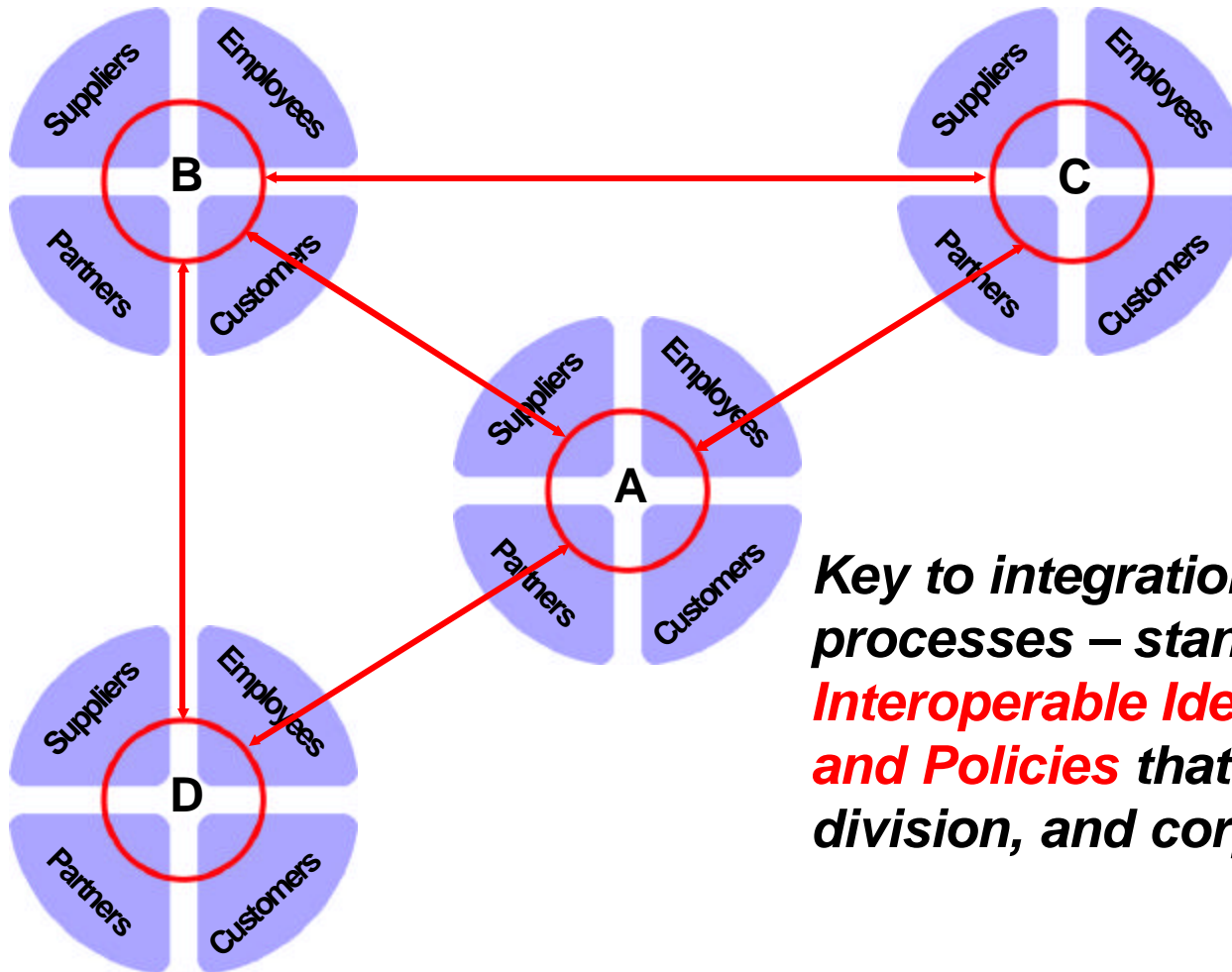
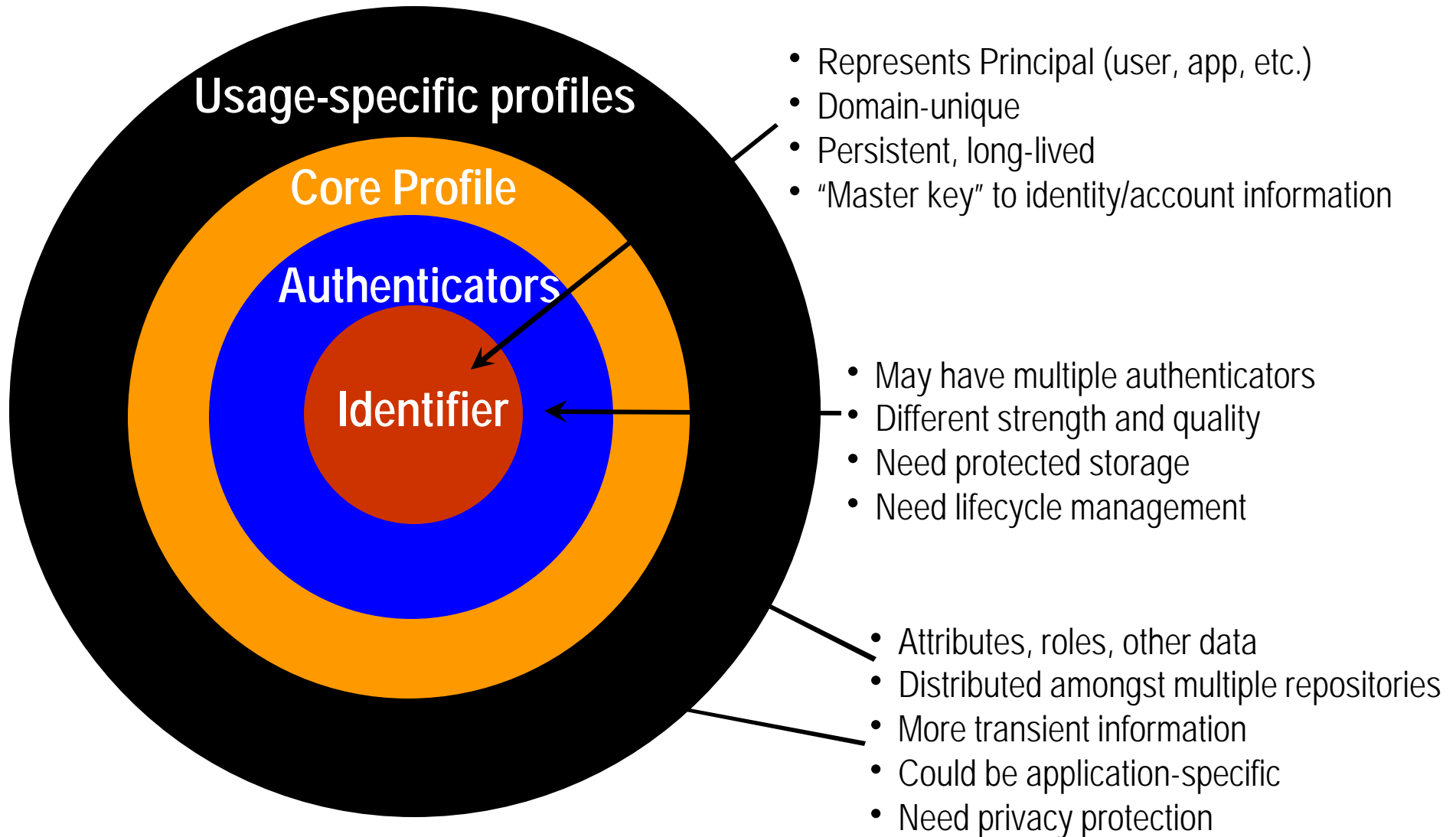


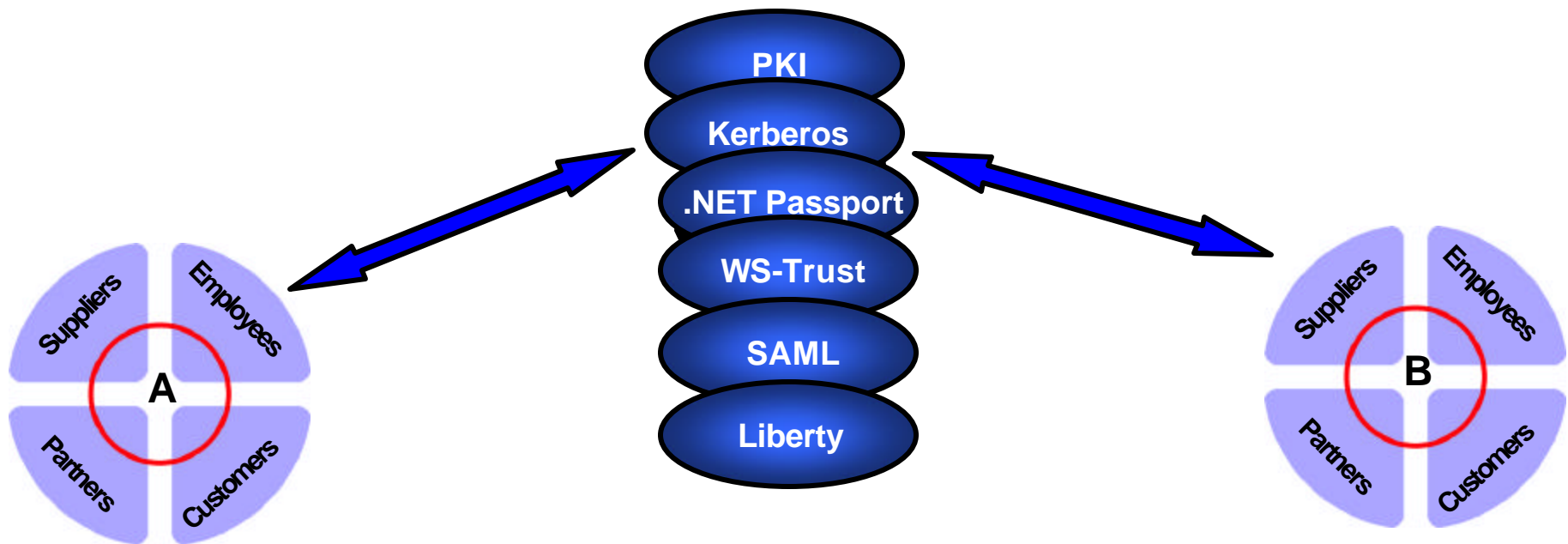
Liberty Identity System role in securing Web Services

***Slava Kavsan, Chief Technologist
RSA Security Inc.***



Key to integration of business processes – standards-based *Trusted Interoperable Identities, Credentials and Policies* that cross application, division, and corporate boundaries





LIBERTY ALLIANCE PROJECT

Liberty Alliance Project

About 160 for-profit, not-for-profit and government organizations representing a billion customers

Sample of Liberty members



LIBERTY IDENTITY FEDERATION FRAMEWORK (ID-FF)

Enables identity federation and management through features such as identity/account linkage, simplified sign-on, and basic session management

LIBERTY IDENTITY SERVICES INTERFACE SPECIFICATIONS (ID-SIS)

The schema and instantiation of the technical Implementation as defined by ID-WSF to provide for interoperable identity services. Such specifications defined at the Liberty Alliance and elsewhere might include personal identity service, contact book service, geo-location service, presence service and so on

LIBERTY IDENTITY WEB SERVICES FRAMEWORK (ID-WSF)

This module will provide the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles

SAML

HTTP

WSS

WSDL

XML Enc

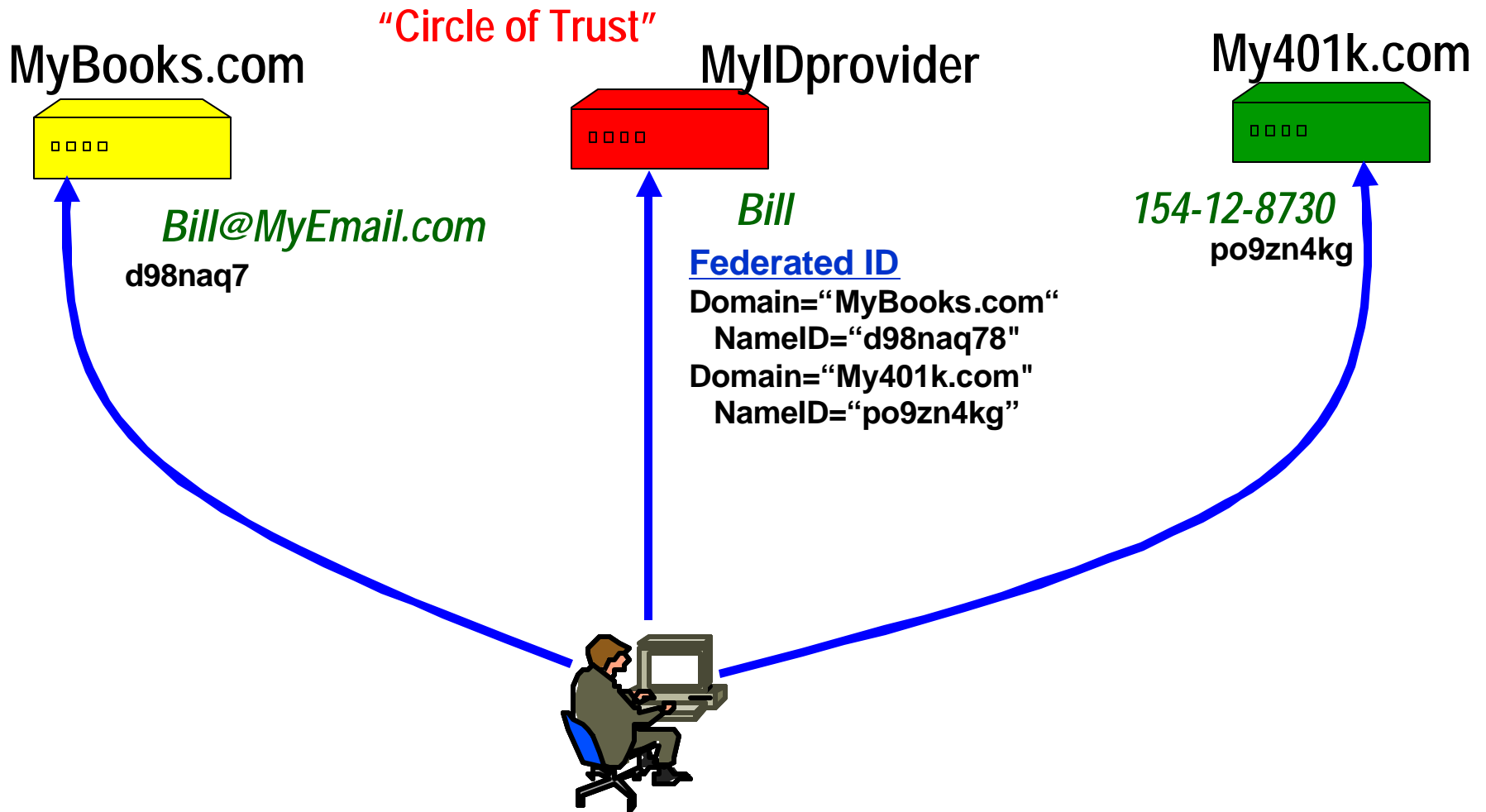
WAP

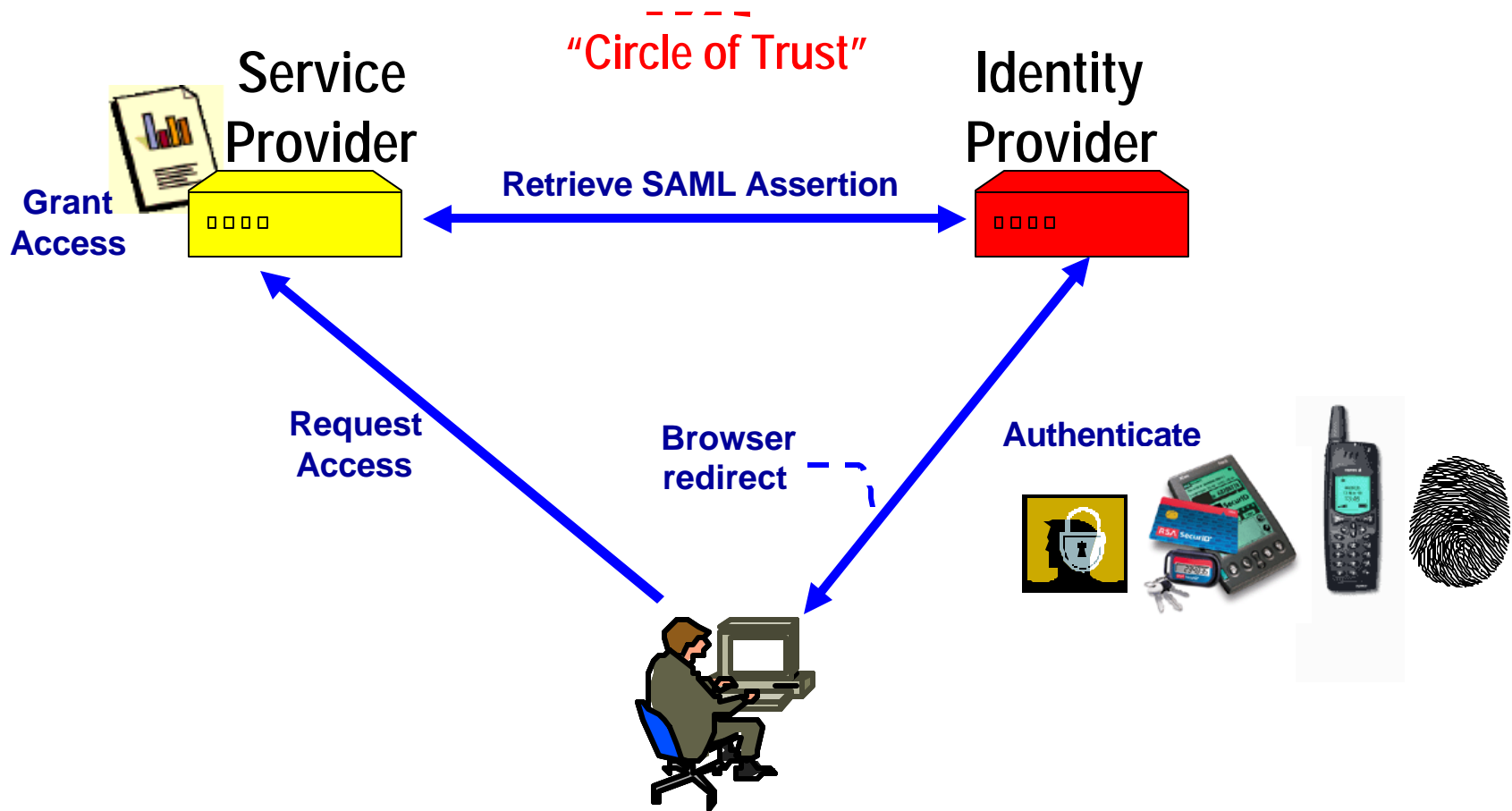
XML

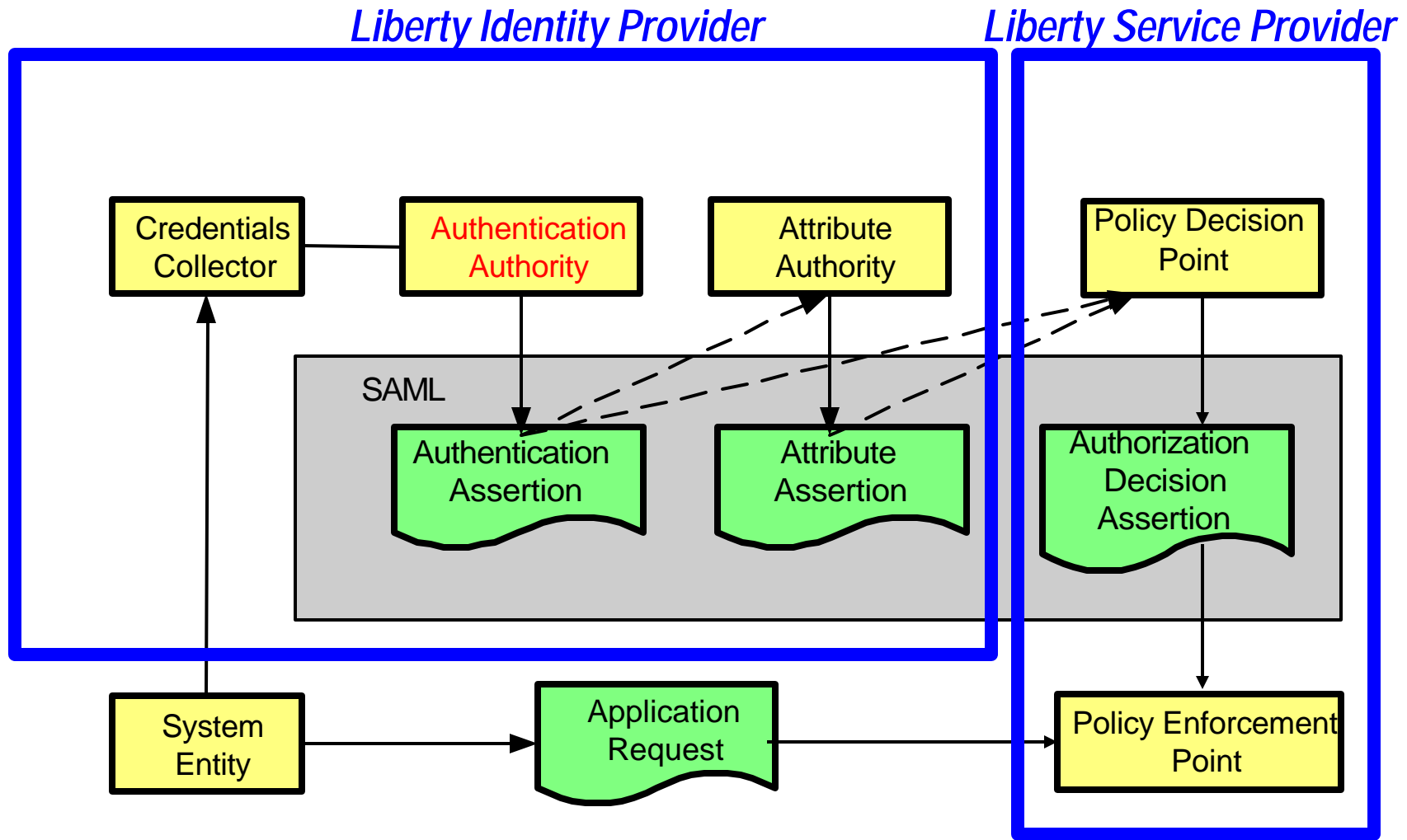
SSL/TLS

SOAP

XML-DSIG







- **Facilitating Trust Infrastructure within Web Services-enabled community**
- **Enabling SSL connections**
- **Signing XML, SOAP, WS-Security Tokens and protocol messages**
- **User Authentication Method (X.509)**
- **Binding asserted Security Tokens to the Subject**

Cryptographic Trust

Business Trust

	Direct (shared secret or Public Keys)	Indirect (common or inter-trusted Root CAs or KDCs)	None (possibly non crypto-based)
Direct (bilateral agreements)	Pairwise Trust	Pairwise Trust	Unsecured Operation
Indirect (chain of agreements)	Brokered Trust	Brokered Trust	Unsecured Operation
None (possibly via membership in the same business community)	Community Trust	Community Trust	Community Trust (weak case)

- Trust Models are not mutually exclusive and can be hybridized
- Different levels of trusts characterizing these Trust Models can be used to control resource access policies
- Various scalability/trust-level/complexity tradeoffs for each model
- Liberty Alliance published a non-normative document describing these models, tradeoffs and implementation guidelines
- Liberty Alliance published protocol specifications necessary to implement these trust models as well as security mechanisms to enable “basic” delegation