S3-030718

Liberty Alliance Project

Setting the Standard
for Federated Network Identity

Timo Skyttä
Nokia Mobile Software
Strategic Architecture

Today’s Agenda

※Liberty Alliance Background

※The Business Case for Federated Identity

※Liberty Momentum & Progress

※Federated Identity: Not Just A Technology Issue

※Architecture & Circle of Trust

Liberty Alliance Vision

Mission:

To serve as the premier open Alliance for federated network identity management & services by ensuring interoperability, supporting privacy and promoting adoption of its specifications, guidelines and best practices.

Goals:

- Provide open standard and business guidelines for federated identity management spanning all network devices
- Provide open and secure standard for SSO with decentralized authentication and open authorization
- Allow consumers/businesses to maintain personal information more securely, and on their terms

What is the Liberty Alliance ?

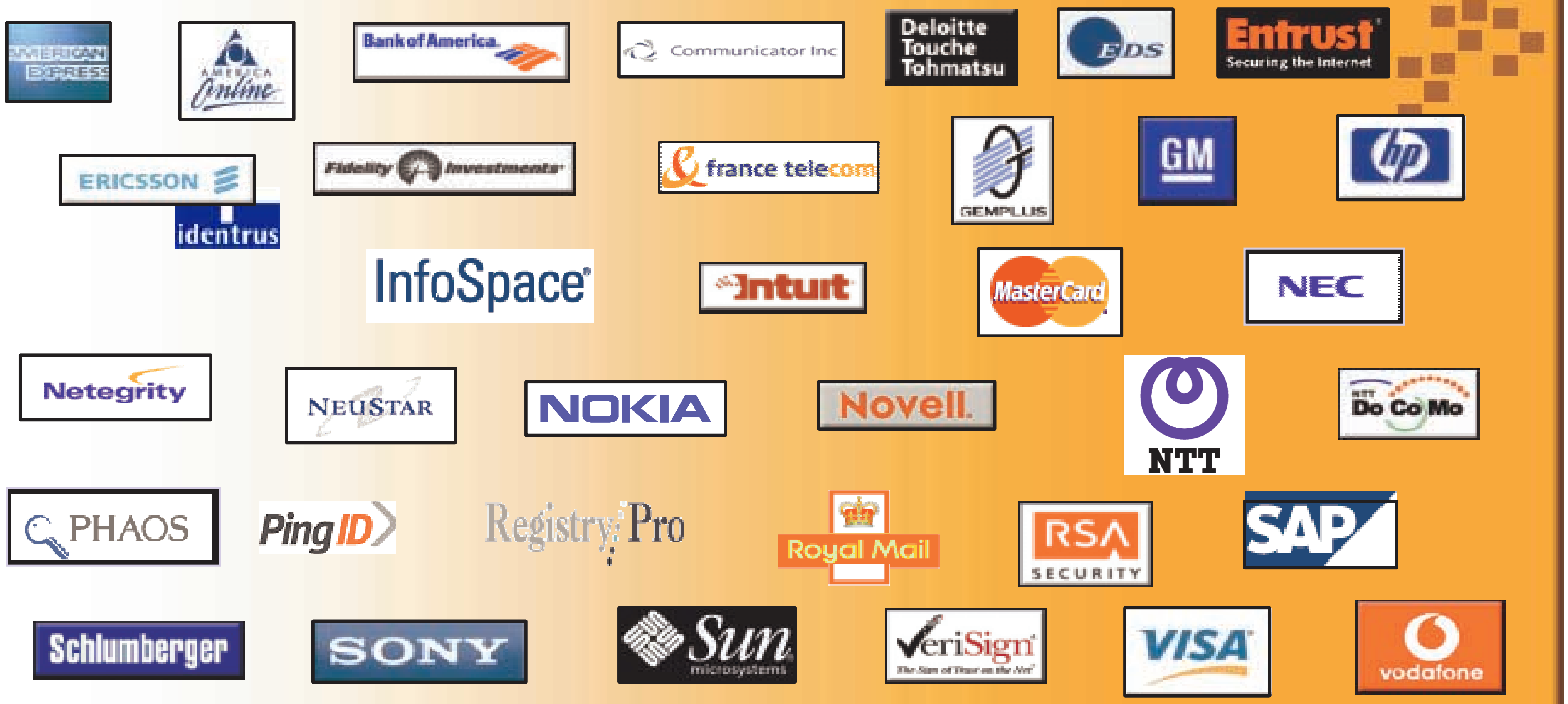
- A **business** alliance, formed in Sept 2001 with the goal of establishing an open standard for federated identity management
- Global membership consists of consumer-facing companies and technology vendors as well as policy and government organizations
- The only open organization working to address the technology and business issues of federated identity management

LIBERTY ALLIANCE PROJECT

Who is the Liberty Alliance today?

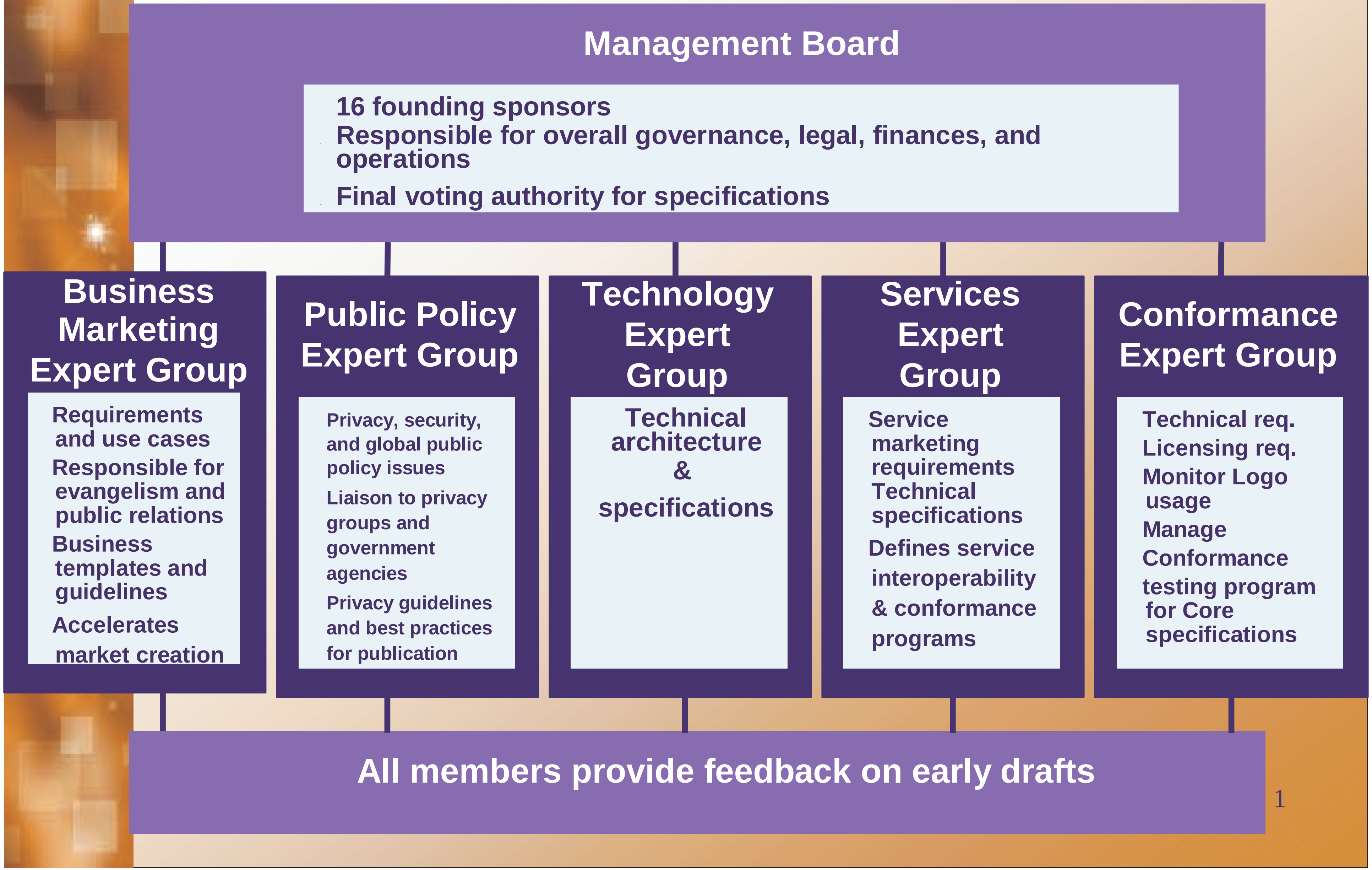
Over 150 for-profit, not-for-profit and government organizations, representing a billion customers, are currently Alliance members

The following represent Liberty's Board Members and Sponsors



LIBERTY ALLIANCE PROJECT

How does Liberty work ?



Management Board

- 16 founding sponsors
- Responsible for overall governance, legal, finances, and operations
- Final voting authority for specifications

Business Marketing Expert Group

- Requirements and use cases
- Responsible for evangelism and public relations
- Business templates and guidelines
- Accelerates market creation

Public Policy Expert Group

- Privacy, security, and global public policy issues
- Liaison to privacy groups and government agencies
- Privacy guidelines and best practices for publication

Technology Expert Group

Technical architecture & specifications

Services Expert Group

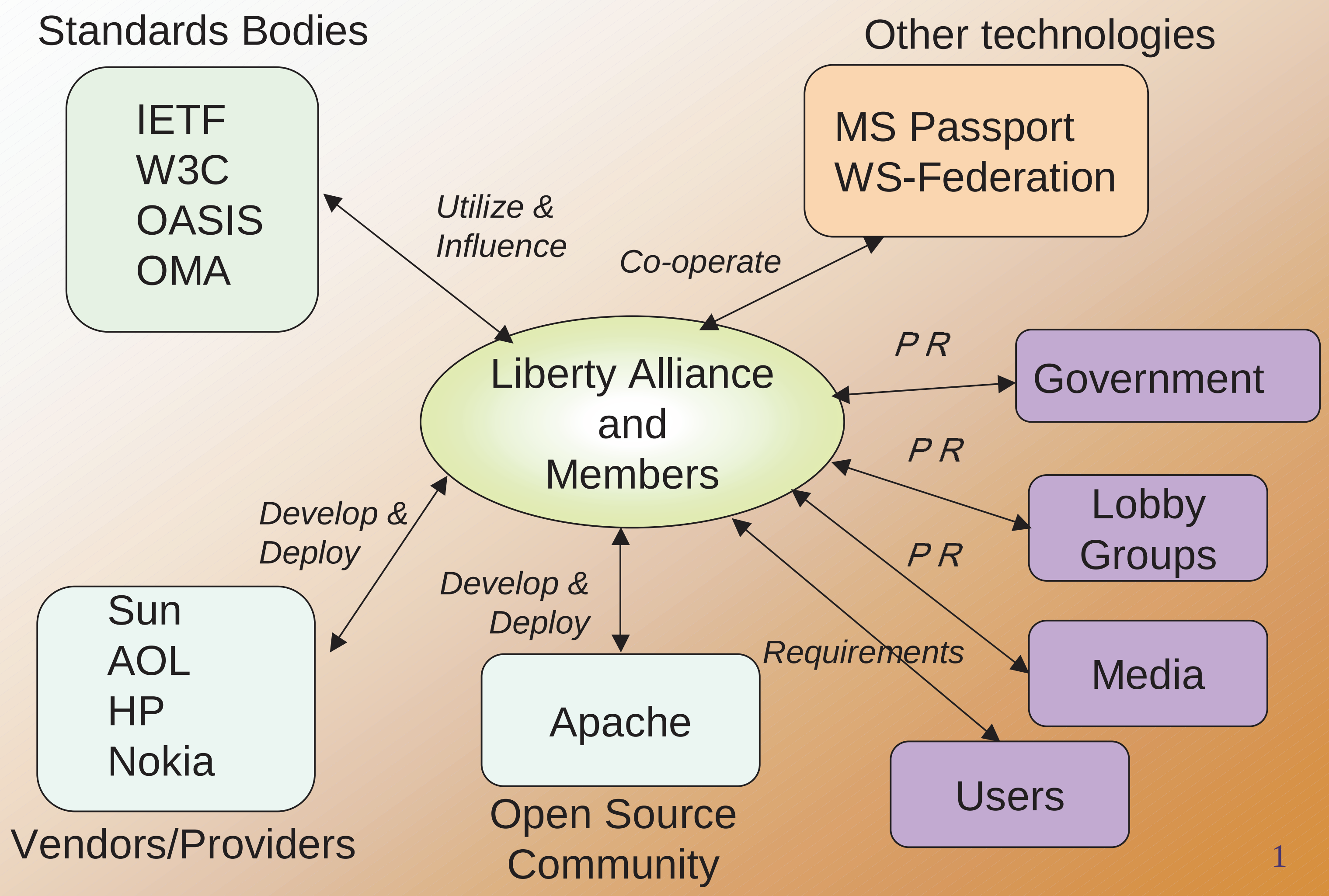
- Service marketing requirements
- Technical specifications
- Defines service interoperability & conformance programs

Conformance Expert Group

- Technical req.
- Licensing req.
- Monitor Logo usage
- Manage Conformance testing program for Core specifications

All members provide feedback on early drafts

Open Interaction and Participation



Standards Bodies

IETF
W3C
OASIS
OMA

Other technologies

MS Passport
WS-Federation

Liberty Alliance and Members

Government

Lobby Groups

Media

Users

Sun
AOL
HP
Nokia

Vendors/Providers

Apache

Open Source Community

LIBERTY ALLIANCE PROJECT

Defining Liberty

Liberty Alliance IS…

※ IS a member community delivering technical specifications, business and privacy best practices

※ IS providing a venue for testing interoperability and identifying business requirements

※ IS developing an open, federated identity standard that can be built into other companies’ branded products and services

※ IS driving convergence of open standards

Liberty Alliance IS NOT

※ IS NOT a consumer-facing product or service

※ IS NOT developed and supported by one company

※ IS NOT based on a centralized model

The Business Case

The Role of Federated Identity in Web Services

“Federated Identity Management is a strategic capability that will solve real business problems”

Burton Group, July 2003

LIBERTY ALLIANCE PROJECT

The Problem Today

1. Companies need solutions
   1. How to leverage new trends to generate revenue
   2. How to lower lower costs
   3. And still address customer worries about privacy & security

- Companies are spending billions of dollars on Web Service projects (figures vary by analyst)
  - Very few enterprises have completed projects

- Current barriers to wide-scale adoption
  - Lack of technical standards for managing identity
  - Lack of interoperability between products and services
  - Lack of a federated model
  - Lack of privacy and security best practices
  - Lack of business best practices

Identity problems exploding:

- No common method to approach identity
- Fragmentation of customers identities across different many different sources
- Growing privacy / regulatory pressures
- Increasing potential and risk of identity theft
- Convergence of internet and mobile world
- Desire to provide higher value-add services to customers

Industries Ready for Federated Identity

- **Wireless**
  - Number Portability Act – enabling customers to retain their mobile phone number when changing carriers
  - Emerging privacy legislation makes use of phone number as an identifier towards services quite difficult
  - Limited data entry capabilities (small screens, small keypads)
  - Users want immediate access to personalized services
  - Exploitation of data services and m-commerce
- **Finance**
  - State and national legislation driving need to protect privacy and identity
  - Increasing opportunity to drive new partnerships and initiatives dependent upon identity initiatives
- **Healthcare**
  - HIPAA legislation – organizations are responsible for ensuring identifiable information is protected while stored or in transit
- **Government**
  - Increasing incentives for e-filing and online tax returns
  - Bush administration's eAuthentication mandate (led by GSA)

Liberty Progress & Momentum

Recent Accomplishments

January 2002 – Liberty begins specification development

July 2002 – Liberty releases Phase 1 specifications

April 2003 – Liberty releases Phase 2 specification drafts;
demonstrates interoperability among 20 products;
donates Phase 1 specifications to OASIS (SAML)

June 2003 – Liberty releases first business guidelines;
releases Phase 1 Japanese specifications

October 2003 – Conformance Program and "Multitrack" model
for Services development (Services EG)

November 2003 – Phase 2 Specifications Finalized
1st Conformance test event in Madrid 11.-14.11.2003

Liberty-enabled products & services

Communicator (available)
Computer Associates (Q4*)
DataKey (available)
DigiGan (Q3*)
Ericsson (Q4)
Entrust (Q1 2004)
France Telecom (Q4 2003)
Fujitsu Invia (available)
Gemplus (TBD)
HP (available)
July Systems (available)
Netegrity (2004)
NeuStar (available)
Nokia (Q4 2003)
Novell (available)
NTT (TBD)
NTT Software (available)
Oblix (2004)
PeopleSoft (available)
Phaos Technology (available)
Ping Identity (available)
PostX (available)
RSA (Q4)
Salesforce.com (TBD)
Sigaba (available)
Sun Microsystems (available)
Trustgenix (available)
Ubisecure (available)
Verisign (Q4*)
Vodafone (2004)
WaveSet (available)

*Delivery dates being confirmed

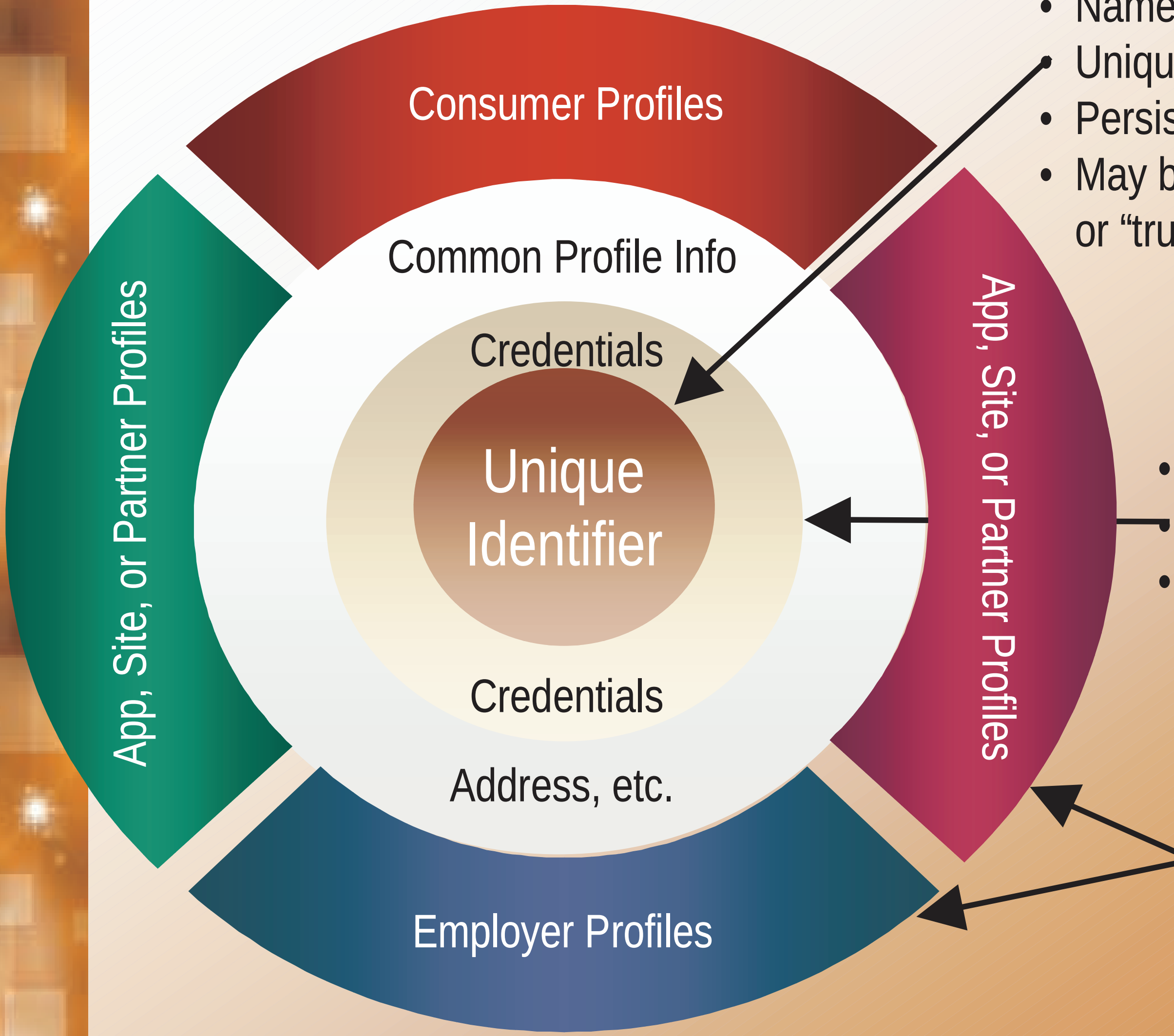
Circle of Trust Concepts & Liberty Architecture

LIBERTY ALLIANCE PROJECT

Identity Management Concepts

What is (digital) identity?

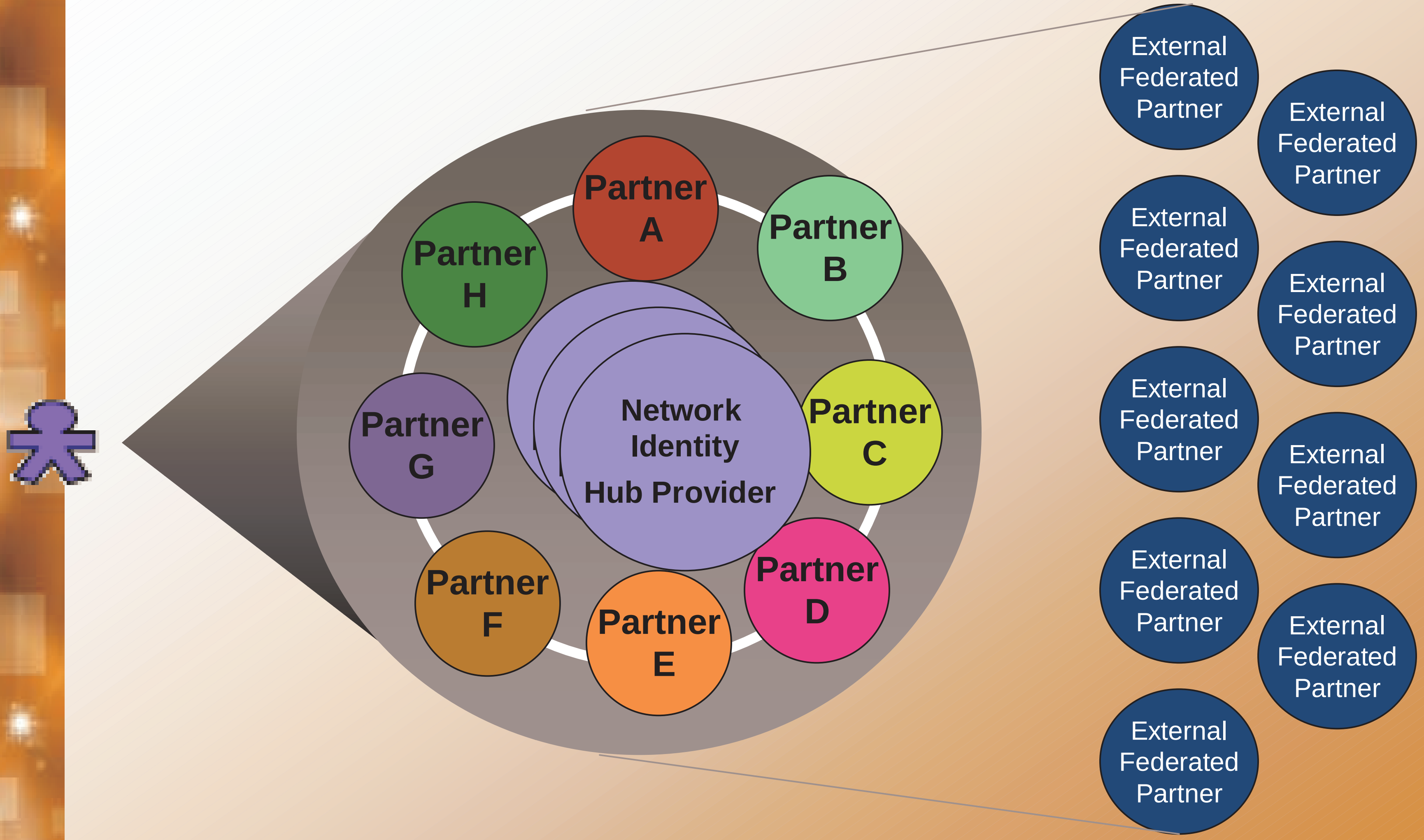
- Represents principals (users, apps, etc.)
- Name, number, other identifier,
- Unique in some scope
- Persistent, long-Lived or one-time
- May be “anonymous” ,“pseudonym” or “true name”



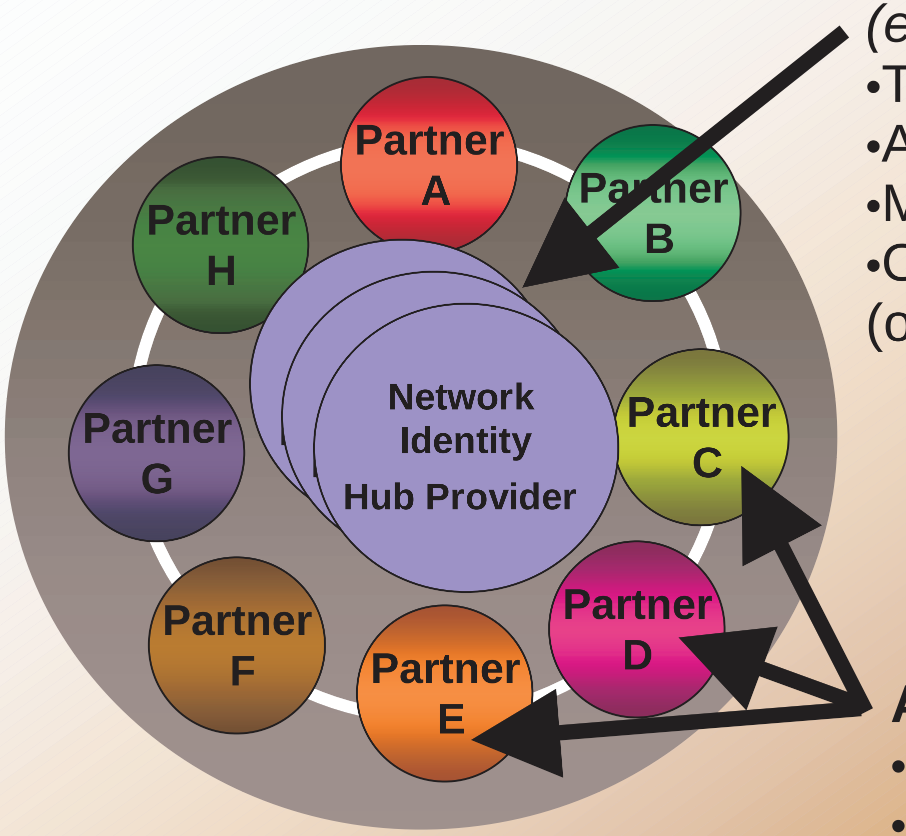
- May have multiple credentials
- Different strengths, different apps
- Can change w/more frequency

- Attributes, entitlements, policies
- More transient, fluid information
- Often specific to apps or sites

"Circle of Trust" Concept


Partner A
Partner B
Partner C
Partner D
Partner E
Partner F
Partner G
Partner H
Network Identity
Hub Provider
External Federated Partner
External Federated Partner
External Federated Partner
External Federated Partner
External Federated Partner
External Federated Partner
External Federated Partner
External Federated Partner
External Federated Partner

“Circle of Trust” Model



Identity Service Provider (s) (IdP)
(e.g. Financial Institution, HR)

- Trusted entity
- Authentication infrastructure
- Maintains Core Identity attributes
- Offers value-added services (optional)

Affiliated Service Providers

- Maintain additional user attributes
- Offers complimentary service
- Don't (necessarily) invest in authentication infrastructure

Common Security Principles in Liberty

- **In general, Liberty enables the usage of existing, analyzed and well-know security mechanisms**
- **Confidentiality**
  - Messages may need to be kept confidential and inhibit unauthorized disclosure, either when transit or when stored persistently
- **Integrity**
  - Messages need to arrive at the intended recipient with data integrity
  - Unauthorized changes shall not be made without detection
- **Authentication**
  - May be required by a receiver to process the message; sender may require the authentication of the response
- **Anti-replay**
  - Message responses must correspond to message request
- **Privacy requirements**
  - Inhibiting the unauthorized disclosure of personally identifiable information

LIBERTY ALLIANCE PROJECT

Liberty’s focus on Privacy

- The Alliance addresses privacy/policy within its specification development process.
- Collaborates with outside policy makers, influencers and within Liberty to ensure specifications and guidelines support privacy laws and fair information practices
- Published Privacy and Security Best Practices to help implementors and deployers develop privacy-sensitive applications on the Liberty framework.

Security & Privacy Guidelines

※ID-WSF Security & Privacy Overview (TEG)

- An overview of the security and privacy issues in ID-WSF technology and briefly explains potential security and privacy ramifications of the technology used in ID-WSF

※Privacy and Security Best Practices (PPEG)

- Highlights certain national privacy laws, fair information practices and implementation guidance for organizations using the Liberty Alliance specifications.

Privacy Features - Summary

- Non technical privacy features:
  - Consumer consent needed for any transaction, specifications and guidelines stress this all over the place
  - Consumer choice of Identity Provider(s)
  - Decentralized or federated storage of Personally Identifiable Information (PII) or any other information related to your identity
- Technical privacy features:
  - Allow consumer remain anonymous or pseudonymous while Service Provider uses NON-PII information to provide personalized services
  - XML Digital Signature, messages designed to allow signing
  - Usage Directives supported in all transactions, allows to use any Privacy Preferences Expression Language (PPEL, see example in the P3P White paper))
  - Consumer Consent header supported in all transactions
  - Interaction Service – allows the holder of consumer information to contact consumer in real time when consent or permission is needed
  - Access control (permissions) easy to “plug-in” (XACML etc..) and be included in the digitally signed message

Non-Technical Privacy features

※ Consumer consent

- All of the relevant specifications include the reference to the need of consumer consent for relevant transactions.

※ Consumer choice of Identity Providers

- Federated architecture allows consumer to choose an Identity Provider independent of the used network or service.
- Selection is only constrained by laws, regulations and business models, not the Liberty specifications

※ Decentralized or federated storage of PII or other information related to your identity

- Federated architecture allows the information related to a specific identity to be stored in relevant locations defined by the consumer, government or business relationship between the consumer and certain Service Provider
- Storage of PII or other identity related information is only constrained by laws, regulations and business models, not the Liberty specifications

Technical Privacy Features – XML Digital Signature

- ※ XML Digital Signature, XMLDsig, specified by W3C, see: ***http://www.w3.org/TR/xmldsig-core***
- ※ Defines how an XML document is Digitally Signed
- ※ All Liberty Architecture Messages have been designed to allow use of XMLDsig
  - – Use of XMLDsig doesn't not make sense in all deployments
- ※ XMLDSig allow a proper verification of the transaction parties, and if messages are signed and stored, allows for later auditing
- ※ All other privacy enabling technical features benefit from use of XMLDsig

Technical Privacy Features – Pseudonymous access

※ Identity Federation in Liberty creates a pseudonym, constructed of a random set of characters and being unique in the context of a specific Identity Provider and Service Provider

※ Pseudonym is linked during the fedederation to the existing user information both at Identity Provider and Service Provider

※ Federation event itself does not create or transfer any new information related to the user in question, i.e. neither the Identity Provider or Service Provider acquire any new information related to the user in question during the federation

※ Liberty specifications provide means for a Service Provider to access Identity Services using the pseudonymous Identity

※ Service Provider gets all the necessary information to invoke Identity Services including Encrypted or one-time identifiers known and usable only by the invoked Identity Service.

Technical Privacy Features – Anonymous access

※ **Liberty specifications provide means for a Service Provider to access Identity Services without a need to know who the consumer they are providing services to really is.**

※ **Service Provider gets all the necessary information to invoke Identity Services including Encrypted or one-time identifiers known and usable only by the invoked Identity Service.**

※ **This anonymity can be used, depending on the business model, for a number of services:**

- Location based service invocation without the Service Provider needing to know consumer phone number
- Access to consumer preferences, such as music, gaming, food etc… without knowing the real identity of the consumer

Technical Privacy Features – Usage Directives

- Allows for indication of associated privacy policy in both information request or reply
- A <UsageDirective> appearing in a request message expresses intended usage.
- A <UsageDirective> appearing in a response expresses how the receiver of the response is to use the response data.
- A <UsageDirective> in a response message containing no response message data, a fault response for example, may be used to express policies acceptable to the responder.
- A message containing Usage Directive can be signed using XMLDsig and thus bind together the released personal information and associated policy

A Usage Directive on a Request for the Address of a Principal

```
<S:Envelope xmlns:S="h ttp://schemas.xmlsoap.org/soa p/envelope/"
                          xml ns:sb="urn:liberty:wsf:soa p-bind:1.0"
                          xml ns:pp="rn:liberty:idpp:1.0 ">
  <S:Header>
     < sb:UsageDirective
                      id="directive1000"
                      ref="#datarequest001"
                      S:mustUnderstand="1">
        <cot :PrivacyPolicyReference
                          xmlns:cot="http: //circle-of-trust.com/isf">
                          http://circle -of-trust.com/policies/eu-compliant
        </cot:PrivacyPolicyReference>
    </ UsageDirective>

</S:Header>
<S:Body>
                          <pp:Query id="datarequest001" xmlns="urn:liberty: pp:1.0">
                          <pp:Re source>data:d8ddw6dd7m28v628< /pp:Resource>
                          <pp :QueryItem>
                          < pp:Select>/pp:IDPP/pp:IDPPA ddressCard</pp:Select>
                          </pp:QueryItem>
                          </pp:Query>
</S:Body>
</S:Envelope>
```

XMLDsig binds
all this together

Technical Privacy Features – Consumer Consent header

※ This header block is used to explicitly claim that the Principal consented to the present interaction

※ Liberty defines one well-known URI Liberty implementers and deployers MAY use to indicate positive Principal consent was obtained with respect to whatever interaction is underway or being initiated.

※ This URI is known as the "Principal Consent Obtained" URI (PCO). The value of this URI is: urn:liberty:consent:obtained

※ This URI does not correspond to any particular Consent Agreement Statement. Rather, it simply states that consent was obtained. The full meaning and implication of this will need to be derived from the execution context.

Request for the Address of a Principal – Consent header

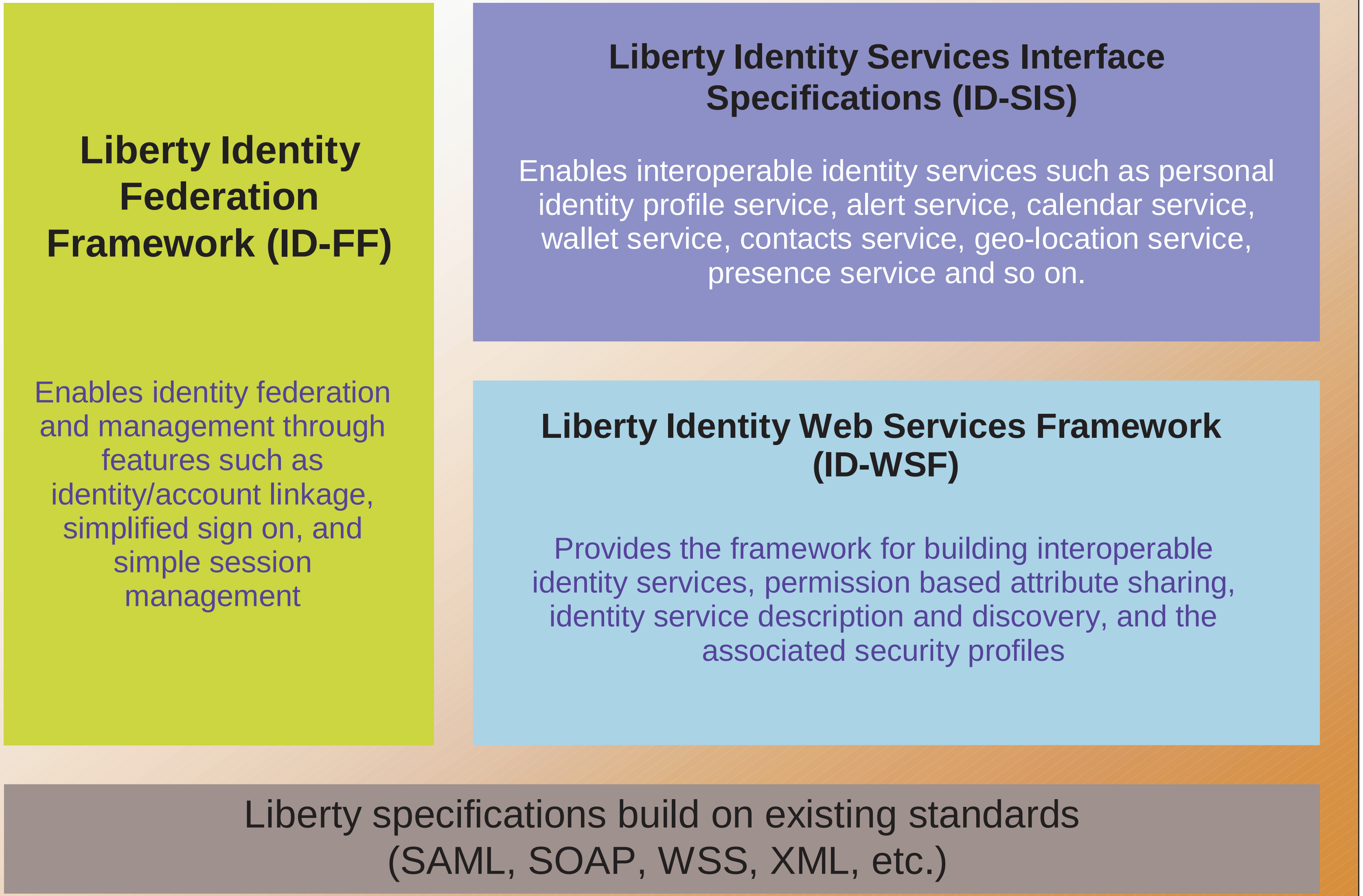
```
<S:Envelope xmlns:S="h ttp://schemas.xmlsoap.org/soa p/envelope/"
             xml ns:sb="urn:liberty:wsf:soa p-bind:1.0"
             xml ns:pp="rn:liberty:idpp:1.0 ">
 <S:Header>
  < sb:UsageDirective
              id="directive1000"
              ref="#datarequest001"
              S:mustUnderstand="1">
    <cot :PrivacyPolicyReference
                xmlns:cot="http: //circle-of-trust.com/isf">
                http://circle -of-trust.com/policies/eu-compliant
    </cot:PrivacyPolicyReference>
  </ UsageDirective>
  <sb:Consent id="A1243957324 95743"
    uri="urn:liberty:consent:obtained"
    timestamp="2112-03-15T11: 12:10Z"/>
</S:Header>
<S:Body>
             <pp:Query id="datare quest001" xmlns="urn:liberty: pp:1.0">
             <pp:Re source>data:d8ddw6dd7m28v628< /pp:Resource>
             <pp :QueryItem>
             < pp:Select>/pp:IDPP/pp:IDPPA ddressCard</pp:Select>
             </pp:QueryItem>
             </pp:Query>
</S:Body>
</S:Envelope>
```

XMLDsig binds all this together

Technical Privacy Features – Interaction Service

- It may sometimes be necessary for an identity service to interact with the owner of the information that it is exposing, to collect attribute values, or to obtain permission to share the data with Service Provider
- The Interaction Service specification defines schemas and profiles that enable an Identity Service to interact with the owner of the information that is exposed by that Identity Service
- Typical situation are :
  - Collect consent for a service provider to access your personal information
  - Collect consent for a service provider to access an Identity Service such as Wallet, Calendar Personal Profile etc…
  - Collect missing information to allow the transaction to complete
- Remove need for “blanket” approval for information or Identity Service usage, consent can be applied very specifically

The Complete Liberty Architecture



Liberty Identity Federation Framework (ID-FF)

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

Liberty Identity Services Interface Specifications (ID-SIS)

Enables interoperable identity services such as personal identity profile service, alert service, calendar service, wallet service, contacts service, geo-location service, presence service and so on.

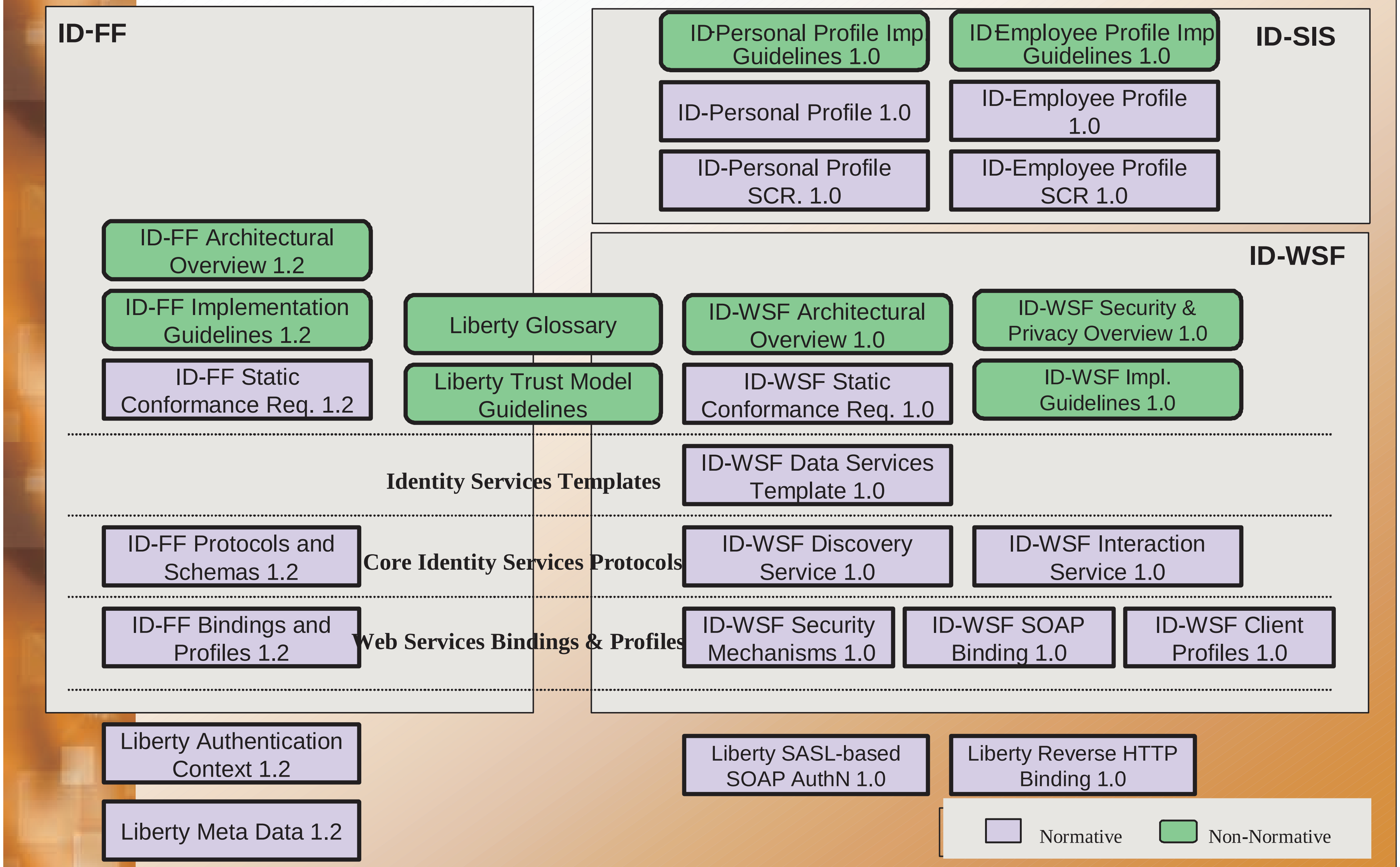
Liberty Identity Web Services Framework (ID-WSF)

Provides the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles

Liberty specifications build on existing standards (SAML, SOAP, WSS, XML, etc.)

LIBERTY ALLIANCE PROJECT

Liberty Specification Map



ID-FF

ID-FF Architectural Overview 1.2

ID-FF Implementation Guidelines 1.2

ID-FF Static Conformance Req. 1.2

Liberty Glossary

Liberty Trust Model Guidelines

ID-SIS

ID-Personal Profile Imp Guidelines 1.0

ID-Employee Profile Imp Guidelines 1.0

ID-Personal Profile 1.0

ID-Employee Profile 1.0

ID-Personal Profile SCR. 1.0

ID-Employee Profile SCR 1.0

ID-WSF

ID-WSF Architectural Overview 1.0

ID-WSF Security & Privacy Overview 1.0

ID-WSF Static Conformance Req. 1.0

ID-WSF Impl. Guidelines 1.0

Identity Services Templates

ID-WSF Data Services Template 1.0

Core Identity Services Protocols

ID-FF Protocols and Schemas 1.2

ID-WSF Discovery Service 1.0

ID-WSF Interaction Service 1.0

Web Services Bindings & Profiles

ID-FF Bindings and Profiles 1.2

ID-WSF Security Mechanisms 1.0

ID-WSF SOAP Binding 1.0

ID-WSF Client Profiles 1.0

Liberty Authentication Context 1.2

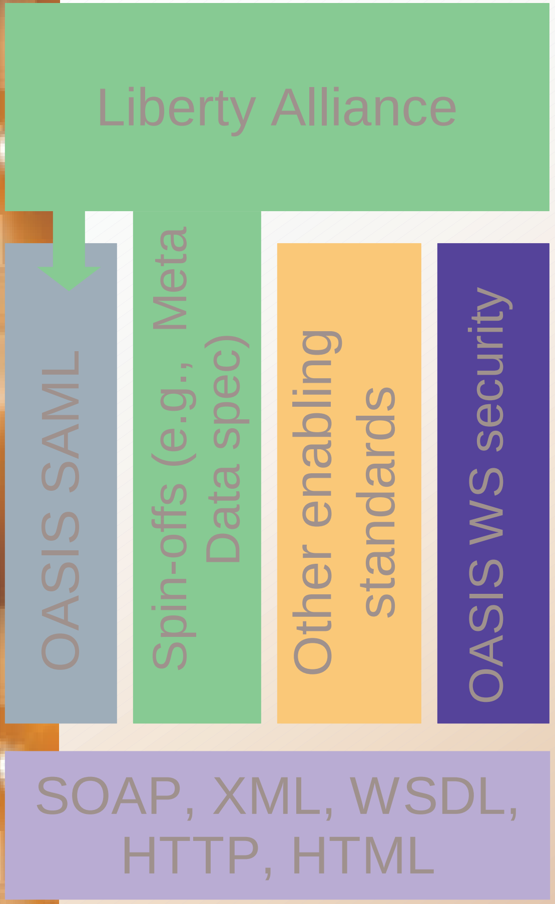
Liberty Meta Data 1.2

Liberty SASL-based SOAP AuthN 1.0

Liberty Reverse HTTP Binding 1.0

□ Normative 🟩 Non-Normative

Where does Liberty Fit?



Liberty Alliance:

a diverse industry consortium that is developing specifications for federated network identity, simplified sign-on, and authorization among diverse network and applications domains

Other enabling standards:

- SPML (Service Provisioning Markup Language)
- XML Access Control Markup Language (XACML)
- XML Key Management Specification (XKMS)
- XML Digital Signature

WS-security:

mechanisms implemented in SOAP headers designed to enhance SOAP messaging providing a quality of protection through message integrity, message confidentiality, and single message authentication

SAML 1.1 (Security Assertion MarkUp Language):

a set of XML and SOAP-based services, protocols, and formats for exchanging authentication and authorization information

*** See archived Liberty Webinar for more SAML information*

Additional Information

Learn more about the technical aspects of Liberty Alliance

Free webinar from HP

“Federated Identity”

www.presentationselect.com/hpinvent/archives.asp

See the specifications and white papers at

http://www.projectliberty.org

Thank You

Questions ?