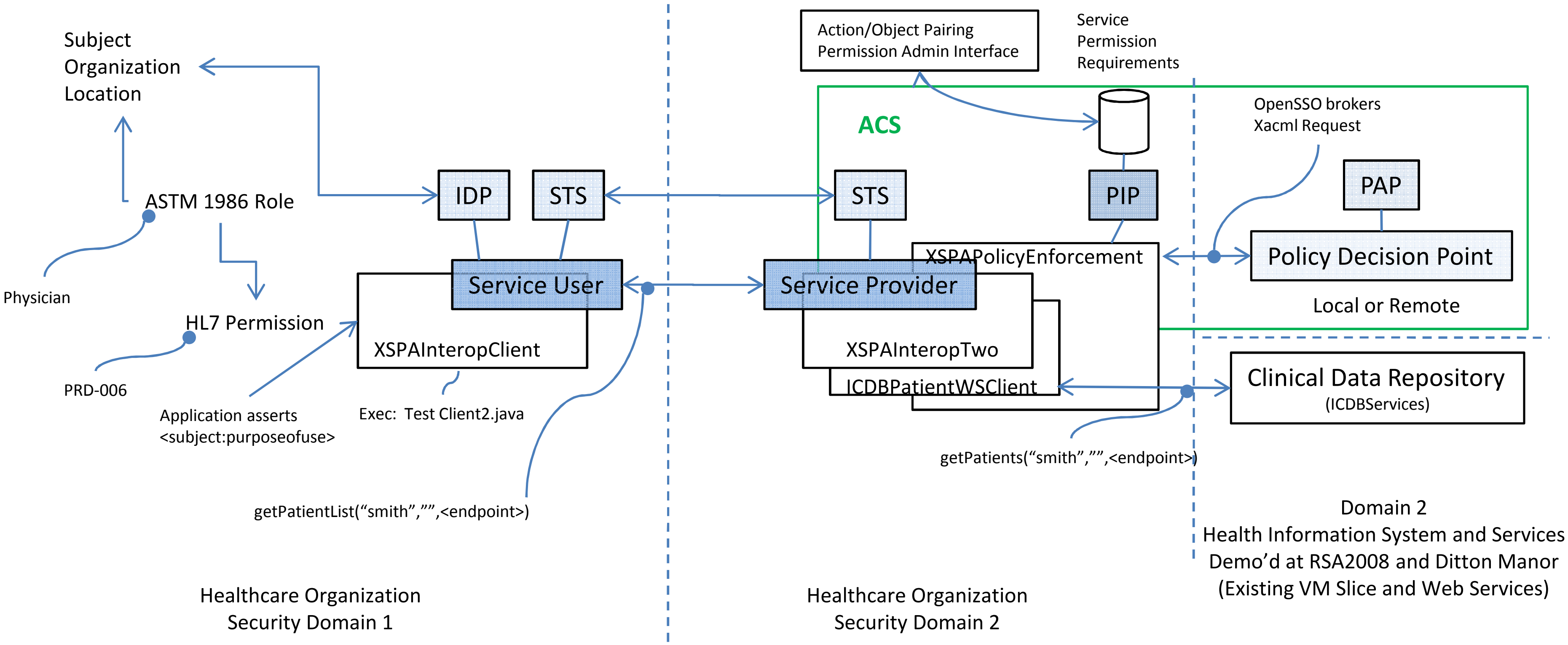
HITSP

OASIS

XSPA
Cross-Enterprise Security and Privacy Authorization

WS-Trust Interop
Fine Grain Access Control Validation

Simple Patient Lookup – Permission Requirements Enforced



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

Component Origin

▨	Vendor Provided
■	VA Provided
□	VA Provided

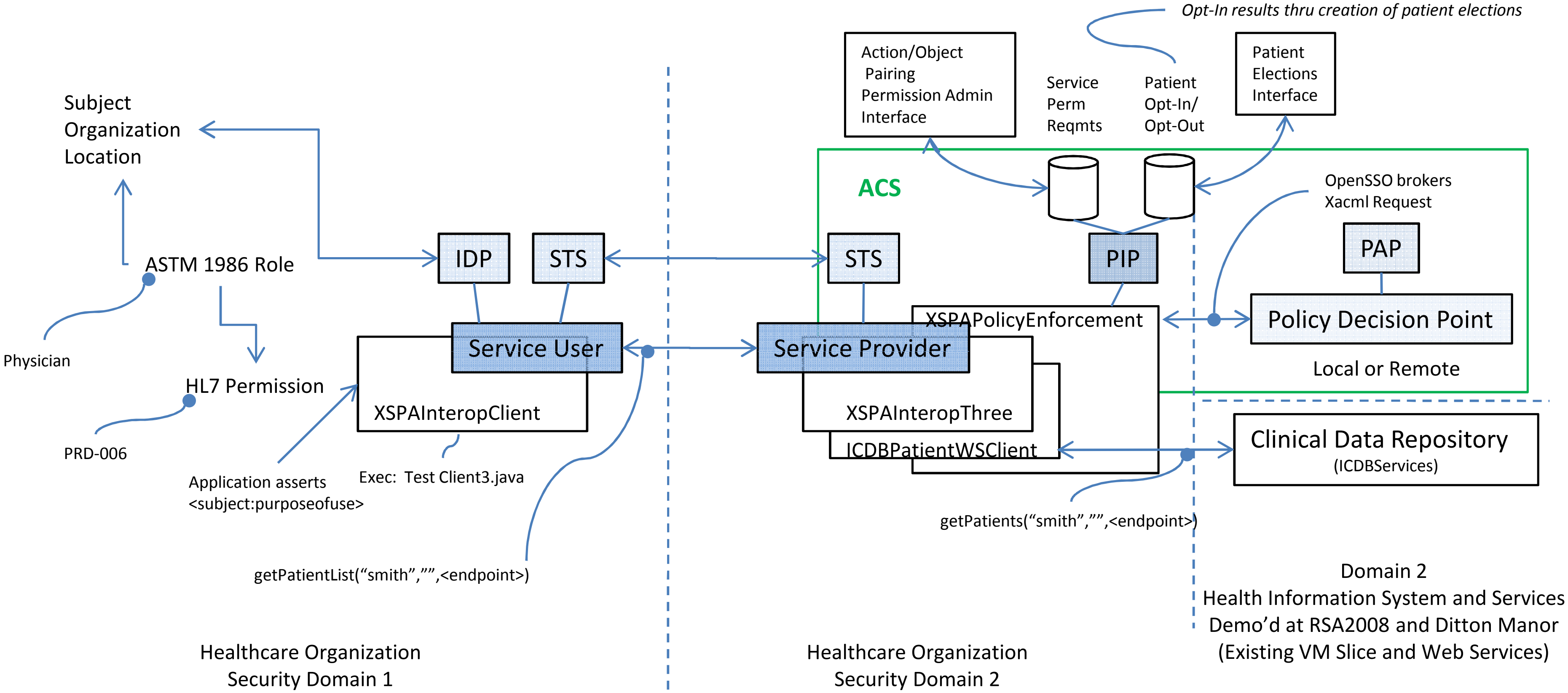
XSPA

Cross-Enterprise Security and Privacy Authorization

WS-Trust Interop

Fine Grain Access Control Validation

Simple Patient Lookup – Permissions Enforced, Patient Consent Directives Enforced
(WS-Trust Version of simplistic Patient Authorization)



Opt-In results thru creation of patient elections
Action/Object Pairing Permission Admin Interface
Service Perm Reqmts
Patient Opt-In/ Opt-Out
Patient Elections Interface
Subject
Organization
Location
ACS
OpenSSO brokers Xacml Request
PAP
IDP
STS
STS
PIP
ASTM 1986 Role
Physician
HL7 Permission
PRD-006
Service User
XSPAInteropClient
Service Provider
XSPAPolicyEnforcement
Policy Decision Point
Local or Remote
XSPAInteropThree
ICDBPatientWSClient
Clinical Data Repository (ICDBServices)
Application asserts <subject:purposeofuse>
Exec: Test Client3.java
getPatientList("smith","",<endpoint>)
getPatients("smith","",<endpoint>)
Domain 2
Health Information System and Services
Demo'd at RSA2008 and Ditton Manor
(Existing VM Slice and Web Services)
Healthcare Organization
Security Domain 1
Healthcare Organization
Security Domain 2

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

Component Origin

▨	Vendor Provided
■	VA Provided
□	VA Provided

HITSP

OASIS

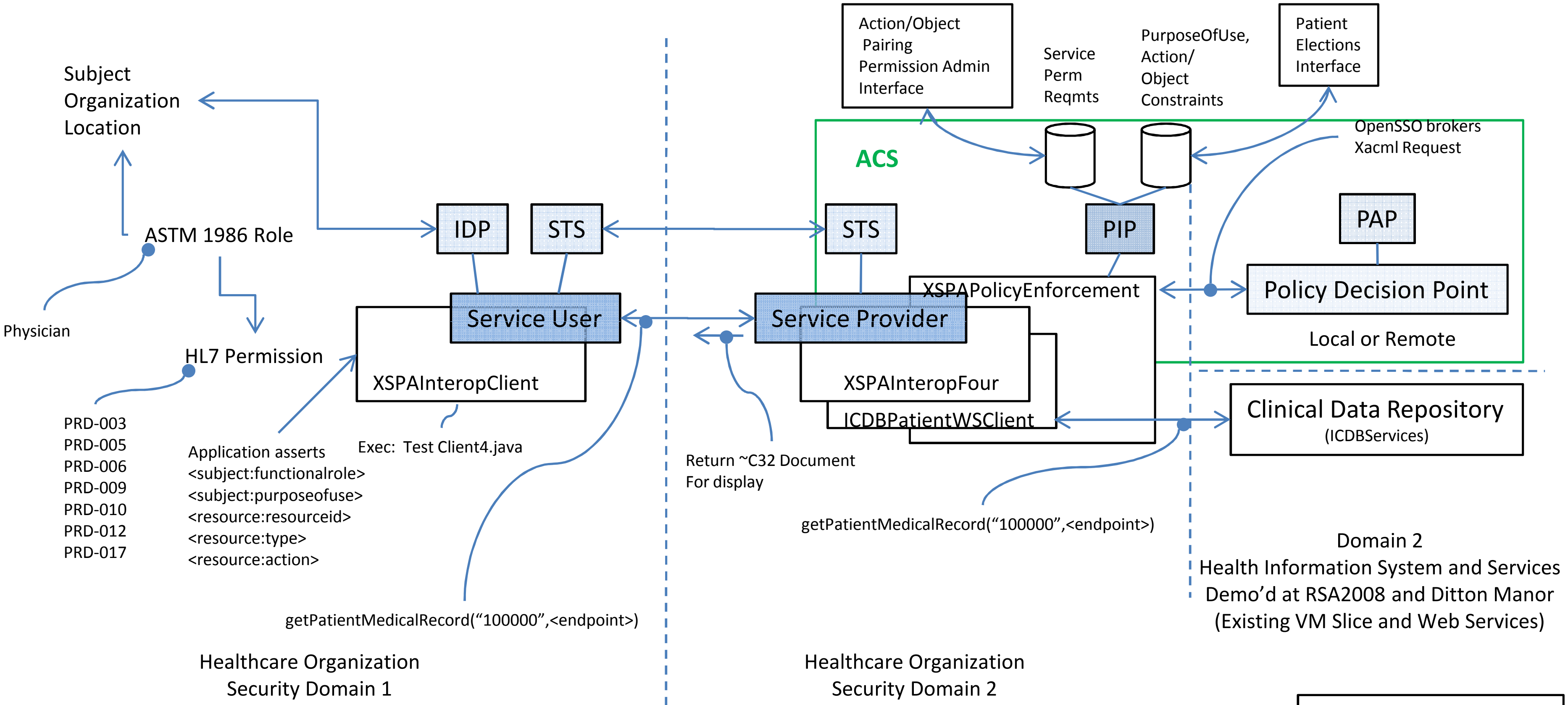
XSPA

Cross-Enterprise Security and Privacy Authorization

WS-Trust 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)

Component Origin

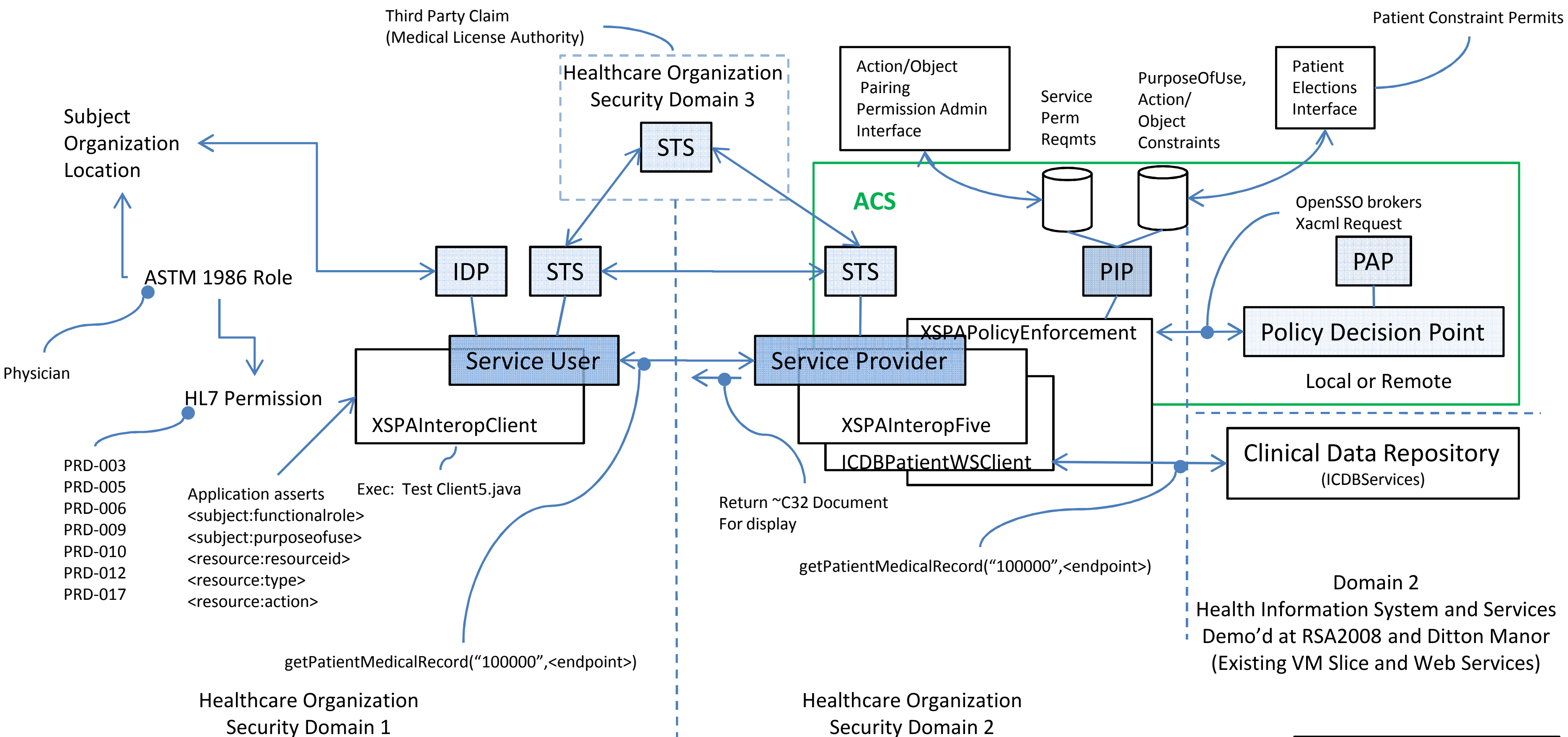
▨ Vendor Provided
■ VA Provided
□ VA Provided

XSPA Cross-Enterprise Security and Privacy Authorization

WS-Trust Interop

Fine Grain Access Control Validation

Multi-Party Authorization Request – Access Requires Additional Claim



Third Party Claim
(Medical License Authority)

Healthcare Organization
Security Domain 3

STS

Subject
Organization
Location

ASTM 1986 Role

Physician

HL7 Permission

PRD-003
PRD-005
PRD-006
PRD-009
PRD-010
PRD-012
PRD-017

IDP

STS

Service User

XSPAInteropClient

Application asserts
<subject:functionalrole>
<subject:purposeofuse>
<resource:resourceid>
<resource:type>
<resource:action>

Exec: Test Client5.java

getPatientMedicalRecord(“100000”,<endpoint>)

Healthcare Organization
Security Domain 1

Action/Object
Pairing
Permission Admin
Interface

Service
Perm
Reqmts

PurposeOfUse,
Action/
Object
Constraints

Patient
Elections
Interface

Patient Constraint Permits

ACS

STS

PIP

OpenSSO brokers
Xacml Request

PAP

Policy Decision Point

Local or Remote

XSPAPolicyEnforcement

Service Provider

XSPAInteropFive

ICDBPatientWSClient

Return ~C32 Document
For display

getPatientMedicalRecord(“100000”,<endpoint>)

Clinical Data Repository
(ICDBServices)

Domain 2
Health Information System and Services
Demo’d at RSA2008 and Ditton Manor
(Existing VM Slice and Web Services)

Healthcare Organization
Security Domain 2

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

Component Origin

▨ Vendor Provided
■ VA Provided
□ VA Provided