



OPEN HEALTH TOOLS

Privacy, Access and Security Services (PASS)

November 15, 2007



Charter-- Overview

- **This charter was developed in accordance with the Open Health Tools Development Process and will outline the mission and scope of the Privacy, Access and Security Project (PASS).**

Charter-- Mission

- **The mission of the Privacy, Access and Security Services project is to provide a set of encapsulated, loosely-coupled and composable service components that can contribute to ensuring the confidentiality and integrity of healthcare information within a service-oriented environment.**
- **The PASS project is intended to:**
 - build upon open standards and profiles,
 - allow developers to focus on clinical and business solutions, rather than healthcare security and privacy issues,
 - facilitate interoperability in the healthcare environment, and
 - support realization of the Open Health Tools architectural vision.

Charter-- Scope

- **PASS addresses issues of entity authentication, authorization, access control and accountability, including**
 - Security Services
 - Identity Services
 - Privacy Services
 - Access Services
 - Audit Services
- **In addition to these basic services, PASS expects to provide higher level services providing security and privacy infrastructure supporting OHT service consumers, service providers and**

Charter– IP Issues

- None

Charter– Deviations

- None

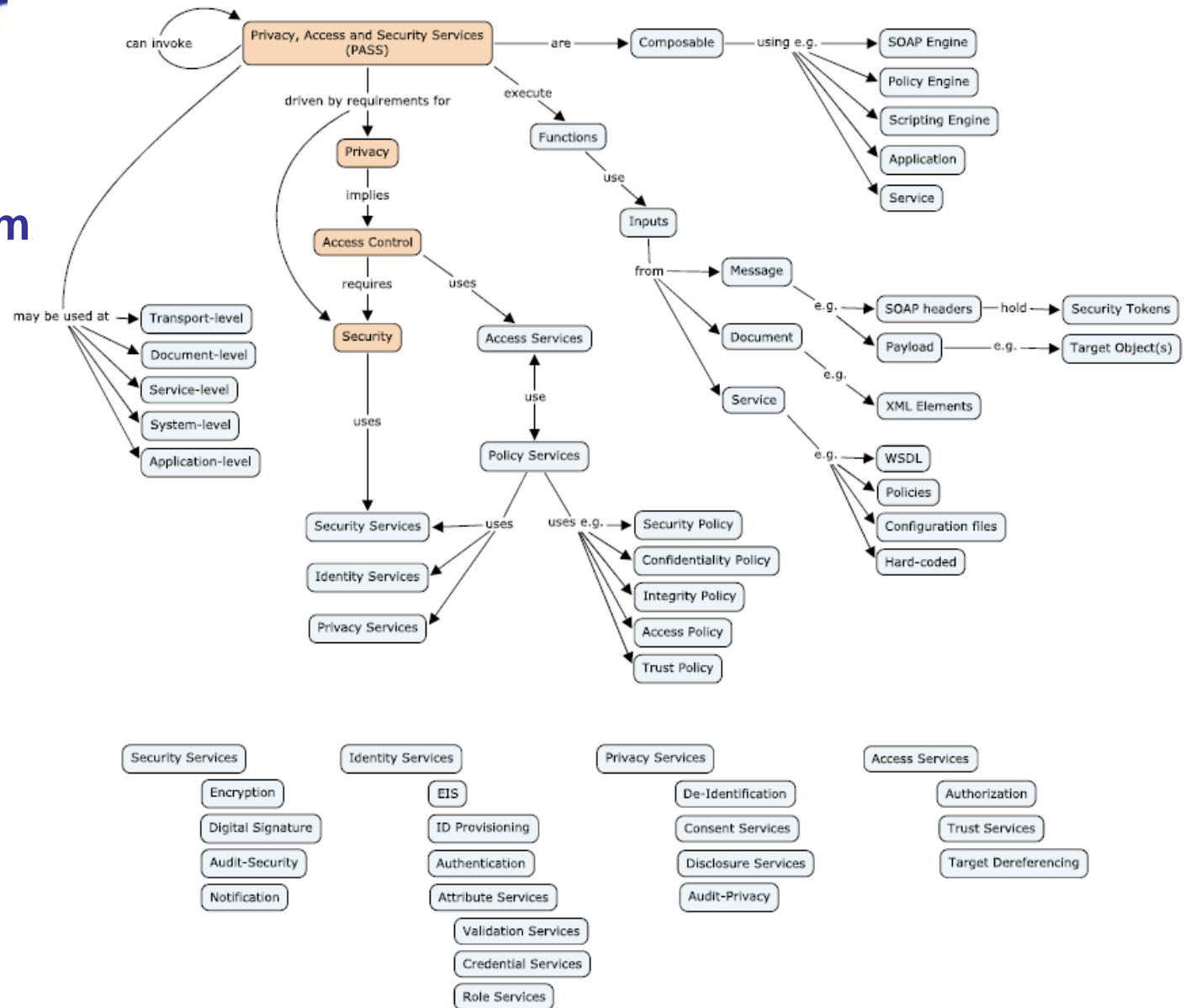
Security as an Afterthought

- **SDOs**
 - Acknowledge the need, but...
- **Developers**
 - Get it done, but...
- **Net effect**
 - Not architected
 - Tightly bound to applications
 - Often inadequate
 - Almost always inconvenient

HSSP PASS

- The Service Functional Model (SFM) for each PASS component defines both the functional capabilities accessible through its provided interfaces and any external service dependencies. PASS SFMs are intended to be technology neutral, platform neutral and complementary to existing specifications.

HSSP PASS Concept Diagram



Security-as-a-Service

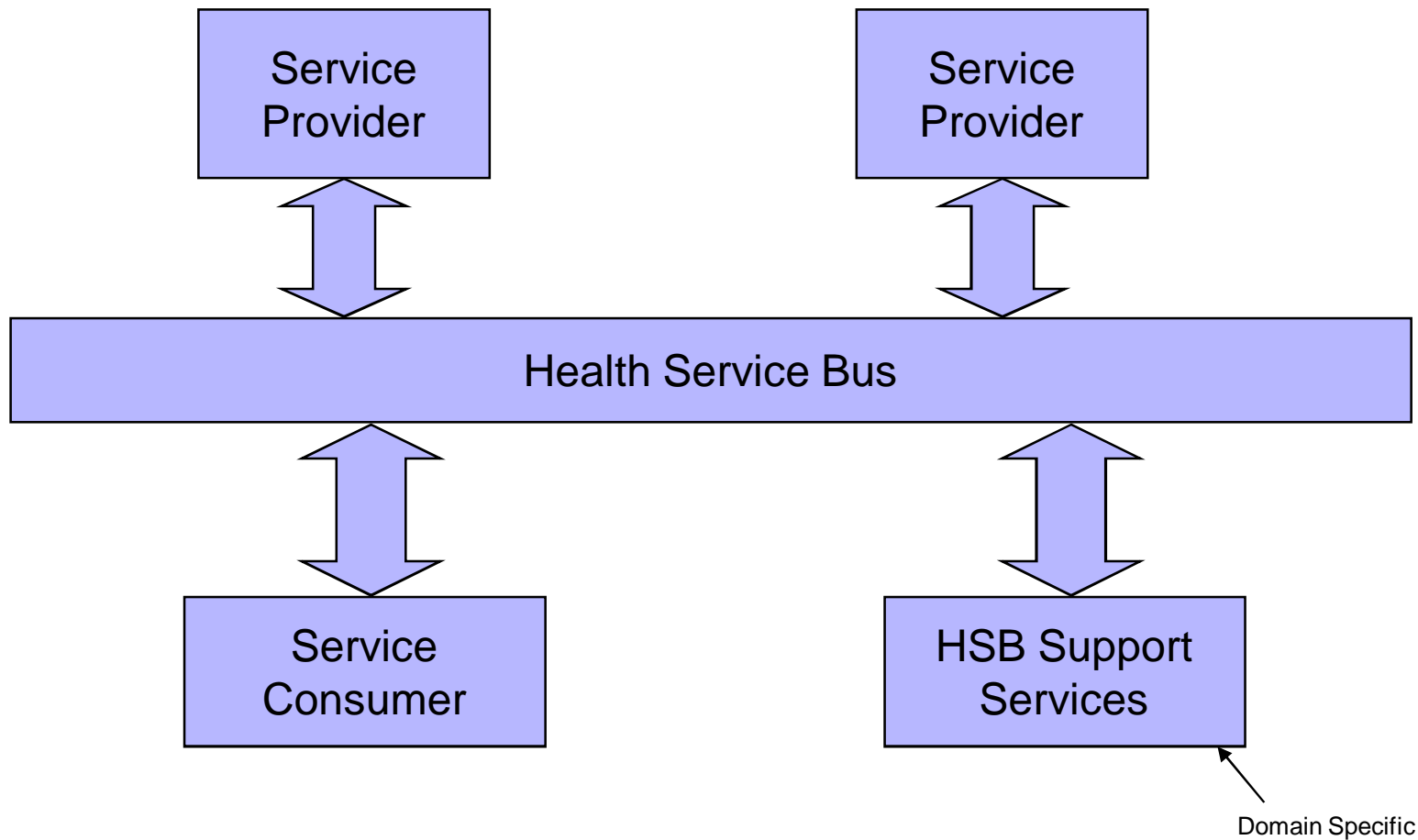
- **Security-as-a-Service within an SOA-oriented architecture implies the decomposition and decoupling of complex security processes that are typically integrated across infrastructure and applications into a set of encapsulated, loosely-coupled security/privacy services.**

Security-as-a-Service

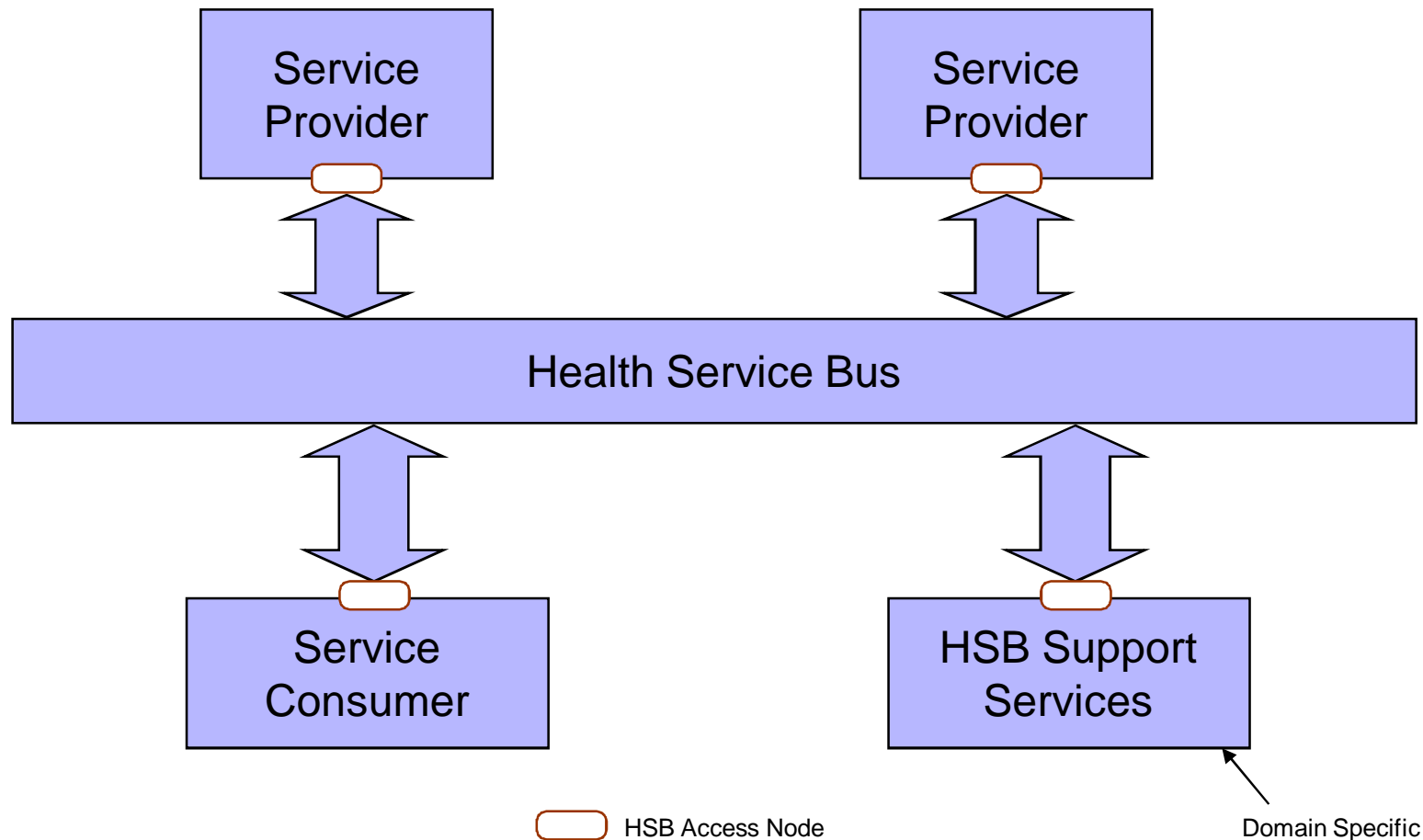
- Security-as-a-Service within an SOA-oriented architecture implies the decomposition and decoupling of complex security processes that are typically integrated across infrastructure and applications into a set of encapsulated, loosely-coupled security/privacy services.

Push security to the edge

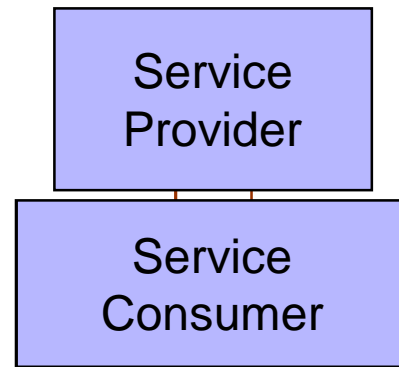
Technical Architecture Overview



Technical Architecture Overview



Technical Architecture Overview



Standards and Profiles

- **WS-HL7 DSTU**
- **IHE ATNA Profile**
 - SSL/TLS
 - Audit
- **HSSP PASS**
- **WS-Security**
- **WS-Trust**
- **SAML**
- **WS-Federation**
- **WS-Policy**
- **XACML**
- **HSSP Entity Identification Service**
- **WS-***

And still we don't have coverage of key healthcare security/privacy use cases...

Pushing Security to the Edge

- Benefits
 - Developers can focus on clinical and business solutions
 - An enabler of payload-neutral messaging infrastructure that maintains healthcare information integrity and confidentiality
 - An enabler of policy-driven approaches to meeting security, privacy and trust requirements
 - An enabler of alternative, flexible architectures that may facilitate organizational convergence
 - Reduces inadvertent tight coupling of services due to security requirements

Subproject possibilities

- **HSB Access Node (includes Policy Enforcement Point)**
 - HL7
 - ISO compatible
 - IHE compatible
 - HITSP compatible
 - WS compatible
- **Policy Decision Point**
- **EIS Implementation**
 - HSSP compatible
 - IHE compatible
- **Workstation Security/Privacy Backplane**
- ...

Next Steps

- **Reference Architecture**