The Identity Web
An Overview of XNS and the OASIS XRI TC

XML WG

December 17, 2002

Marc LeMaitre
VP Technology Strategy
OneName Corporation

Goals of this presentation

- Introduce the idea of the Identity Web
- Provide you with it's motivating forces
- Compare and contrast it to the WWW
- Introduce you to eXtensible Name Service (XNS)
- Give you an update on XNS in standards

1992: What if…

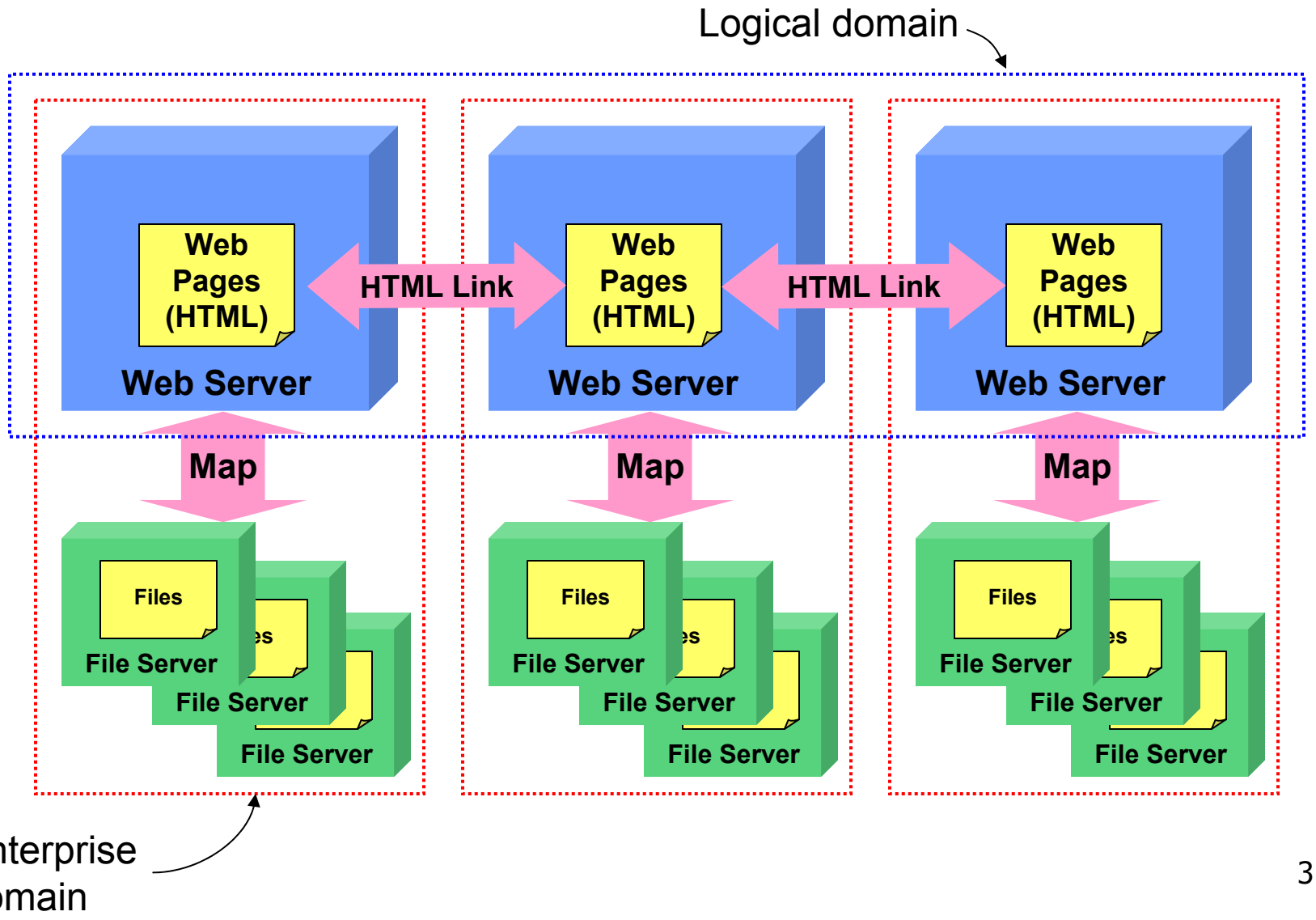
…every digital document on the Internet could be:

- Rendered in a common format
- Exchanged using a common protocol
- Addressed and linked using a common syntax

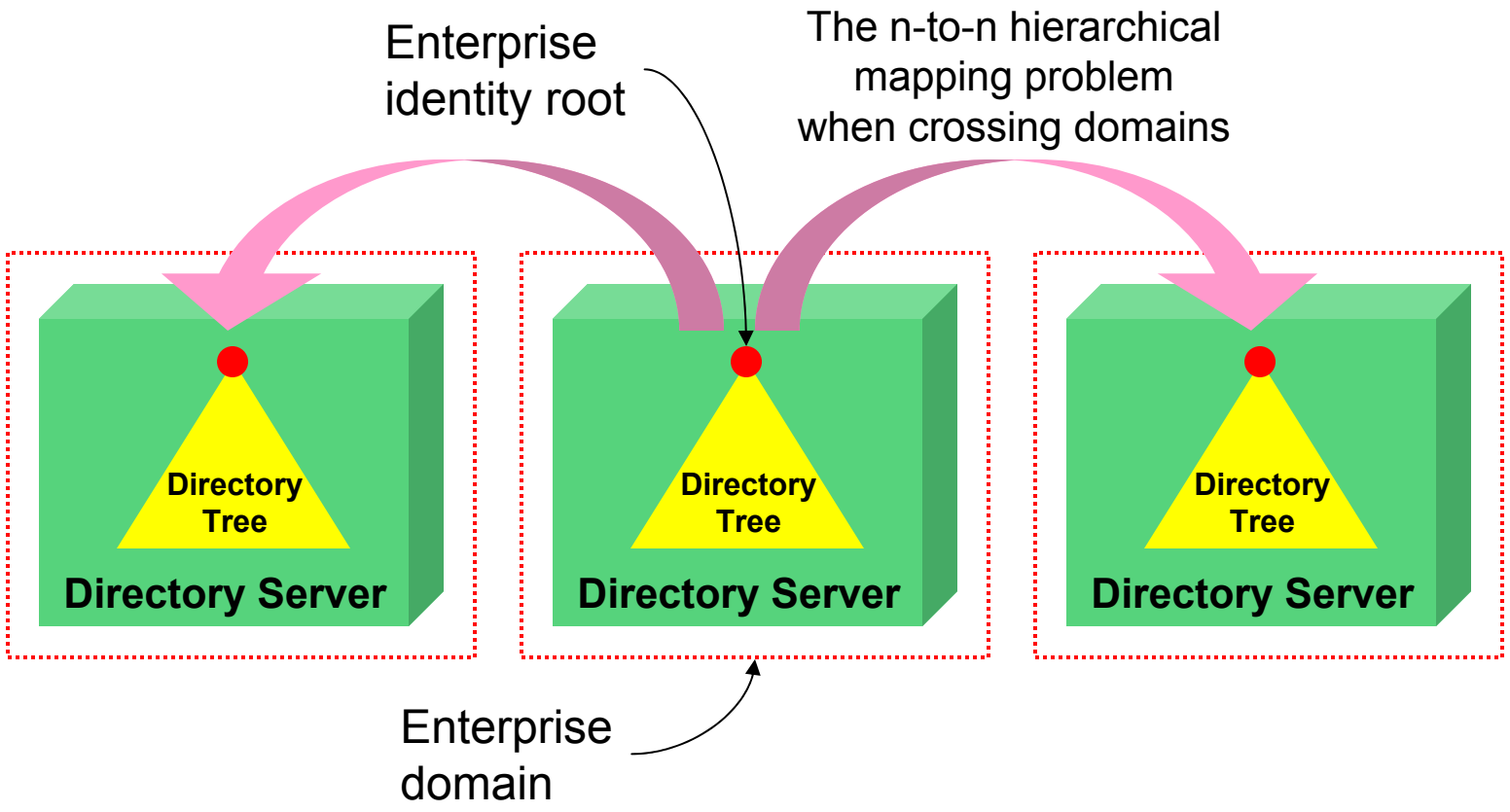
The result would be…

…the World Wide Web

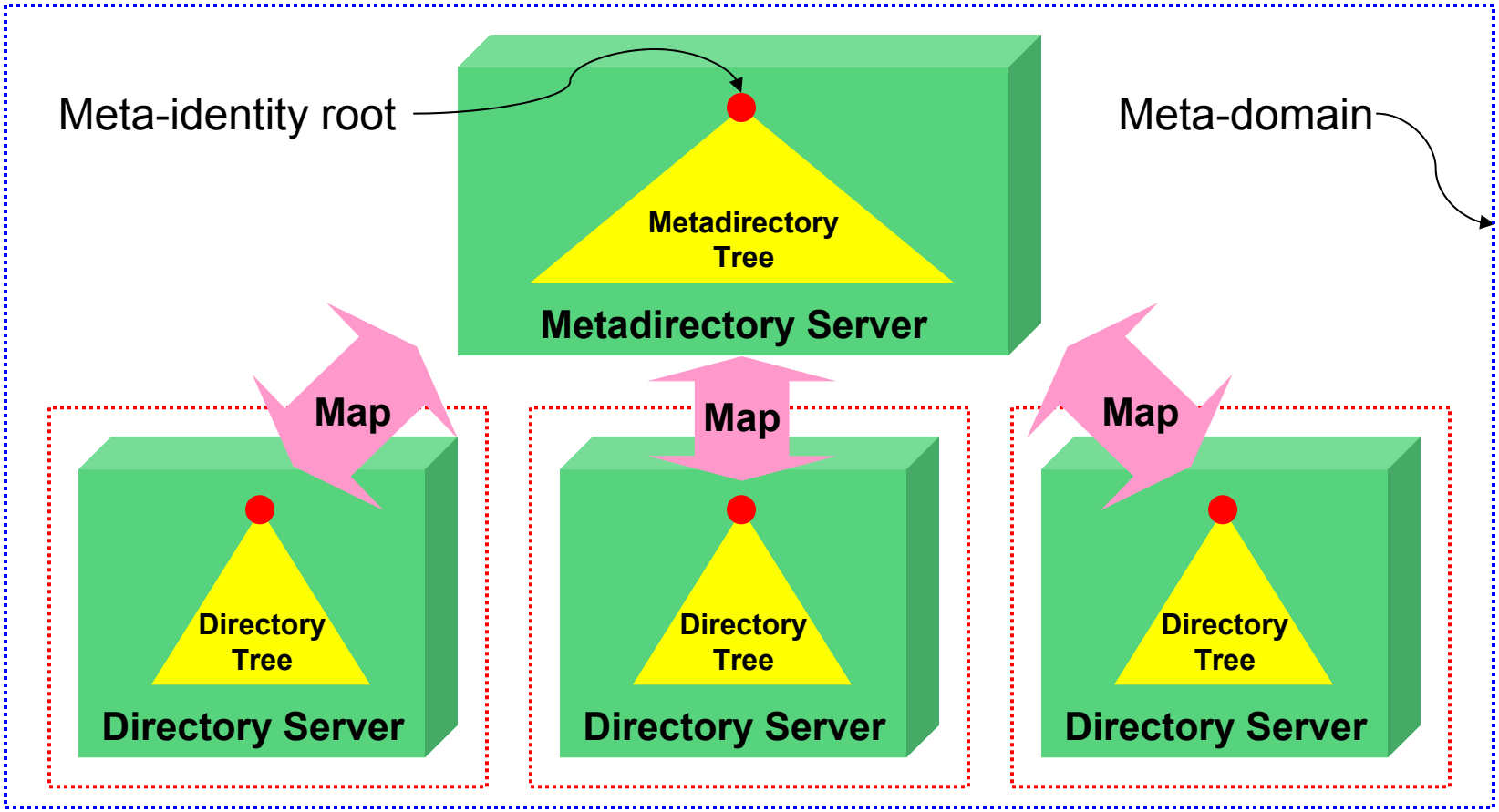
Evolution of content on the WWW



Enterprise directory services issues



Meta-directory service issues



2002: What if…

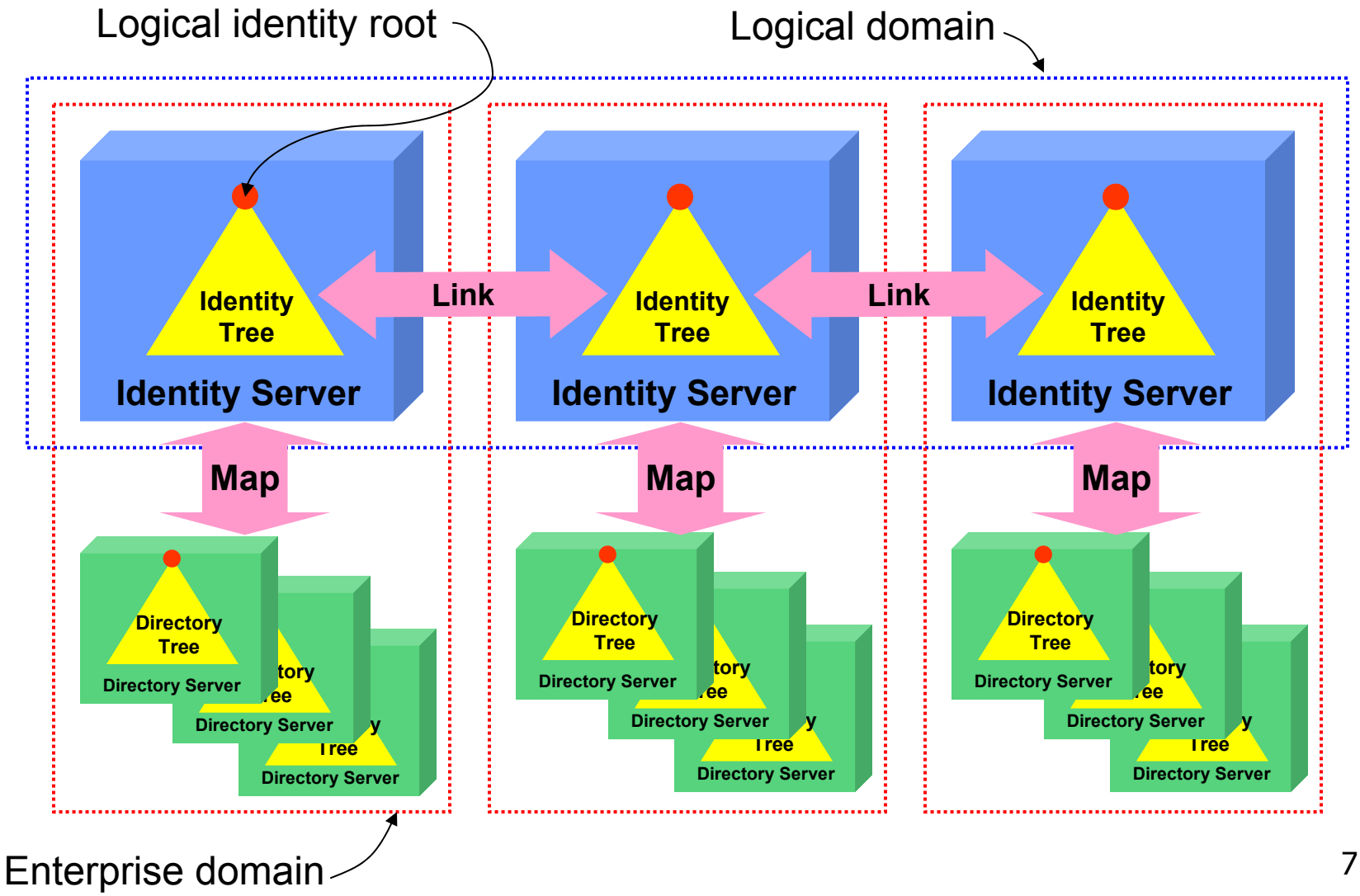
…every digital identity on the Internet could be:

- Rendered in a common format
- Exchanged using a common protocol
- Addressed and linked using a common syntax

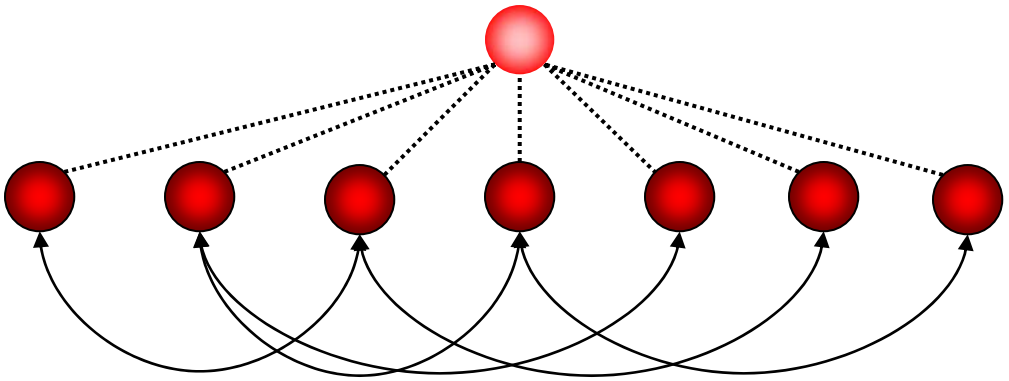
The result would be…

…an Identity Web

The leap to a Web architecture for Identity



The Web Identity Tree



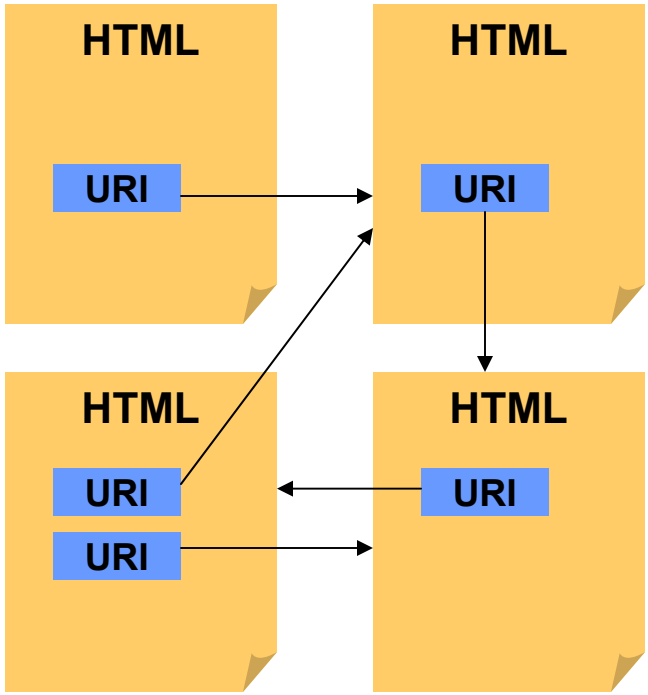
Abstract Root
(XML Schema)

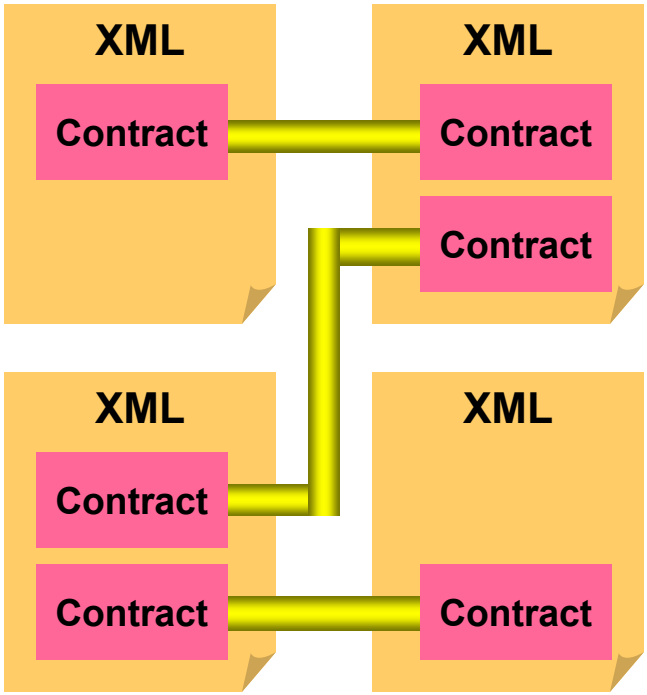
Identity Roots
(XML Identity Documents)

Links

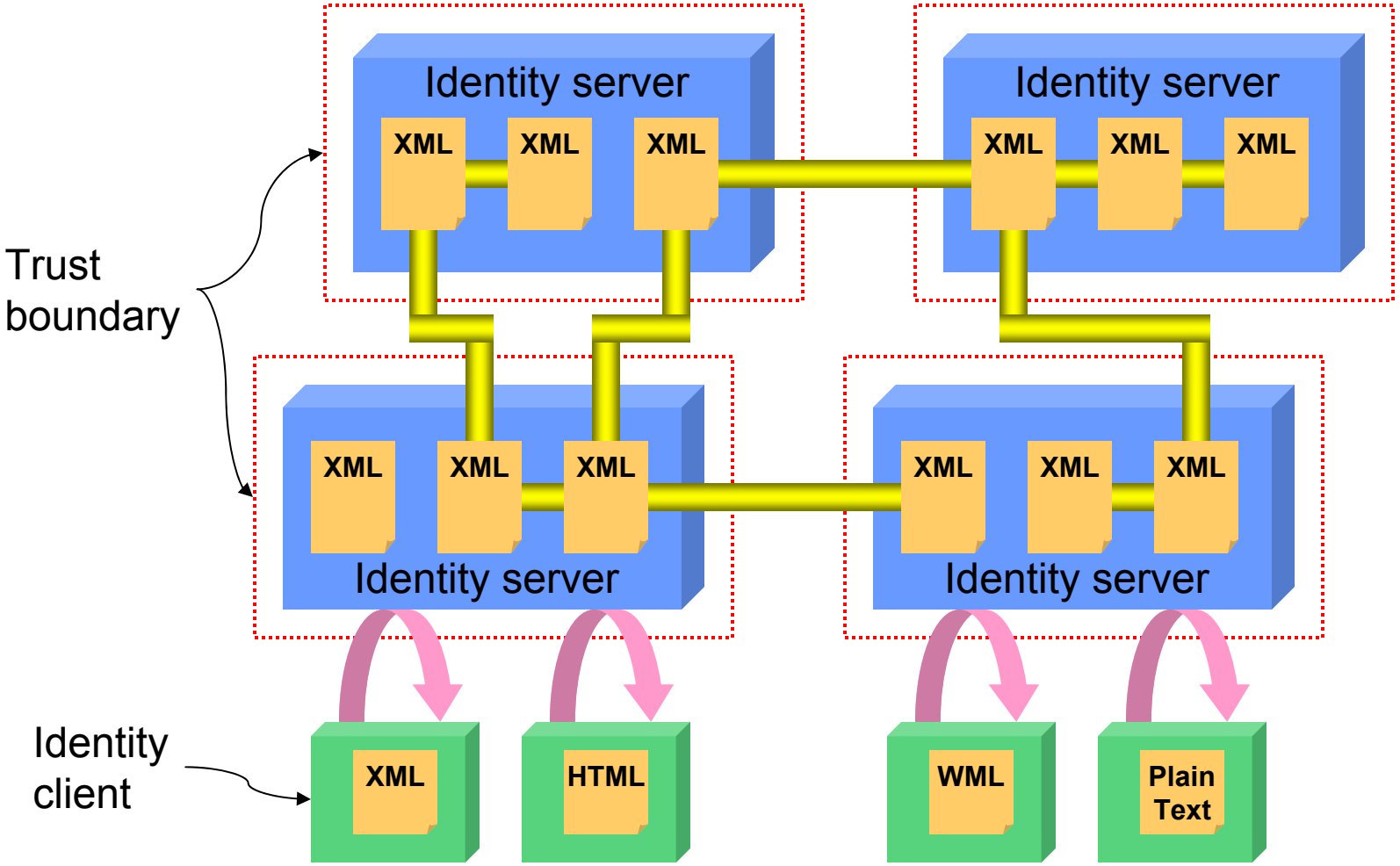
- Flat – like the Web
- All relationships are created by linking – like the Web
- Distributed control and management – like the Web

Document linking vs. identity linking

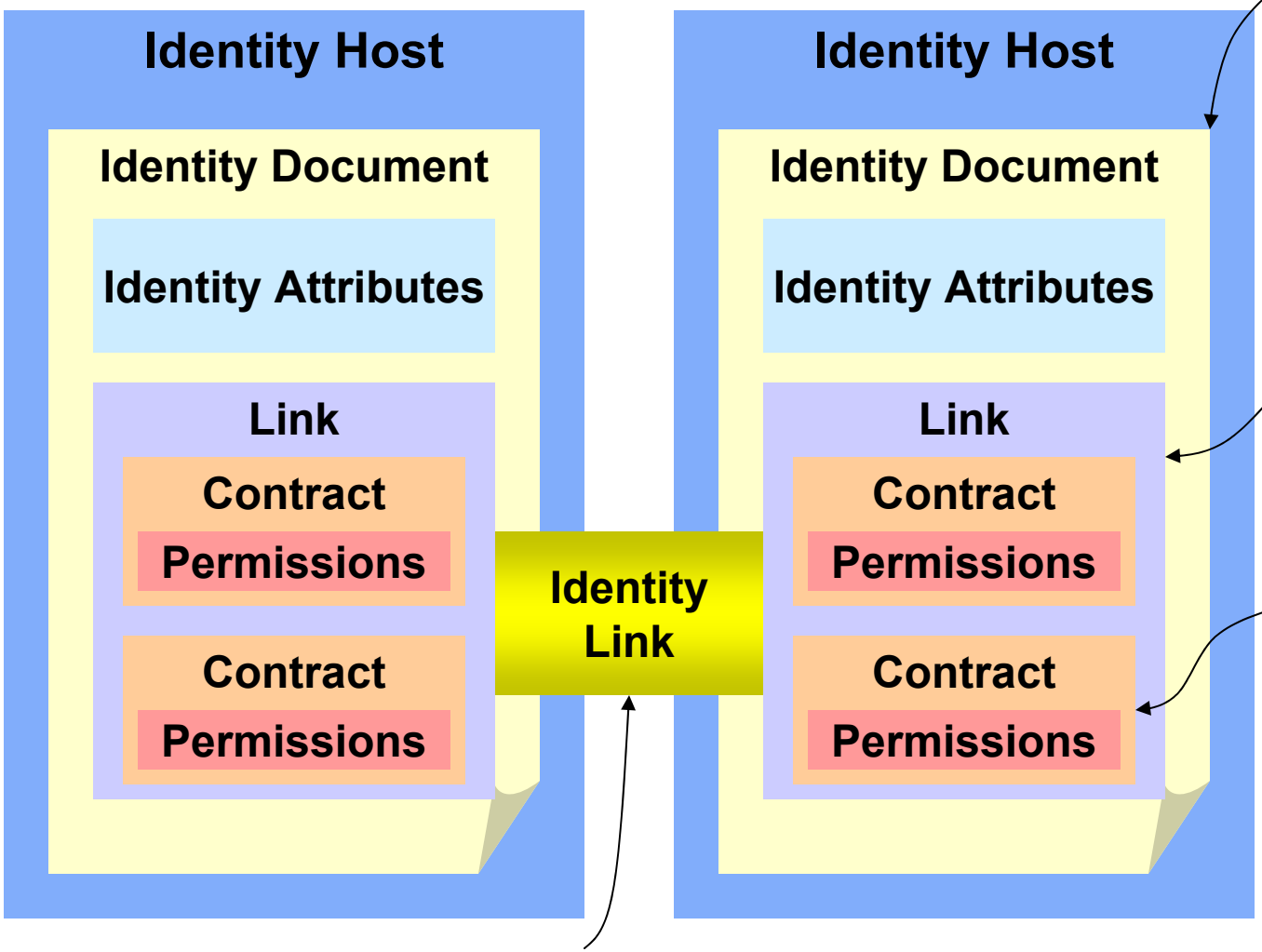




Federating identity servers



Identity linking close up



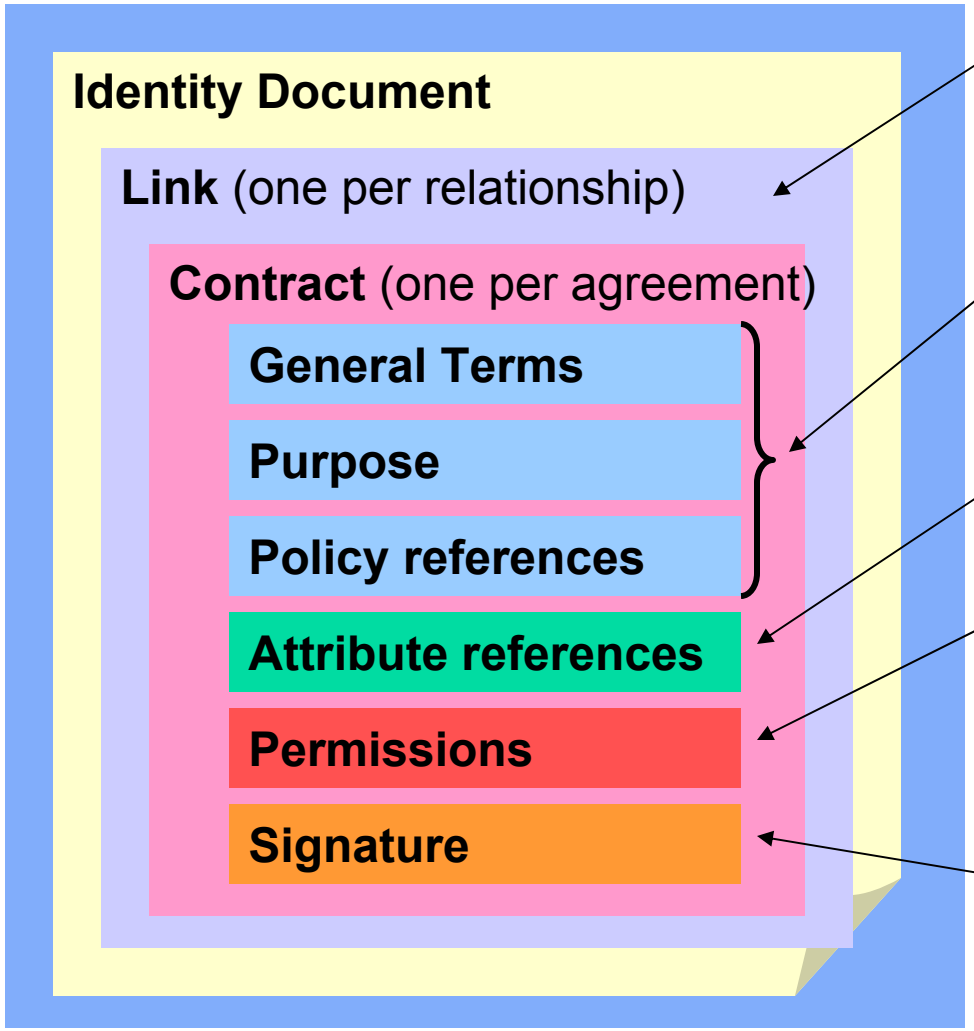
Identity hosts manage XML documents representing attributes associated with an identity. These identity documents can be "virtual", i.e., the physical data can be stored in lower-layer systems.

Each link with another identity is defined by a subdocument inside the identity document.

A link can contain any number of contracts, each defining a set of data shared with the other identity and the applicable security, privacy, and synchronization permissions.

Links create trusted, bidirectional data "pipes" between any two XNS identities anywhere.

Contract structure



A link object can contain any number of contract objects covering different data & purposes.

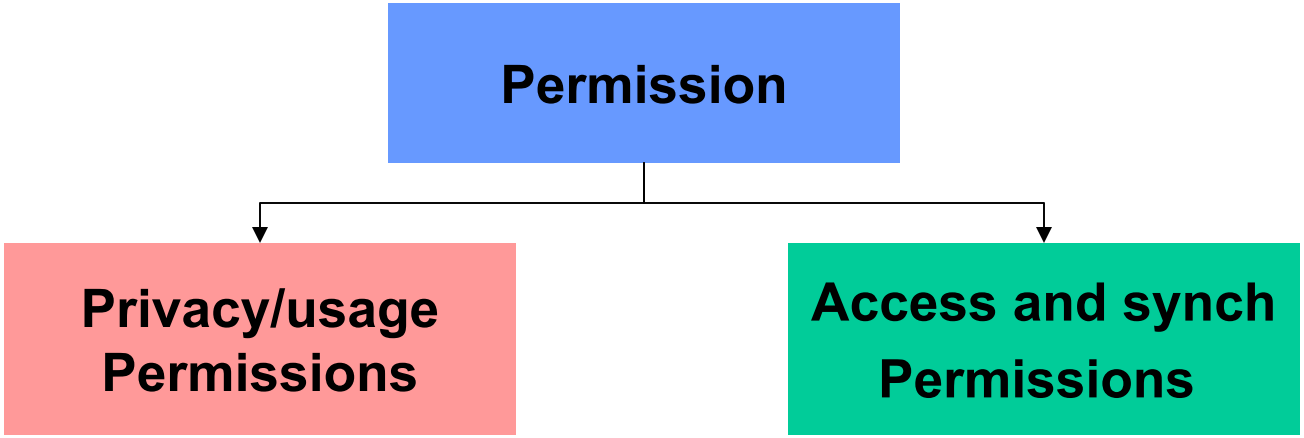
Each contract states the terms, purpose, and applicable policies (policy references use URNs).

Contracts reference the attributes they cover using URNs.

Permission objects are extensible to model any type of privacy policy (opt-out, opt-in, opt-over using any type of Rights Markup Language – (RML)) in any legal jurisdiction. They also cover access control and synchronization.

Contracts are signed and stored by both parties for auditing and non-repudiation.

Permission objects



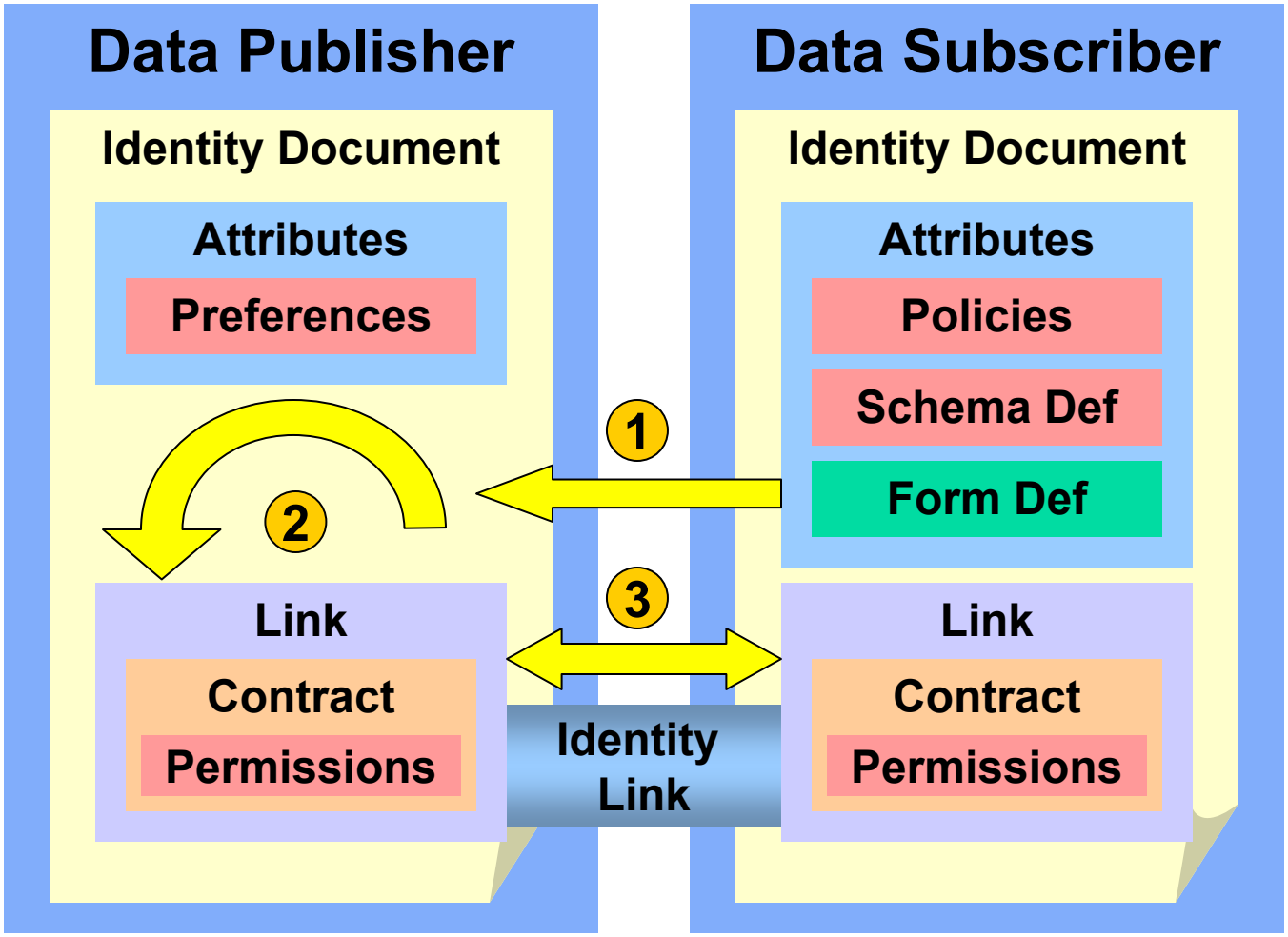
Controls:

- Permission type (disclosure, contact, retention)
- Purpose (human-readable)
- Parties (for disclosure)

Controls:

- Access to data
- Persistent Get and Set permissions for data

The negotiation process

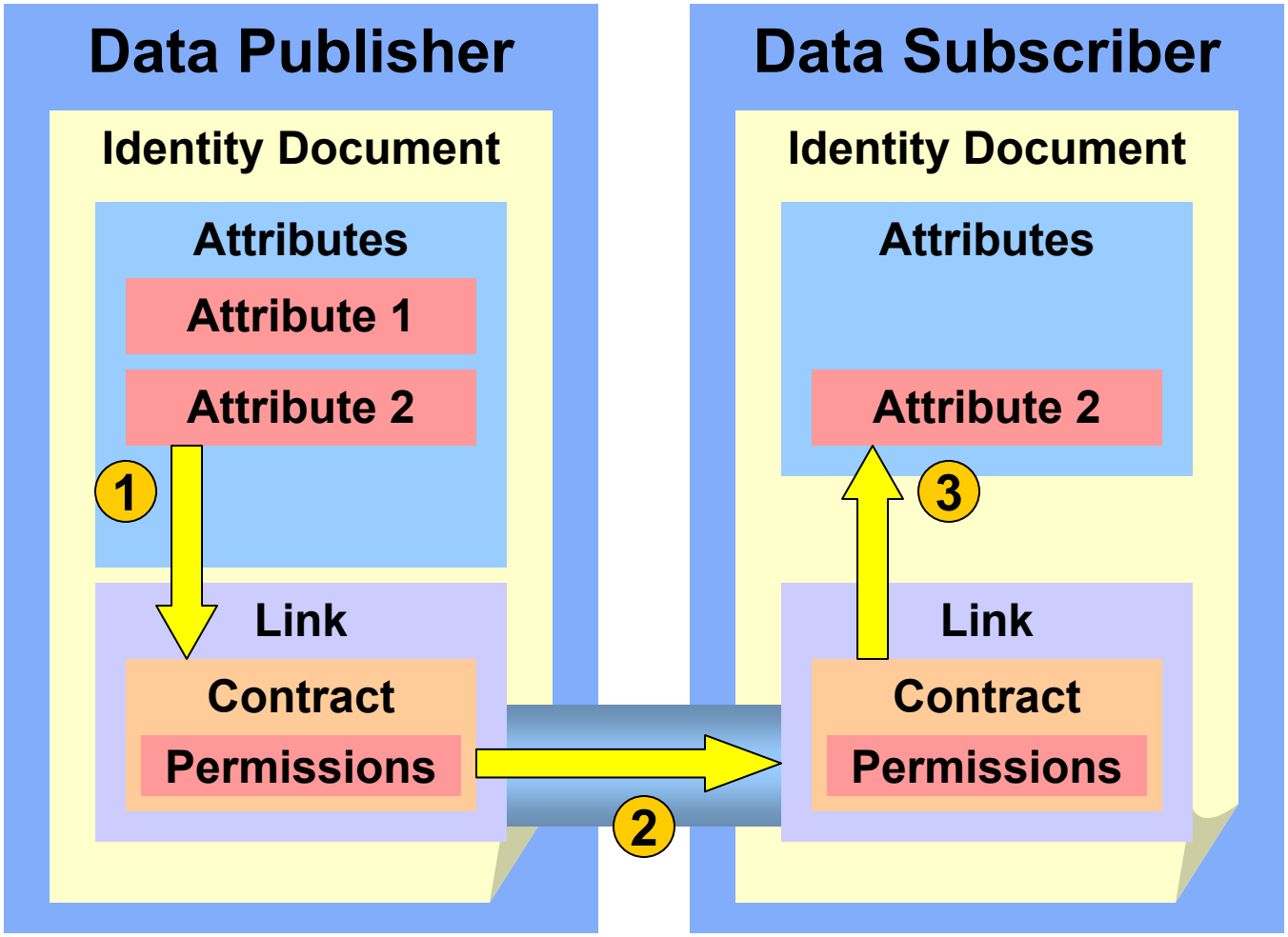


1) The data subscriber sends an XML form definition (essentially a template contact) to the data publisher.

2) The data publisher processes the form based on the publisher's attributes and preferences and negotiates the contract.

3) Both parties "sign" the contract and store a copy in their link.

The synchronization process



1) When the publisher updates an attribute, they check to see which contracts reference that attribute.

2) If the contract specifies a push, the publishing identity composes a Set message and attaches an assertion.

3) The data subscriber authenticates the message and triggers processing of the updated attribute.

Recap……..

- The Identity Web is a new abstraction layer for cross-domain data sharing using a Web architecture of linked XML documents
- Linked documents contain contracts controlling the flow and usage of data negotiated by the controlling identities
- It is deployed through a federated network of identity servers

Introduction to eXtensible Name Service

How to build an Identity Web

XNS design requirements

- Logical persistent addressing
  - Enable application- and domain-independent mapping of resource identities and their associated data
    - A resource is anything that can be represented on a network – person, organization, machine, application etc)
- Logical schema sharing and versioning
  - Dictionaries of shareable, reusable data definitions
- Logical security and privacy controls
  - Enables federation and delegation across domains
- Logical exchange, linking, and synchronization
  - Scalable, extensible peer-to-peer data sharing

- XNS consists of:
  - A syntax for addressing XML identity docs using eXtensible Resource Identifiers (XRIs)
  - 14 WSDL service modules for federated naming and directory services using XRIs & XML identity docs
  - A considerable amount of thinking about how to support a REST architecture like the Web

XNS Public Trust Organization (XNSORG)

- Founded in 2000
- Licensed the rights to XNS from OneName
- Published XNS 1.0 specs on July 10, 2002
- Responsible for community governance of XNS and delegation of specifications to other standards organizations
- Sponsors include:

GEMPLUS beyond smart NRI OneName VISA wave

The XNS 1.0 Specifications

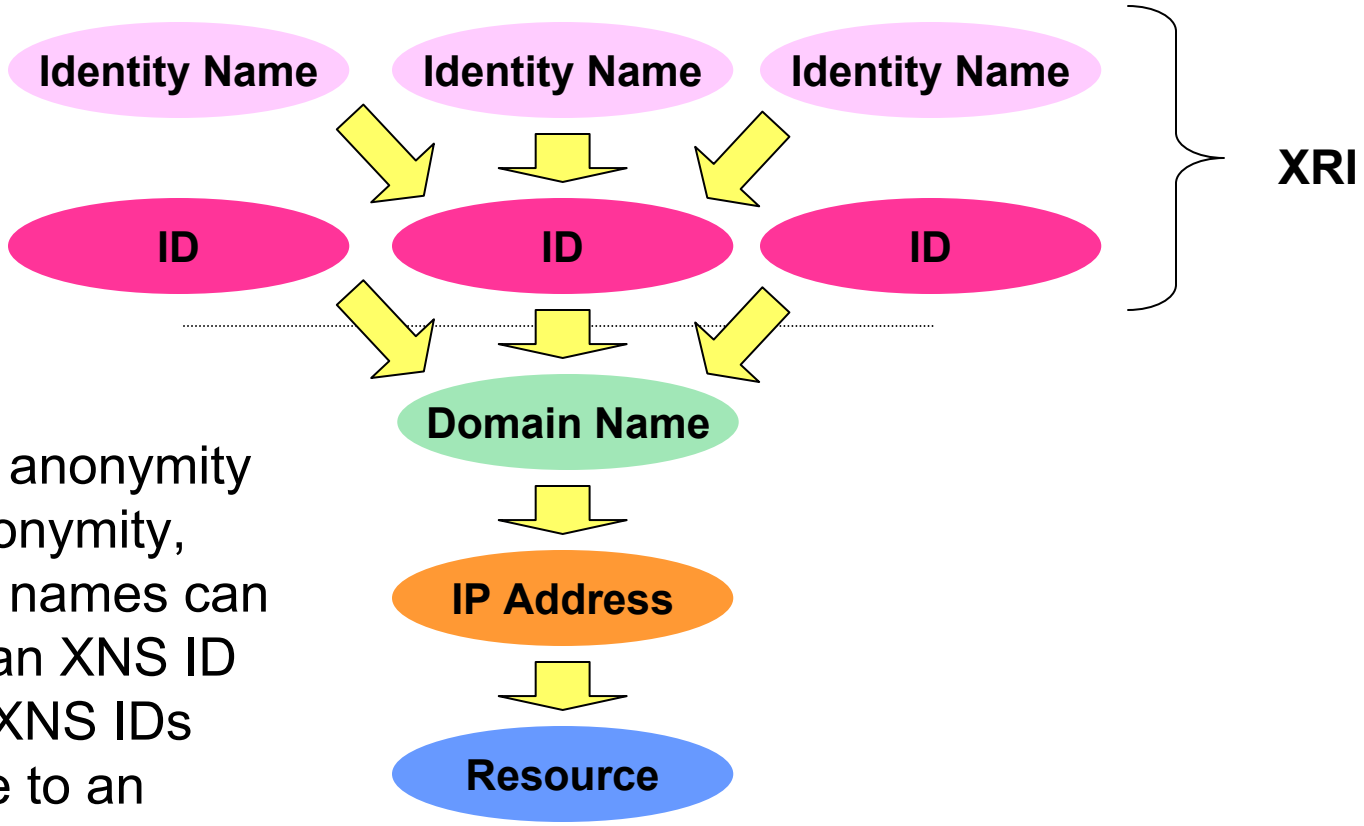
XNS 1.0: a two-part specification
Part 1 – Identity addressing

- An XML-based URI and URN syntax for addressing identity documents called eXtensible Resource Identifiers – XRIs
- Embrace the benefits of URNs
  - Independent of application
  - Independence of transport type
  - Independence of resource type
- Extend the benefits of combined URIs and URNs

XRIs extend the benefits of URIs and URNs

- Human readable and memorable identifiers
  - Some subset should be human friendly
- Permanent identifiers
  - Persist beyond the life of a particular network representation
- Privacy-protected identifiers
  - For people and their PII (blinding/obfuscation/non triangulation)
- Cross-referenceable identifiers
  - Representing the same logical, well-known resource across physical domains or locations
- Versionable identifiers
  - Managing state across multiple instances of a resource at different network locations
- Federated identifiers
  - Manage identifiers that are delegated between authorities
- Linked data
  - Link physically-disparate data of an identified resource into logical data objects

XRIs support many-to-one relationships



To support anonymity and pseudonymity, many XNS names can resolve to an XNS ID and many XNS IDs can resolve to an identity.

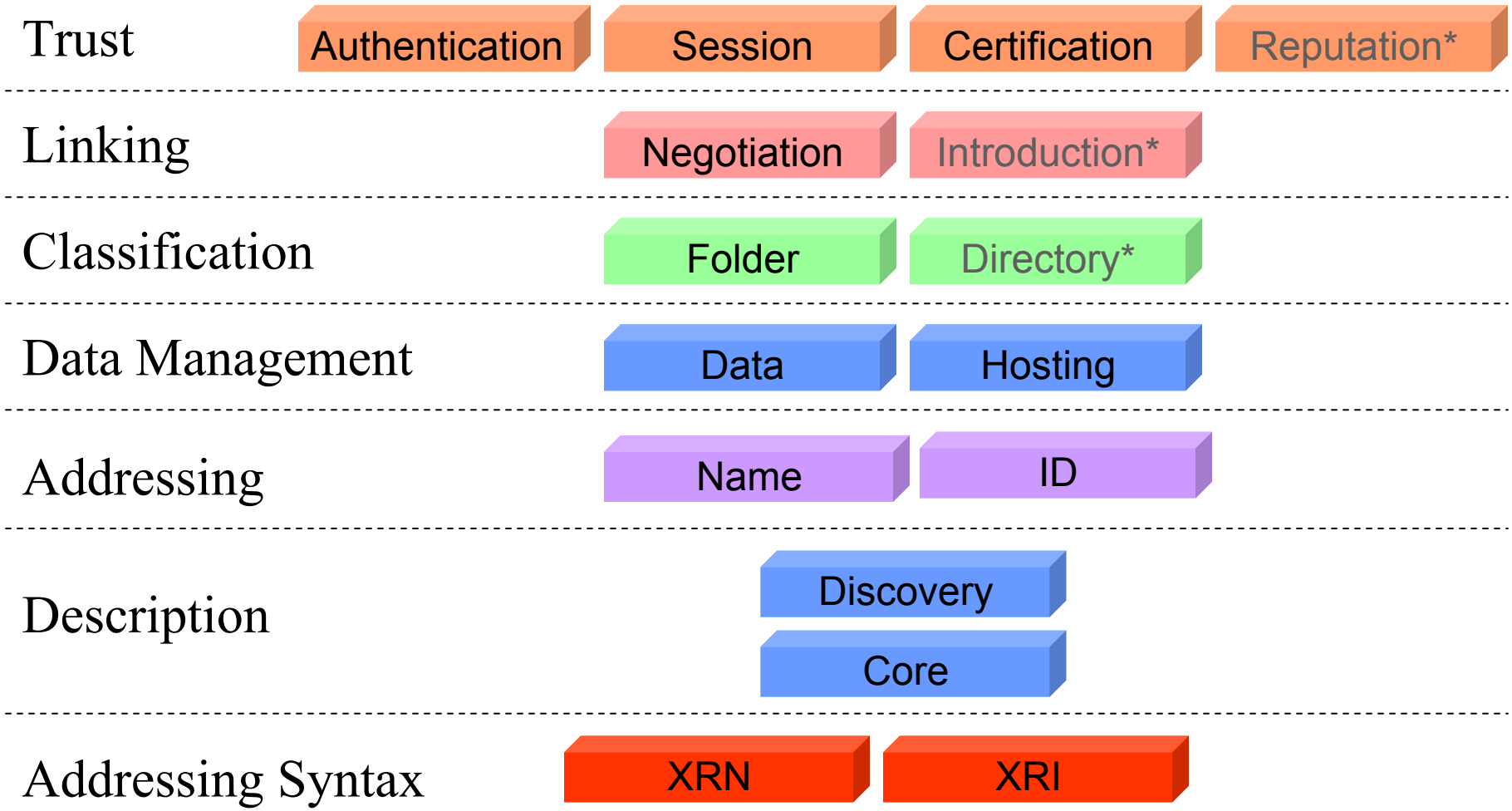
The OASIS XRI TC

- First step in XNS standardization process
- OASIS Call for Participation issued Dec. 6
- First meeting January 9, 2003
- Will focus on specifications for the URI and URN format of an XNS address (called an XRI – Extensible Resource Identifier)
- Charter participants include AMD, Cisco, Novell, Visa International, EDS, Gemplus, Nomura Research, Wave Systems, OneName, XNSORG

XNS 1.0: a two-part specification
Part 2 – Identity Services

- A suite of WSDL services for:
  - Registering/resolving identity document addresses
  - Reading and writing attributes from identity documents
  - Obtaining and asserting identity credentials (a special form of attribute)
  - Forming contracts between identity documents
- Ongoing work to simplify these services to fit into a REST architecture

The XNS WSDL services suite



* Not defined in XNS 1.0 specifications

Treating identities as XML documents

- Core defines the XNS abstract schemas
- Discovery defines the XNS metaschema vocabulary and enables location of schema instances
- Hosting adds/deletes/moves identity documents at a host identity (network endpoint)
- Data gets/sets identity data (attributes) within an identity document
  - XRI addressing enables efficient global resolution of every attribute and attribute version

Directory services at the identity layer

- Folder provides directory services internal to an identity document
  - Similar to the folder function of file systems
- Directory (coming in 2003) will provide directory services across a community of identity documents
  - Will enhance LDAP/DSML functions with XNS addressing, messaging, assertion, and linking
  - Will integrate XQL and XPath-based queries

XNS, SAML, and PKI

- In XNS, credentials are identity attributes
- XNS Trust Management services standardize methods for obtaining and asserting these attributes
- The payload of these messages are SAML assertions
- Certification service is a solution to distributed key management
- Reputation service can supplement trust decisions with community feedback

Conclusion

- XNS services and XRI addressing can provide the digital identity infrastructure necessary for Web services
- The same set of services can be tailored to serve in a REST-based architecture
- XNS helps solve a wide variety of enterprise and Internet data sharing problems
- The OASIS XRI TC begins its work on January 9, 2003
- We would like to extend an invitation to all OASIS members to participate