The Identity Web:
Key Concepts of XNS Architecture

The XNS Public Trust Organization
(XNSORG)

July 9, 2002

Overview

- This presentation provides a brief overview of the key concepts of XNS architecture
- It is designed for architects, developers, and system administrators who want to quickly understand how XNS works
- It accompanies the first release of the XNS Technical Specifications by XNSORG

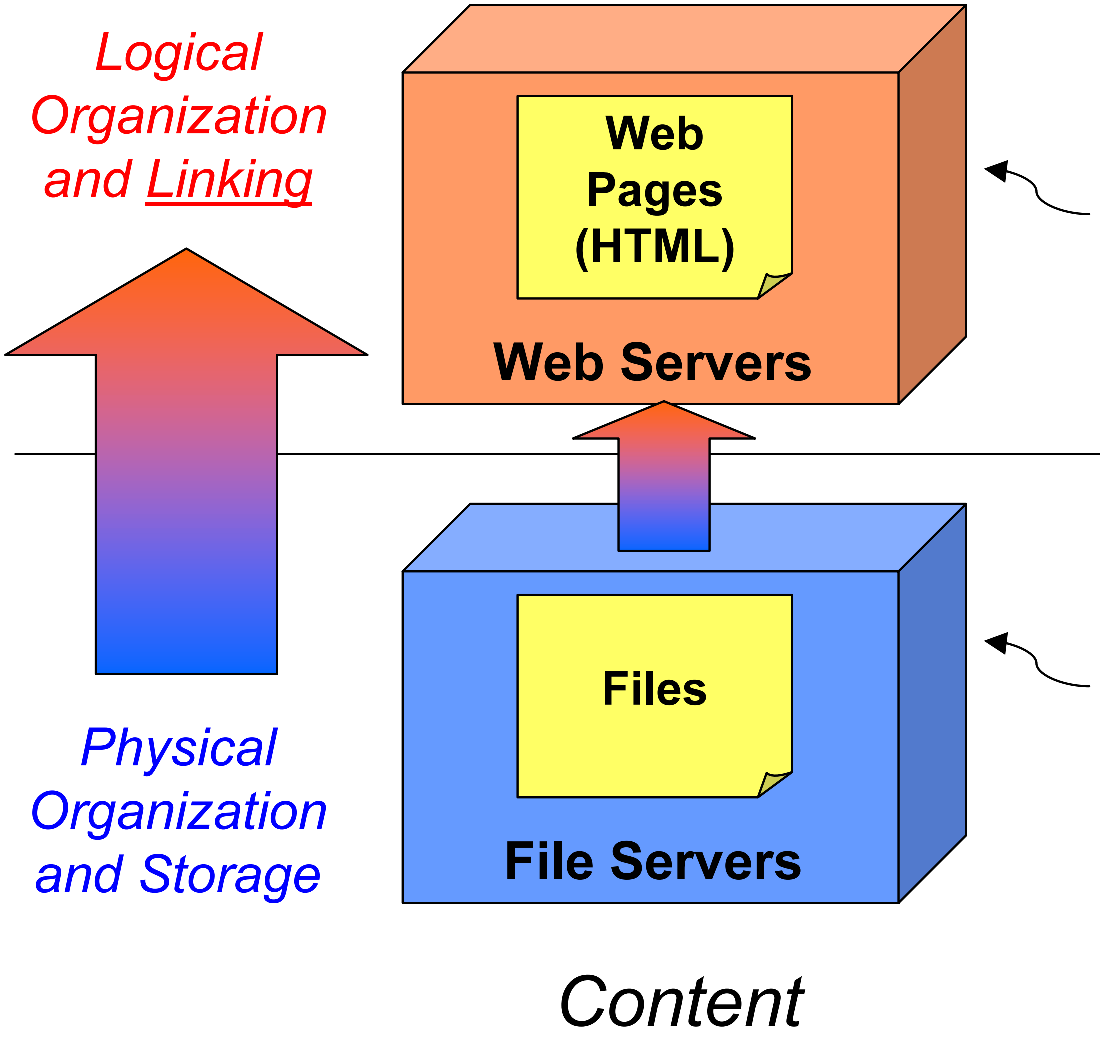
Key concepts of XNS architecture

- The Identity Web
- Identity documents
- Identity addresses
- Identity links
- Identity transactions
- Identity credentials
- Identity services

The Identity Web

- The XNS digital identity protocol allows digital identities to form links the same way Web pages are linked
- The key difference is that *identity linking* can be used to:
    - Exchange private, protected data
    - Govern the data protection applied to that data
    - Maintain persistent relationships
    - Keep the data synchronized

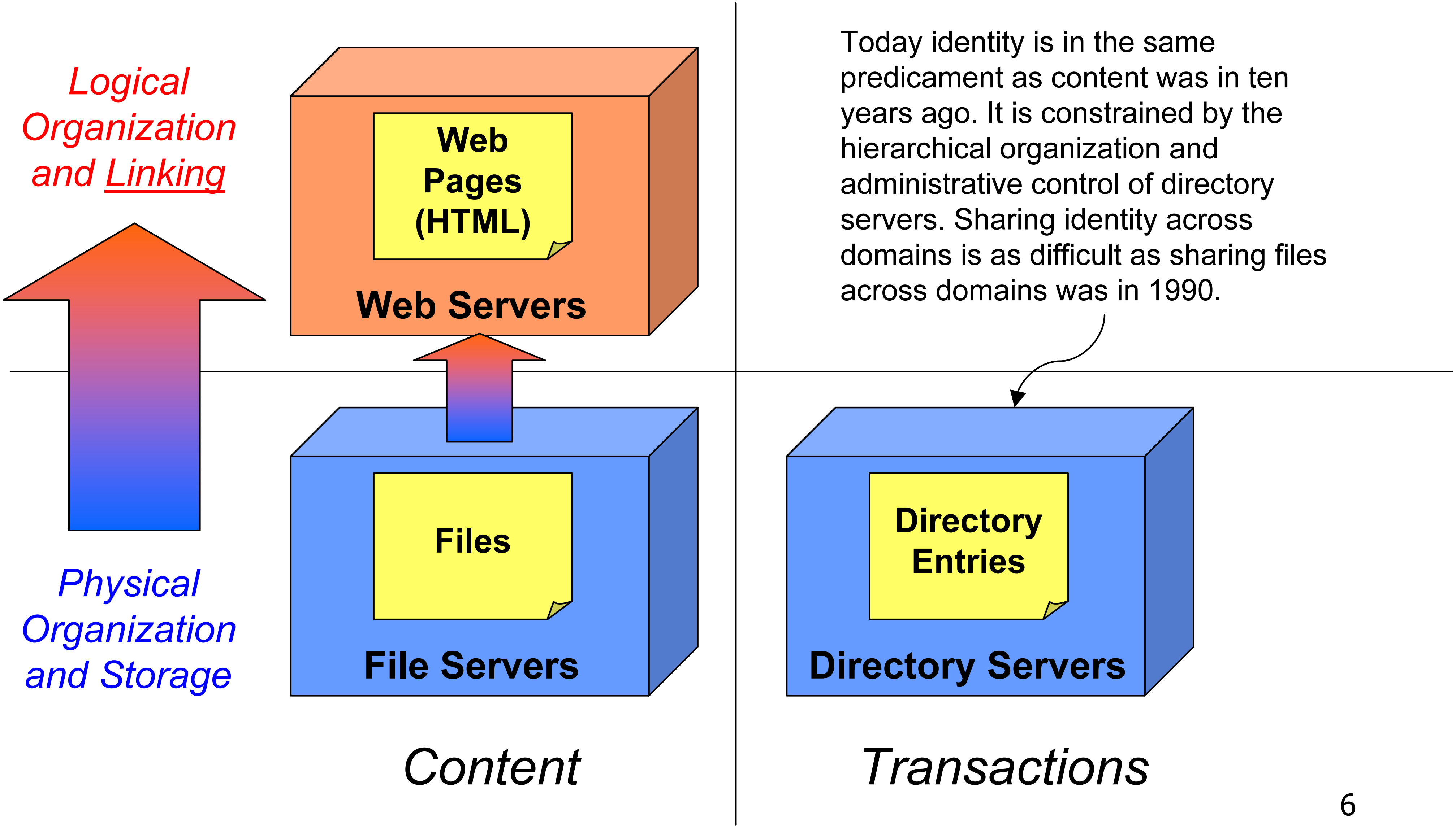
Evolution of the Identity Web (step 1)


Logical Organization and Linking
Web Pages (HTML)
Web Servers
Files
File Servers
Physical Organization and Storage
Content

The force that drove the Web was the elevation of content to a logical level of representation (HTML) and access (HTTP). Now it could be linked (using URLs) across Web servers regardless of the physical system on which it was stored. The rest is history.

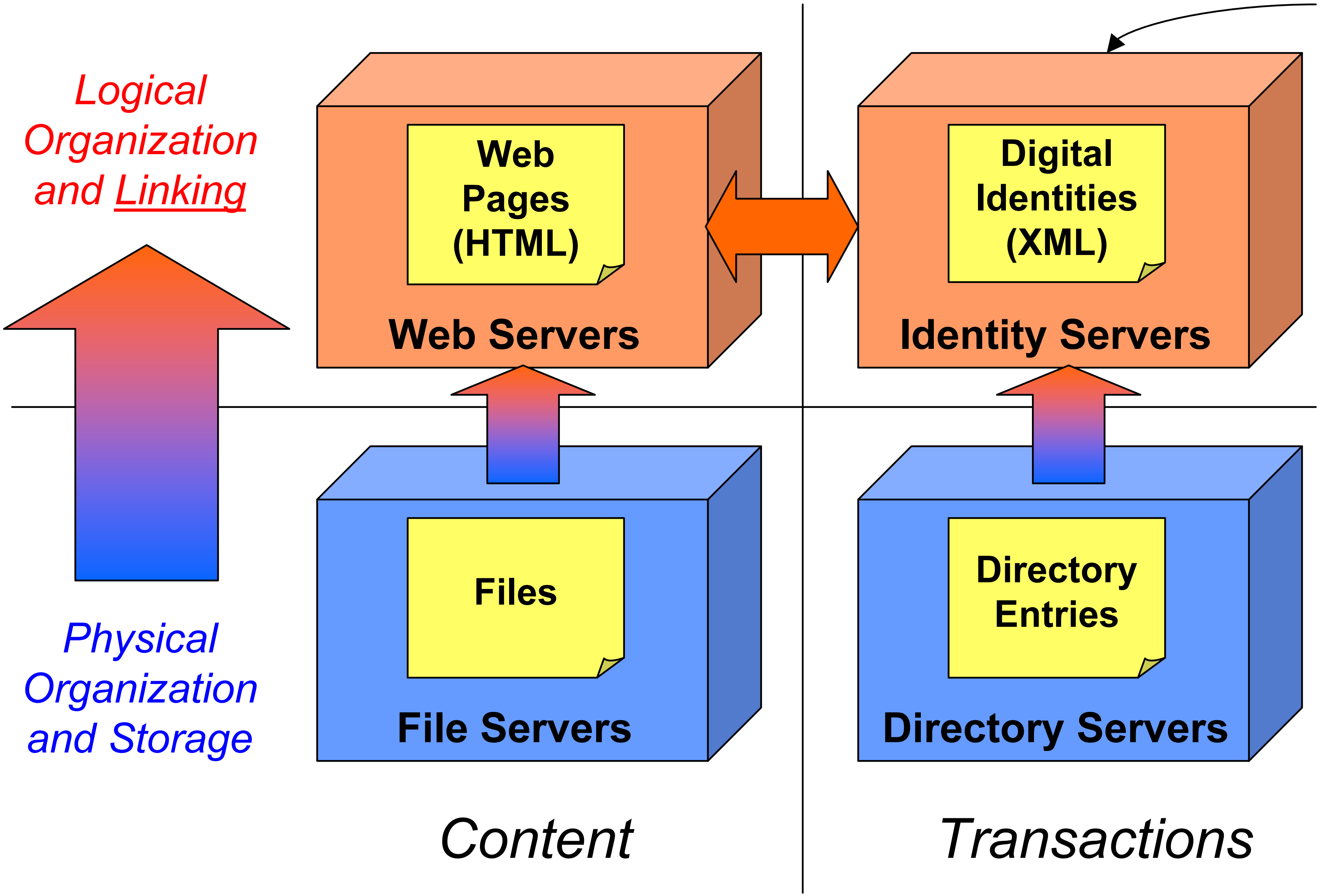
Millions of files were available on Internet-connected enterprise file servers but there was no common way to view, access, or link them.

Evolution of the Identity Web (step 2)



Today identity is in the same predicament as content was in ten years ago. It is constrained by the hierarchical organization and administrative control of directory servers. Sharing identity across domains is as difficult as sharing files across domains was in 1990.

Evolution of the Identity Web (step 3)



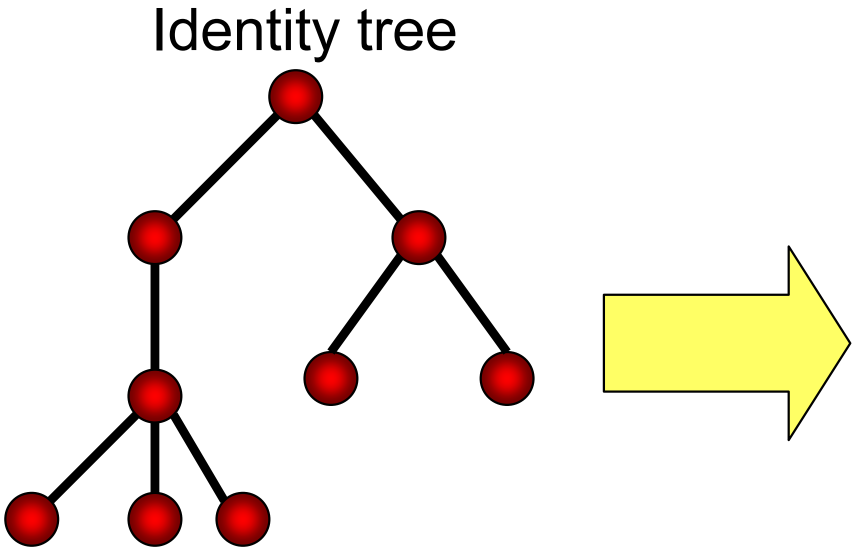
By abstracting identity to the logical level (XML), identity documents and identity servers solve the problem of identity sharing the same way the Web solved the problem of content sharing. In addition, XML digital identities can leverage the logical HTML viewing layer.

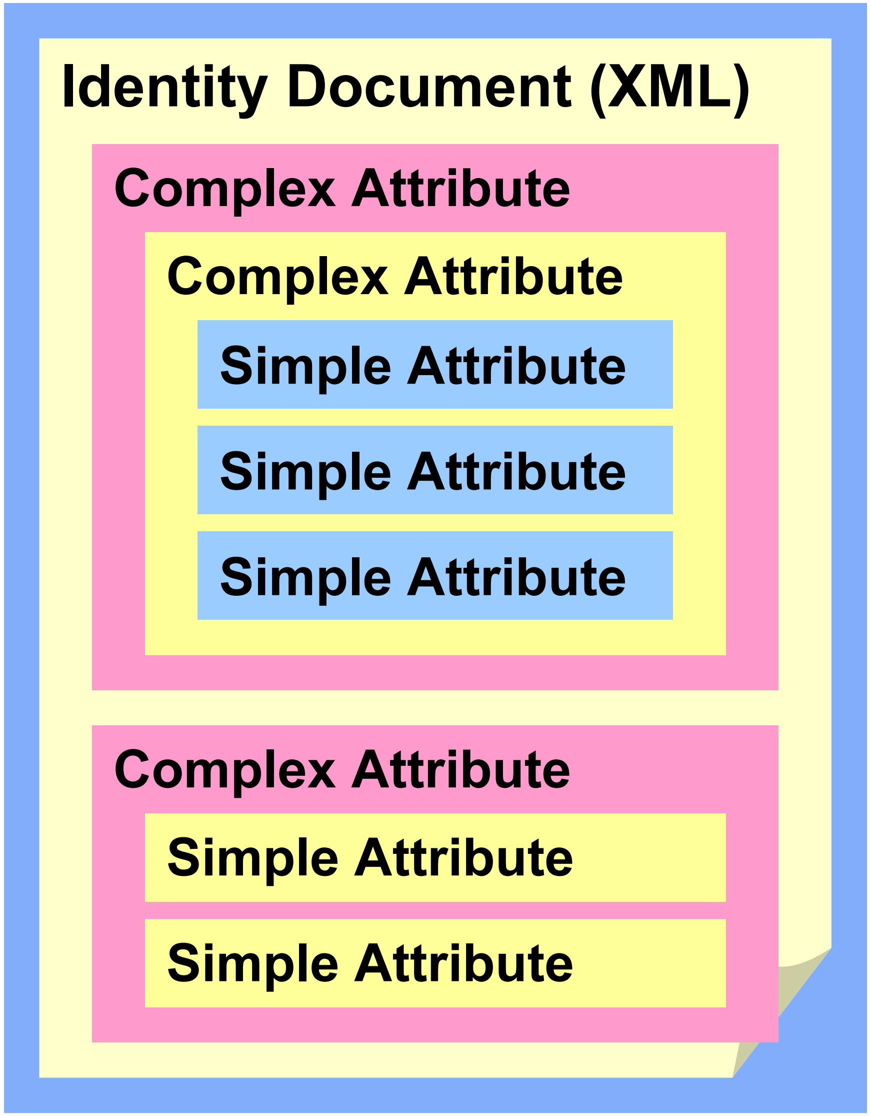
Adoption Factor	Document Web	Identity Web
Solves hard cross-domain interoperability problems	Sharing, linking, and indexing of digital documents (public data)	Sharing, linking, indexing, and control of digital identities (private data)
Uses vendor-neutral open standards	HTML (Documents) URLs & DNS (Addressing) HTTP (Protocol)	XML (Documents) URNs & XNS (Addressing) SOAP (Protocol)
Grows organically from network effect of linking	Hyperlinking – models information relationships	Identity linking – models personal and business relationships
Layers over existing systems	Web servers layer over file servers and databases	Identity servers layer over directory servers and databases
Spawns rich new market opportunities	Web sites, search engines, portals, ad networks, shopping carts, auction sites, rating sites, EAI, etc.	Identity providers, smart search engines, smart wallets, EAI, PKI, CRM, filtering, presence, etc.

Identity documents

- The Web is based on a common document markup language – HTML
- The Identity Web is based on a common document markup language – XML
- XNS is an XML vocabulary designed to provide a DOM interface to identity
- XNS identity documents are self-defining via XNS Discovery Service
  - Enables schema and service definitions to be stored as attributes of an XNS identity document

Identity documents





Identity Document (XML)

Complex Attribute

Complex Attribute

Simple Attribute

Simple Attribute

Simple Attribute

Complex Attribute

Simple Attribute

Simple Attribute

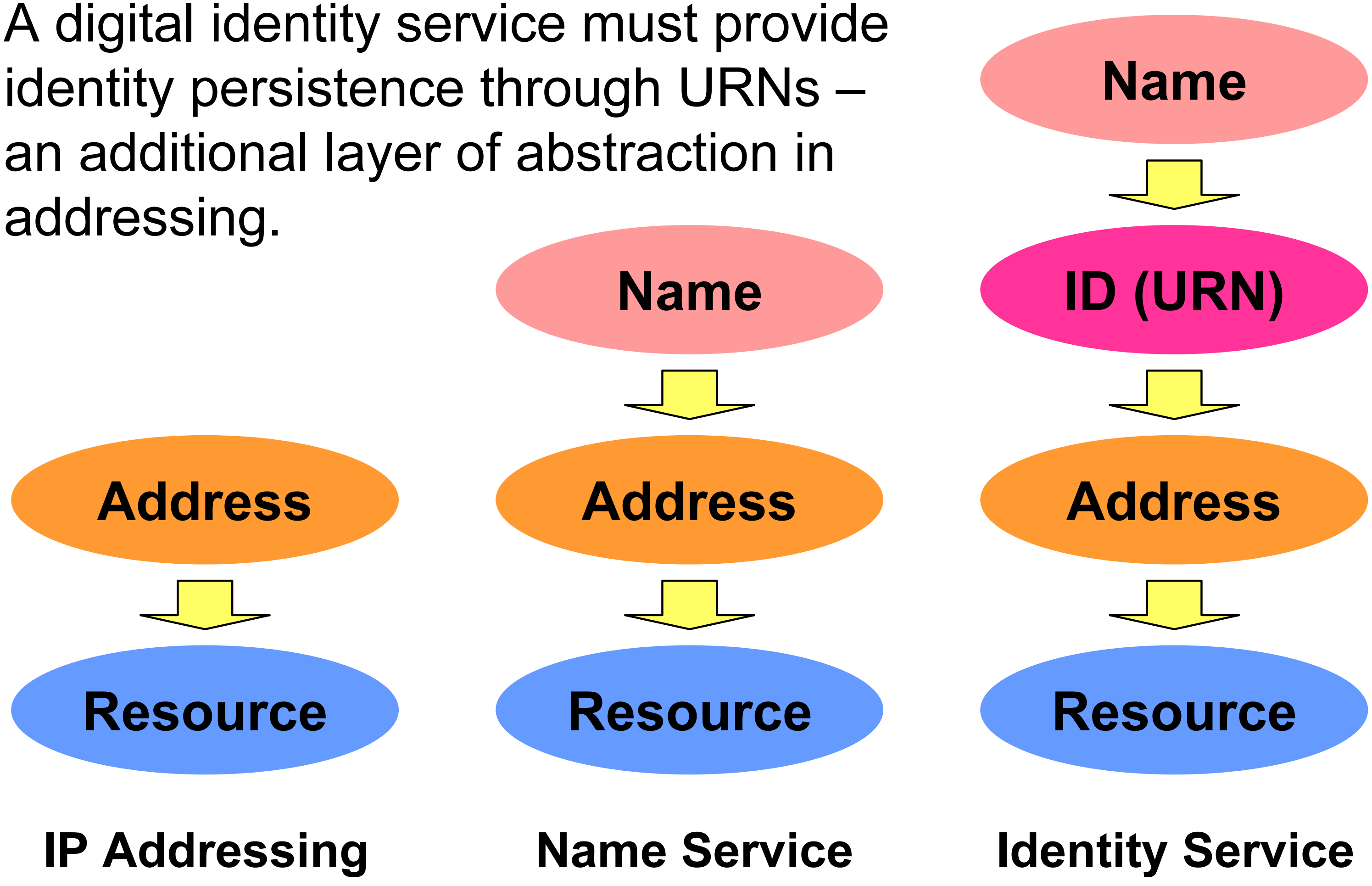
An identity document is an identity tree serialized as an XML document. An identity agent is the software process managing this document.

Identity addressing

- DNS provides a federated naming system
  - DNS names are vital to the URLs linking the Web
  - But links break when names change
- A digital identity infrastructure requires identity persistence
  - Identity doesn’t change when a name changes
  - This requirement is known as a URN (Uniform Resource Name) service
- XNS provides both federated IDs (URNs) and federated names for digital identities

Identity addressing

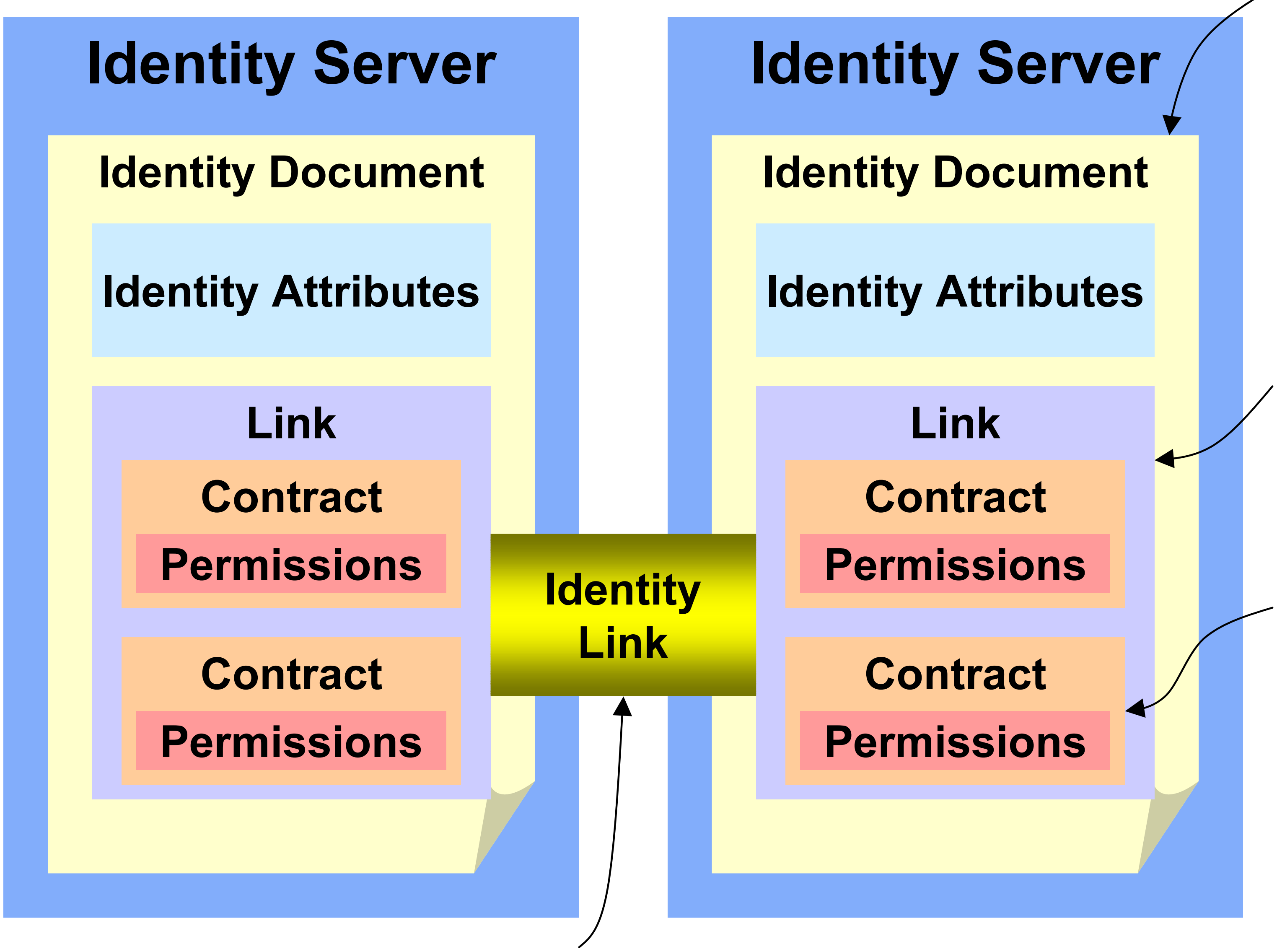
A digital identity service must provide identity persistence through URNs – an additional layer of abstraction in addressing.



Identity linking

- HTML Web pages are linked by inserting a reference to another Web page
- XML identity documents are linked by inserting a document fragment that describes the data exchange relationship
- The top-level element is a Link; it contains any number of Contract elements
- Each contract describes the attributes being shared and the terms governing the sharing

Identity linking



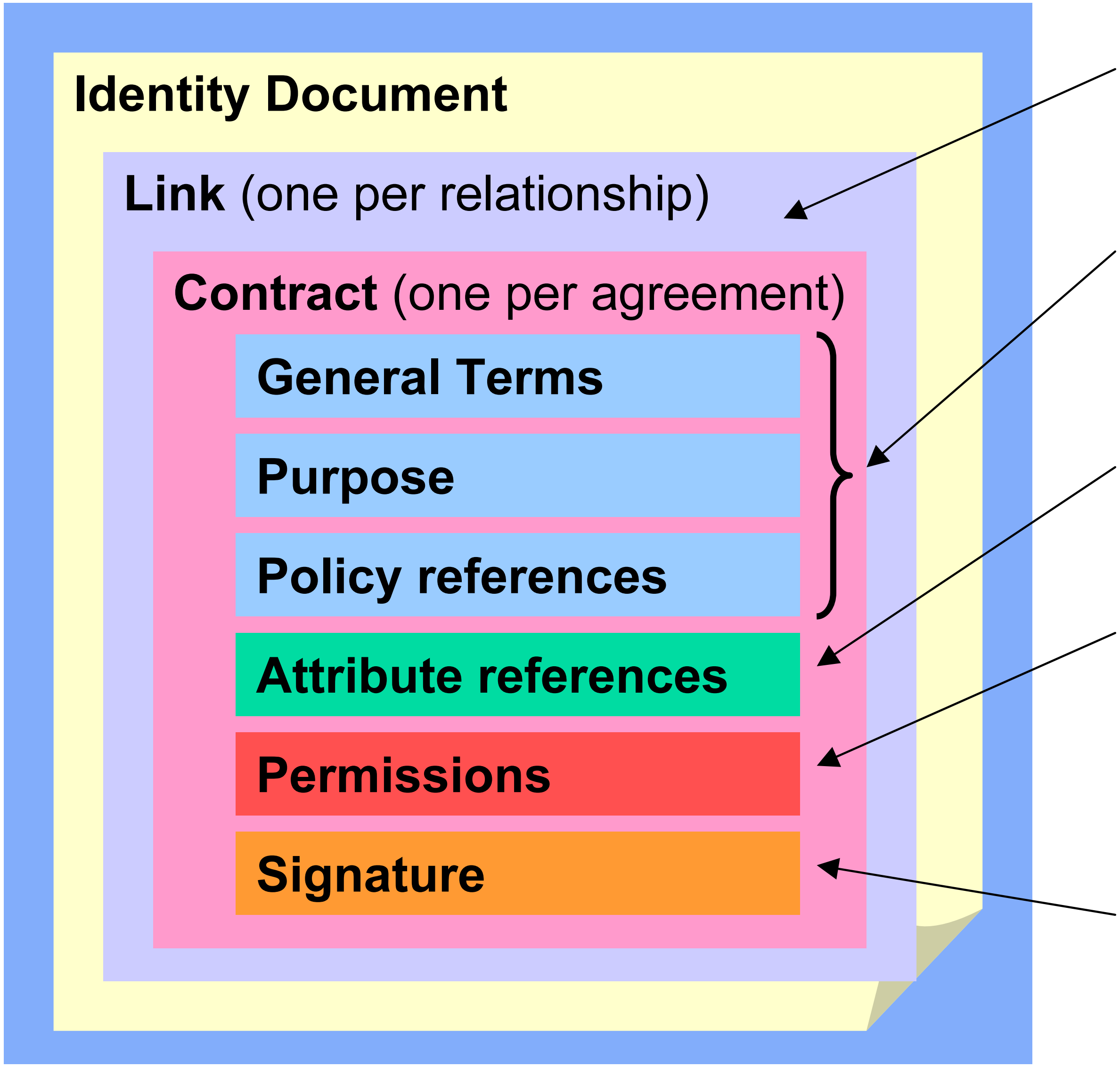
Identity servers host XML documents representing attributes associated with an identity. These documents can be "virtual", i.e., the physical data can be stored in lower-layer systems.

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



Identity Document

Link (one per relationship)

Contract (one per agreement)

General Terms

Purpose

Policy references

Attribute references

Permissions

Signature

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.

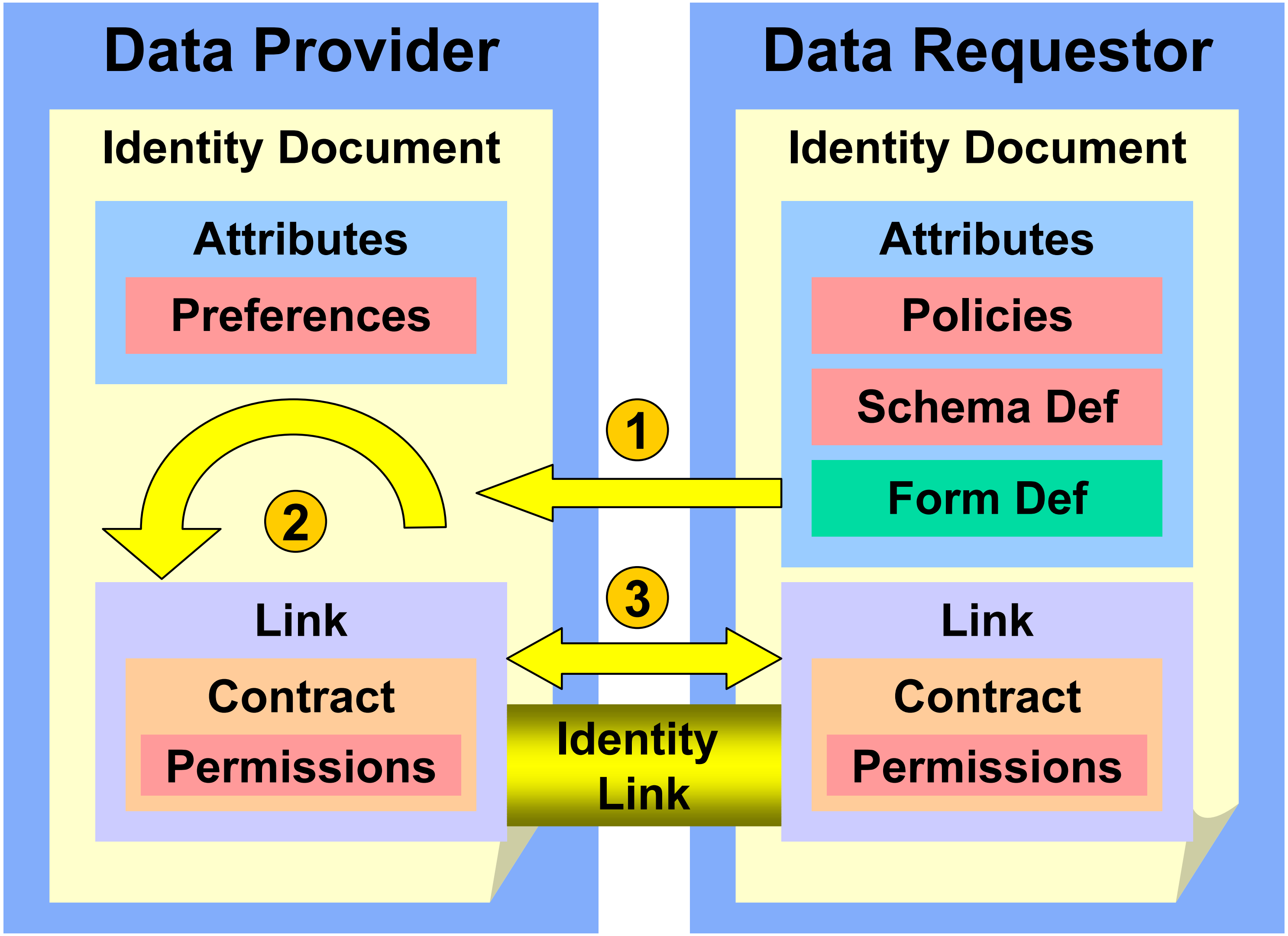
Permission objects are extensible to model any type of privacy policy (opt-out, opt-in, opt-over) in any legal jurisdiction. They also cover synchronization.

Contracts are signed and stored for auditing and non-repudiation.

Identity transactions

- Web pages accomplish bi-directional data exchange using HTML forms
- Identity Web transactions are accomplished using XNS forms
- A Form is a special XNS datatype that stores the XNS datatype instances being requested and the data protection terms being offered
- An XNS transaction is triggered by activating the URN of the form definition

Identity transactions

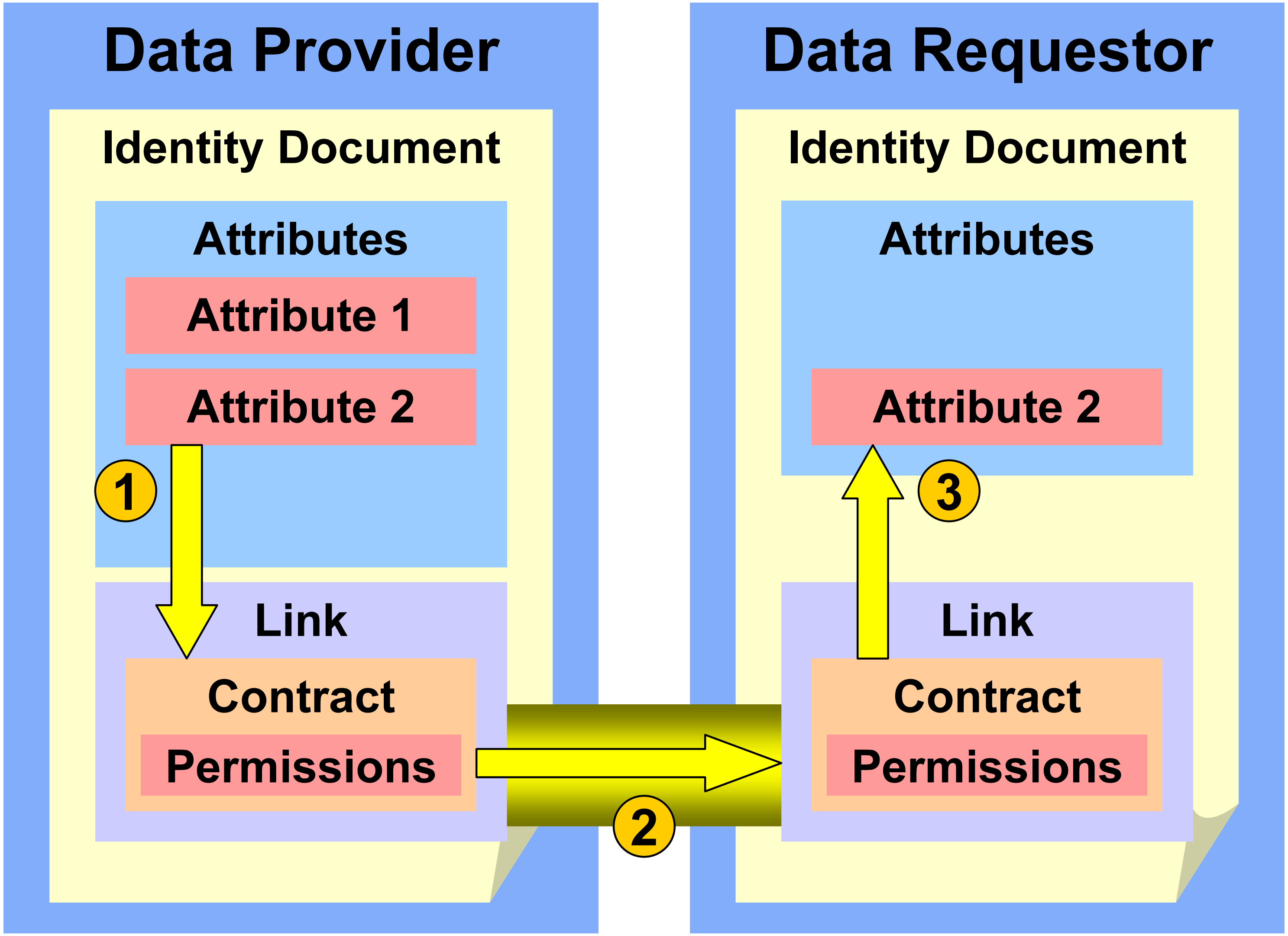


1) The DR identity sends an XNS form definition to the DP identity.

2) The DP processes the form based on the principal's attributes and preferences and negotiates the contract (negotiations may be single or multi-round)

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

Attribute synchronization



1) When the principal updates an attribute, the DP checks to see which contracts reference that attribute.

2) If the contract specifies a push, the DP composes an XNS Set message and attaches a SAML assertion.

3) The DR authenticates the message and updates the attribute.

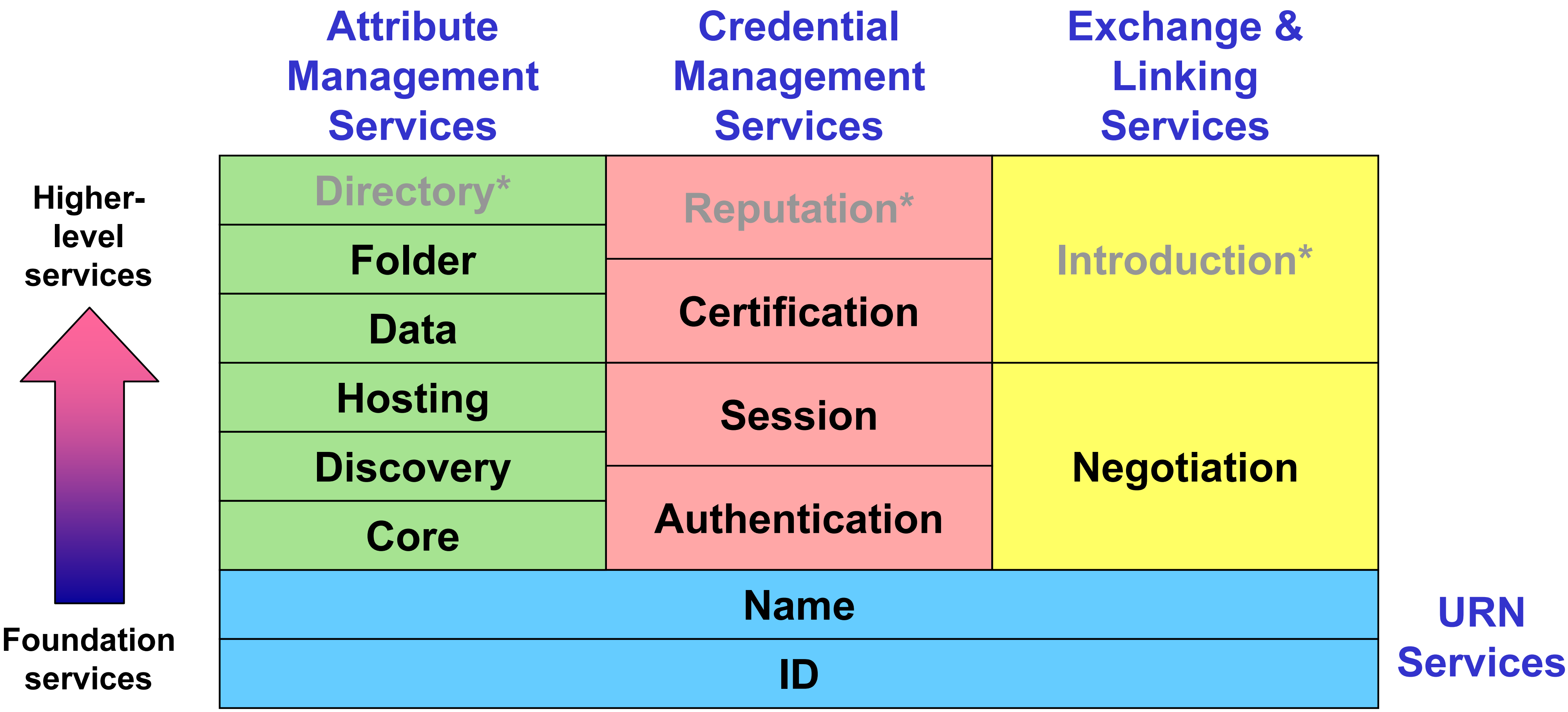
Identity credentials

- Real world trust relationships are based on credentials (passports, driver's licenses, etc.)
- Credentials are special identity attributes stored in identity documents
- XNS 1.0 includes three services specifically for managing credentials
  - Authentication for identity validation credentials
  - Session for login validation credentials
  - Certification for digital certificates (assertions regarding the attributes of an identity)

Identity services

- XNS 1.0 specifies eleven WSDL service definitions plus a XML-based URN syntax
- These services fall into four functional groups
  - URN Services for identity addressing
  - Attribute Management Services for reading, writing, and managing identity documents
  - Credential Management Services for obtaining and asserting identity credentials
  - Exchange & Linking Services for performing identity transactions and identity linking

The XNS 1.0 base services



Attribute Management Services

Credential Management Services

Exchange & Linking Services

Higher-level services

Directory*

Folder

Data

Hosting

Discovery

Core

Reputation*

Certification

Session

Authentication

Introduction*

Negotiation

Name

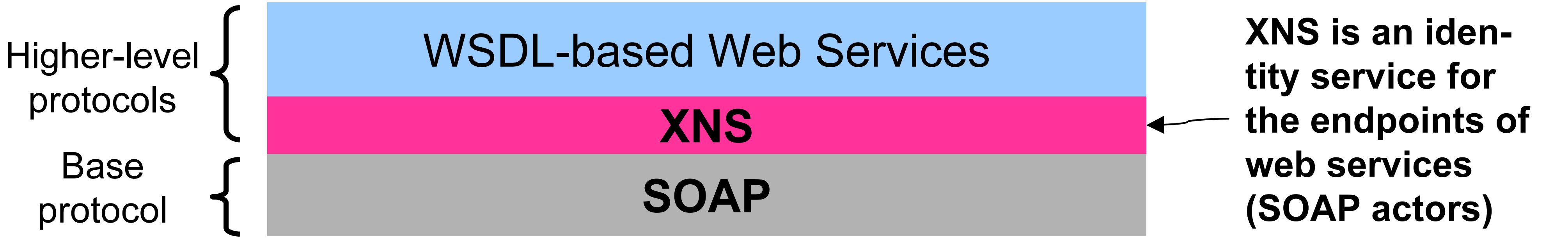
ID

URN Services

Foundation services

* Not defined in XNS 1.0 specifications

XNS parallels DNS at a higher layer



Higher-level protocols

Base protocol

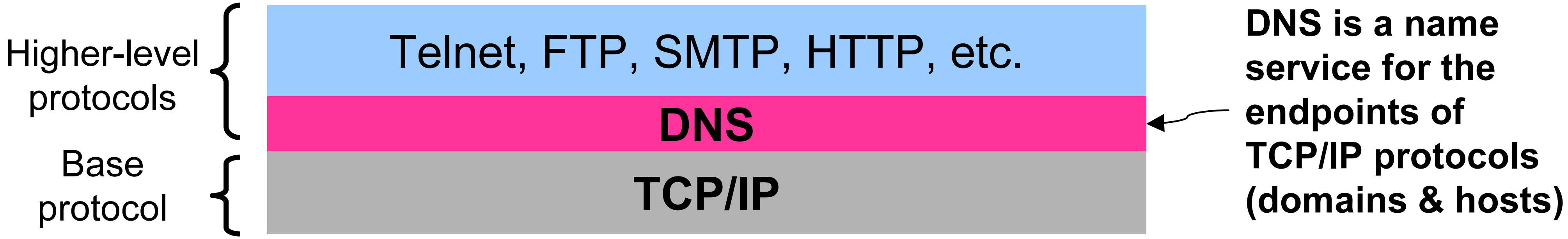
WSDL-based Web Services

XNS

SOAP

XNS is an identity service for the endpoints of web services (SOAP actors)

Application-to-Application Layer (XML Messages)



Higher-level protocols

Base protocol

Telnet, FTP, SMTP, HTTP, etc.

DNS

TCP/IP

DNS is a name service for the endpoints of TCP/IP protocols (domains & hosts)

Machine-to-Machine Layer (Packets)

For more information

- Additional resources available from XNSORG
  - The XNS Technical Specifications
  - XNS Technical White Paper (DNS vs. XNS)
  - XNS Use Cases
  - XNS Service Models
- The XNSORG Web site (www.xns.org)
  - Mailing lists
  - Forums / Wiki