Geneva, 21 September 2007

# Global Namespace Discovery using a XRI root-of-roots assumed by ITU-T

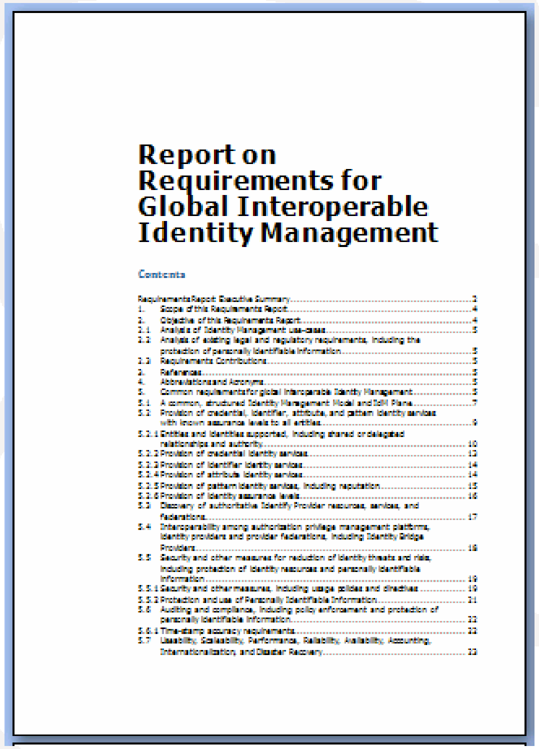
Tony Rutkowski

Chair, ITU-T IdM FG Requirements WG

trutkowski@verisign.com

XRI detail slides courtesy of Reed Drummond
OASIS Extensible Resource Identifier (XRI) TC
http://xri.net/=drummond.reed

# Identity Discovery Requirements



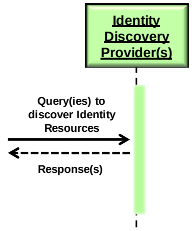
Report on Requirements for Global Interoperable Identity Management

Contents

a) **Discovery of authoritative Identify Provider resources, services, and federations.** A critical IdM challenge in the very dynamic and diverse world of network services and applications is discovering current authoritative sources for the four core IdM categories. It is not enough for the IdM capabilities to exist, if a relying party has no means for knowing who and how to contact the authoritative source of asserted identities. Discovery requirements are therefore an essential part of trusted Identity Management.

### 5.3 Discovery of authoritative Identify Provider resources, services, and federations.

A critical IdM challenge in the very dynamic and diverse world of network services and applications is discovering current authoritative sources for the four core IdM categories described above or the federations that are associated with enabling discovery and access of the relevant IdM resources. It is not enough for the IdM capabilities to exist, if a relying party has no means for knowing who and how to reach and interoperate with the authoritative resources for asserted identities treated in the sub-section below.



Identity Discovery Provider(s)
Query(ies) to discover Identity Resources
Response(s)

Fig. 9. Identity Management Discovery Services

A very significant number of contributions and use-cases during the entire activity period of the Focus Group dealt with Discovery capabilities and associated requirements. Discovery capabilities seem to be widely recognized as one of the most significant needs and gaps – including a consensus that the challenge of providing effective Discovery capabilities are therefore an essential part of trusted Identity Management.

Some federations and communities surrounding Open Identity protocols have developed partial solutions to meet discovery needs within the boundaries of their user communities. However, there are no current means for global or inter-federation discovery.

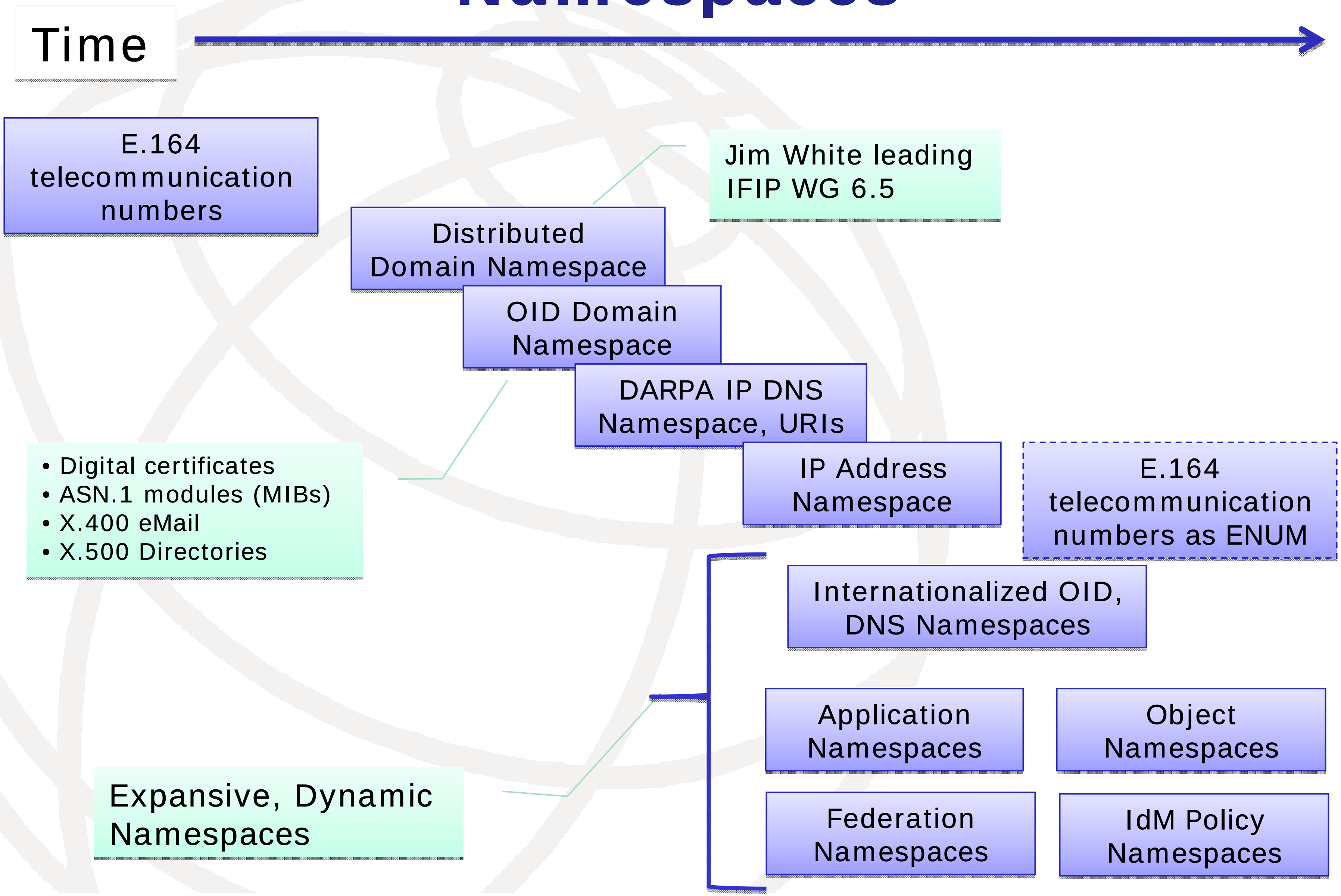
One of the potential solutions to this need involves the use of the OASIS XRI platform and its implementation by a universal global mechanism involving one or more meta-registries and resolvers. Developing a consensus on pursuing this path, including the ITU-T/TSB acting as the global mechanism, remains for further work.

Sec. 7 of the Use-Case Report and existing industry requirements specifications provided source information for this requirement for this model.

R1 : It is required that Identity Providers and Relying parties be able to support mechanisms for a Relying Party to discover other Identity Providers with whom a Requesting/Asserting Entity has both authenticated and provided forms of Identity, subject to applicable Policy. These discovery mechanisms include characteristics and Policies of the interfaces, dynamic registration and de-registration of federation relationships, authentication, permissions, and attributes.

R2 : It is recommended that Identity Providers be able to support business agreement Policies across Federation or other trust domains.

# History of Public Network Namespaces



Time

E.164 telecommunication numbers

Distributed Domain Namespace

Jim White leading IFIP WG 6.5

OID Domain Namespace

DARPA IP DNS Namespace, URIs

- Digital certificates
- ASN.1 modules (MIBs)
- X.400 eMail
- X.500 Directories

IP Address Namespace

E.164 telecommunication numbers as ENUM

Internationalized OID, DNS Namespaces

Application Namespaces

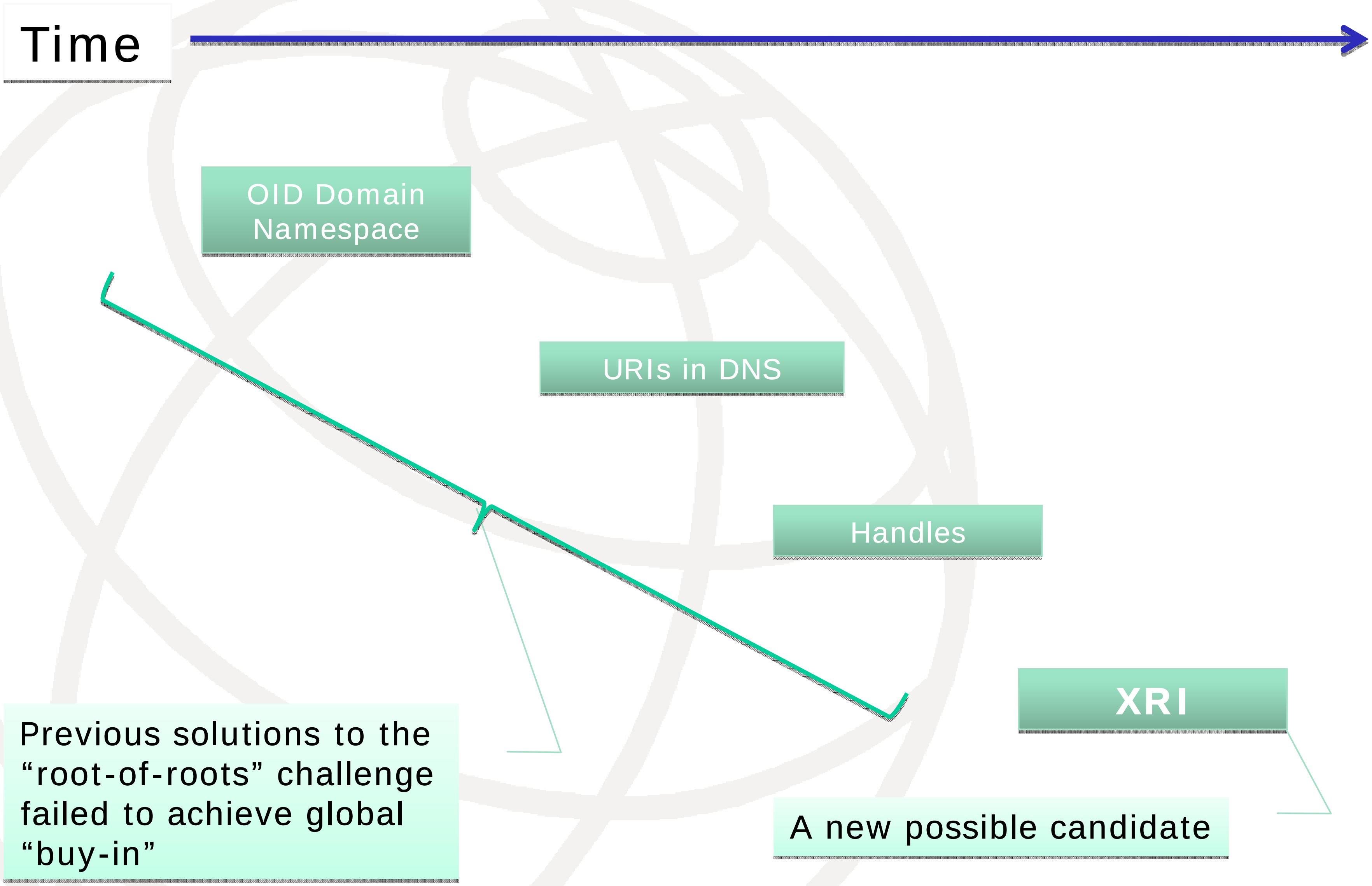
Object Namespaces

Federation Namespaces

IdM Policy Namespaces

Expansive, Dynamic Namespaces

# History of Discovery Solutions



Time

OID Domain Namespace

URIs in DNS

Handles

XRI

Previous solutions to the “root-of-roots” challenge failed to achieve global “buy-in”

A new possible candidate

# Emergence of XRI?

- Attempt to solve the “root-of-root” challenge
- Undertaken by an OASIS Technical Committee started in January 2003
- Resulted in XRI - Extensible Resource Identifier
- An open standard language for structured identifiers that are independent of domain, application, protocol, or language
- “XML for identifiers”

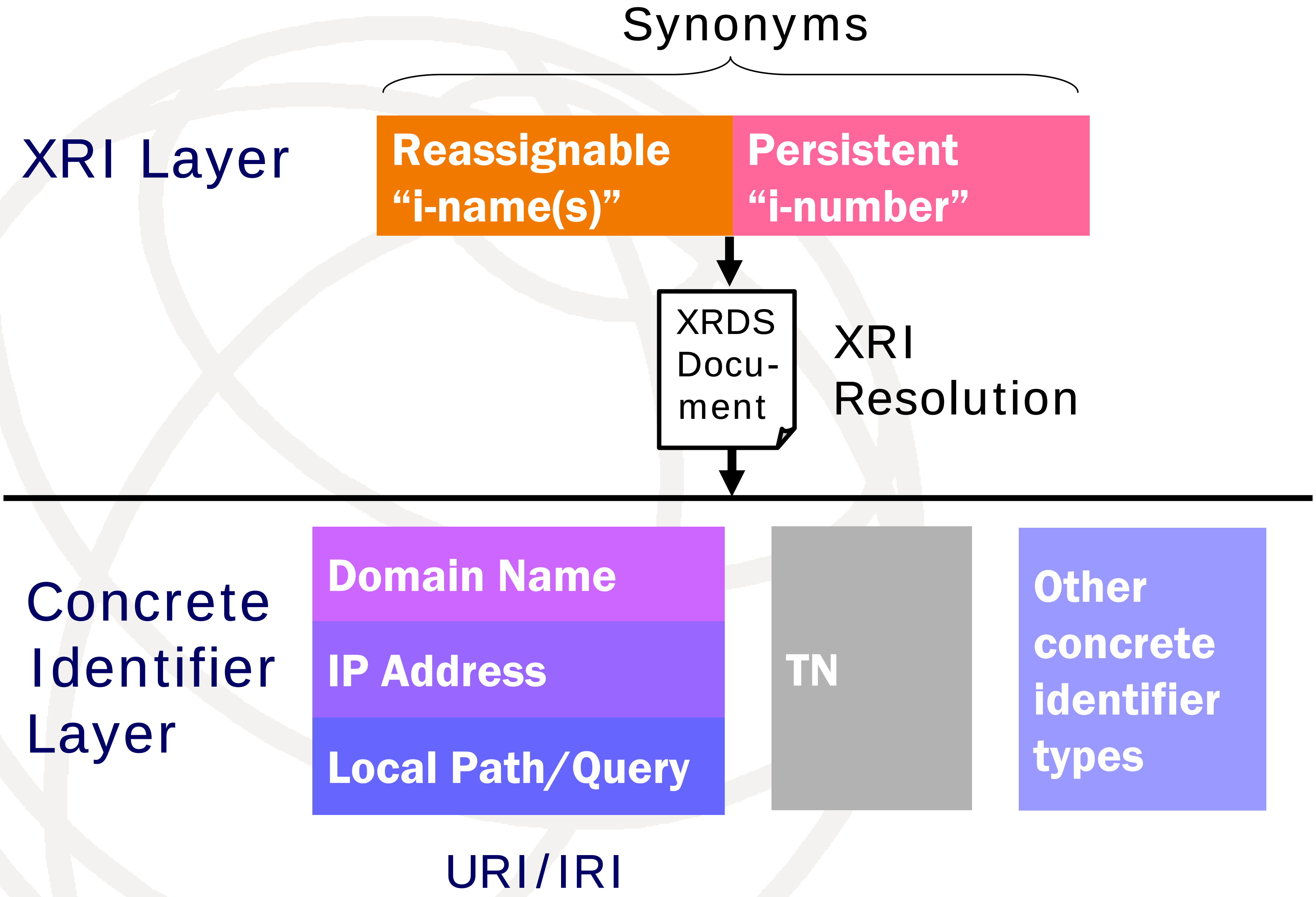
# An Introduction to XRI and XRDS

# What is XRI?

- "XRI is to URIs what DNS is to IP addresses"
  - XRI provides an abstraction layer over concrete URI addressing just like DNS provides an abstraction layer over IP addressing
- XRI provides three key features not available in URI architecture
  - Structured ("tagged") identifiers
  - Robust synonym expression and resolution
  - A uniform extensible discovery, resolution, and description protocol

# What is XRDS?

- Extensible Resource Descriptor Sequence
- Very simple, extensible XML document format for service discovery for any XRI- or URL-identifiable resource
- The logical equivalent of a DNS resource record at the XRI layer of identification
- Adopted as the OpenID discovery format



Synonyms

XRI Layer

Reassignable
"i-name(s)"

Persistent
"i-number"

XRDS Docu-
ment

XRI
Resolution

Concrete Identifier Layer

Domain Name

IP Address

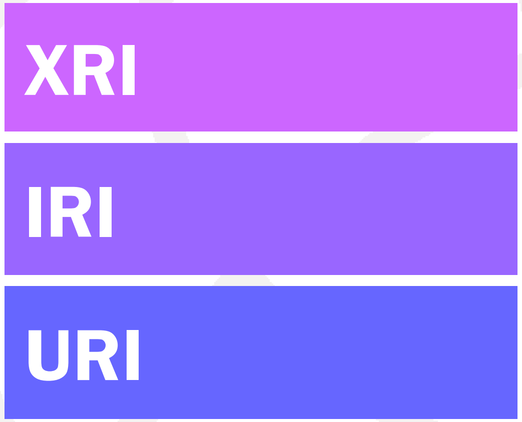
Local Path/Query

TN

Other concrete identifier types

URI/IRI

# How does XRI fit with URI & IRI?



XRI — Same charset as IRI, extends syntax

IRI — Same syntax as URI, extends charset to UCS

URI — Generic syntax, ASCII only

- XRI is backwards compatible with URI (Uniform Resource Identifier) and IRI (Internationalized Resource Identifier)
- Any XRI can be “downcast” into IRI and URI forms for backwards compatibility

# How is XRI like “XML for identifiers”?

- XRI enables self-describing structured identifiers – identifiers that describe other identifiers (“tagging”)
- Two key syntactic constructs:
  - Parenthetical encapsulation
  - Context symbols (=, @, +, $, *, !)
- Examples (using XRI 3.0 syntax:

@company =(http://example.com/user )+fax

@company =(tel:+1.206.618.8530)+fax

# Example XRIs (in XRI-normal form)

=drummond.reed

=!1234.5678.a1b2.c3d4

$(http://equalsdrummond.name)

@cordance

@!8fb6.9dfc.d1fd.e073

+résumé

@cordance*drummond

@cordance*drummond/local/directory/résumé.html

@cordance*drummond/+résumé$v*2+html

@!76d3.f297.90e2.142d!10c7/+!87$v!2

$(ip:206.198.17.5)/some/path?some=query

$(dns:www.cordance.com)/some/path#somefragment

i-name
i-number

# XRI resolution

- Goal: a simple, easily-deployed infrastructure for resolving XRIs to URIs much like resolving DNS names to IP addresses
- Design: use HTTP(S), XRDS documents, and SAML assertions (optional)
- Enable discovery and selection of service endpoint metadata for any type of service associated with a resource

# Example XRDS document for “=example”

```
<XRDS xmlns=“xri://xrds”>
 <XRD xmlns=“xri://xrd*($v*2.0)”>
  <Query>*example</Query>
  <Expires>2005-05-30T09:30:10Z</Expires>
  <ProviderID>xri://=</ProviderID>
  <CanonicalID>xri://=!7c4.58ff.7c9a.e285</CanonicalID>
  <Ref>xri://@!2017.cd67.94c8.023!c83d</Ref>
  <Service>
    <Type>xri://$res*auth*($v*2.0)</Type>
    <URI>http://res.example.com/=!1234.5678.a1b2.c3d4/</URI>
   </Service>
  <Service>
    <Type>http://openid.net/openid/1.1</Type>
    <Type>http://openid.net/openid/2.0</Type>
    <Path>+openid
    <URI>http://authn.example.com/openid/</URI>
  </Service>
  </XRD>
</XRDS>
```

# XRI adoption

- **Boeing** (www.boeing.com, @boeing) is standardizing on XRI for global identifiers
  - Published in their Enterprise Directory service for all people, applications, and devices
  - Deploying in new web services
  - Using for principals in SAML assertions
- **OpenID 2.0** (www.openid.net) supports XRI identifiers and uses XRDS for service discovery
- **I-names** (www.inames.net, @inames) uses XRI for privacy-protected global digital identity and XRDS for service discovery

# A Preview of XRI 3.0

# Background

- XRI Syntax 2.0 was voted a Committee Draft in March ’05 and a Committee Spec in Dec ‘05
- XRI Resolution 2.0 was voted a Committee Draft 01 March ‘05 and has since been widely implemented
  - Produced a large volume of implementation feed-back, especially from OpenID, Higgins, and XDI
  - Resulted in a nine month process to produce Committee Draft 02, to be voted on this month
  - The process also produced requirements (and most of the design work) for XRI 3.0

# Key requirements for XRI 3.0

- More robust forms and transformations
- Support for simplified XRI “tags” and streamlined XRI ABNF and processing rules
- Support for WS-Addressing endpoint references in XRDS documents
- Support for “pluggable” resolution and additional resolution formats (Handle and XDI)

# Simplified XRI "tags"

- XRI 1.0 and 2.0 required all cross-referenced identifiers in an XRI, including other absolute XRIs, to be encapsulated in parentheses

  **=drummond*(+work)/(+tel)*($v*3)**

- The syntax is much simpler and more expressive if absolute XRIs can be concatenated directly

  **=drummond+work/+tel$v*3**

# Support for WS-Addressing EPRs

- XRDS documents currently use service endpoint descriptors (SEPs)
- Adding support for WS-Addressing endpoint references (EPRs) is very straightforward
  - EPRs contain the metadata needed for WS-Addressing
  - An XRDS service endpoint may be described by both a SEP and an EPR in the same XRDS
- This facilitates integration of XRI within WS-* architecture and vice versa

# “Pluggable” resolution

- XRI resolution currently uses HTTP(S) and XRDS documents
- By making it pluggable, other resolution formats and protocols can be supported
  - Handle is already in discussion
  - XDI TC has already done preliminary design work
- Most requirements for doing this have already been incorporated in the extensibility architecture of XRI Resolution 2.0 CD02

# IMPLEMENTATION

# How XRI could support global IdM discovery requirements

- Would require a global consensus on
  - An appropriate protocol (XRI transferred to ITU-T)
  - A suitable registration authority (ITU-ISO auspices)
  - Resolver service (fast XML or equivalent)
  - Directory query service (E.115, IRIS, or similar)
- Instantiation of the consensus in appropriate agreements
- Implementation

# Next Steps

- Broad discussion of the basic requirement and possible XRI solution
- Agreement in ITU-T, WTSA, ISO, and other venues
- Transfer of XRI specifications to ITU-T
- Agreement on ancillary support specifications for registration, resolution and directory
- Transfer of existing registrations to TSB
- Initiation of registration functions by TSB with necessary on-line registrar, resolver, and directory support capabilities

# APPENDIX

# Specification status

| Spec | Covers | Status |
|---|---|---|
| **Syntax** | ABNF, character set, forms and transformations, equivalence | 2.0 Committee Specification (December 2005) |
| **Resolution** | XRDS, generic protocol, trusted protocol (HTTPS & SAML), service selection, reference processing, synonym verification | 2.0 Committee Draft 02 (vote this month) |
| **Dictionary** | Standard XRI tags for language, date, version, etc. | 1.0 Committee Draft (February 2005) |

OASIS

# XRI Technical Committee

VISA

AMD

BOEING

NRI 未来創発

Dream up the future.

Booz | Allen | Hamilton

90 years delivering results that endure

Cordance

NEUSTAR®

epok

AmSoft Systems

identity commons

XDI.org

# The primary goals of XDI

- Develop a standard data interchange schema & protocol based on XRI, XML, & Resource Description Framework (RDF)
  - RDF is the W3C standard for encoding knowledge
  - “XDI is to RDF what HTML is to SGML”
- Enable “link contracts” – machine-readable data sharing agreements that bind shared data to policies governing its use
- Enable machine-readable XDI dictionaries that enable automated mapping of XRI-identified data across schemas & contexts

# Appendix 3
# An Introduction to XDI

# The XDI “Structured Web” model

- Applies the Web model to machine-readable data sharing
  - XDI documents are XRI-addressable the same way HTML documents are URI-addressable
  - XRI addressing/linking goes all the way down to the atomic data element level (URI addressing/ linking goes only to the document fragment level)
  - XDI addressing can reference and link elements across XDI documents just like HTML hyperlinks

# XDI and RDF

- XDI documents are collections of RDF statements using XRIs instead of URIs
  - Using XRI cross-reference syntax, all XDI RDF statements are expressable as structured XRIs
  - XDI RDF vocabulary consists of just four core XRIs to describe resource relationship types
- Dramatically simplifies/standardizes cross-domain data description and exchange
- XDI dictionaries function as machine-readable, self-describing RDF vocabularies

# XDI documents

- XDI documents can be serialized in many different formats
  - XDI/XML
  - XDI/JSON (Javascript Object Notation)
  - X3 – based on RDF N3
  - X-Triples – based on RDF N-Triples
- They all make RDF statements even easier to read that most XML documents
- Following is an example XDI business card in X3 format

# The Community Dictionary Service

- The Higgins Project and the Identity Schemas Working Group of Identity Commons are collaborating on an XDI-based Community Dictionary Service
- This facilitates cross-domain data sharing by using a shared XDI dictionary of common schemas and schema mappings
- An alpha was shown at the Data Sharing Summit (http://datasharingsummit.com)
  - See http://cds.idschemas.idcommons.net

# XDI link contracts

- A link contract is an XDI document governing an XDI data sharing relationship between two XDI data authorities
  - It “binds” XRI-addressable data to XRI-addressable policies governing its use
  - It can cover any type of XDI data (including other link contracts)
  - It can associate any type of data sharing policy
- Link contracts are the first easily portable cross-domain authorization format

# XDI adoption

- First prototype XDI engine implemented by Ootao (www.ootao.com, @ootao)
- ooTao and Kintera (www.kinterainc.com) have announced a major XDI data sharing project for La Leche League
    - 100K+ data sharing accounts
- XDI will be a key data sharing protocol supported by the Higgins Project (www.eclipse.org/higgins/)

# XDI 1.0 specifications

- The proposed XDI 1.0 design takes advantage of key features of XRI 3.0
- The XDI TC plans to draft the XDI 1.0 specifications concurrently with the XRI 3.0 specifications
- This will also enable XDI 1.0 to be supported as an XRI 3.0 resolution format
- The goal is to complete both by the end of Q1 2008