Some Thoughts on Digital Identities

Geoff Huston AM
Chief Scientist, APNIC

November 2023
What do we want from an “identity schema”?

Varying degrees of:

- Uniqueness
- Persistence
- Structure
- Clear Scope of Applicability
- Validity and Authenticity
- Clear line of derivation of “authority”
- Unambiguous resolution

Identity is not a unilateral assertion – it’s a recognition of derived uniqueness within a chosen frame of reference.
What should we avoid in an “Identity” schema?

Varying degrees of:

• Uncoordinated self-assertion
• Arbitrary token value collisions
• Ill-defined temporal validity
• No coherent structure
• Unclear applicability
• Semantic overload
• Structural overload and complexity of the token space
• Cost
So What?

All this is rather abstract

Would an example help?
URLs as a Digital Object Identity schema

• We tend to use URLs as referential tokens to identity digital artefacts:
  • what is synonymous with where in an object-oriented world
  • where then becomes a viable non-clashing identifier scheme that also happens to dictate a resolution mechanism at the same time
  • All we need to a methodical approach to where and we’re done!
• Easy, simple and used ubiquitously in our digital world
What’s the problem with URLs?

• URLs are *where*, not *what*
  “If you go *there* then what you find *there* is what I’m referring to”

• URLs describe a retrieval algorithm for an object instance, not an object identifier

• They are insecure, vulnerable to all kinds of abuse and inappropriate to our conventional methods of utilizing information

• They offer the comforting illusion of identity without imposing the actual cost of true integrity and authority
Identity Scheme Choices

• It’s possible to inject an identity scheme into almost any part of a digital information system
  • Application or Service Identities
    • phone numbers, Skype IDs, email addresses, URLs, Google Search terms
  • Structured Namespace identities
    • DNS names, X.500 Distinguished Names, ISBNs, DOIs, Handles
  • Abstract Identities
    • Public Key, Hashed Public Key, Session Identifier, UUIDs

In this context an “identity” is a token to allow multiple instantiations of an object to be recognised as belonging to a single equivalence class
Identity Scheme Choices

Organised Namespaces

• Compound objects that may include identification of an issuer, subject, issuance, metadata...
  • DNS NAMES
    • Unique chain of named issuer – subject relationships to create a compound name and coupled resolution mechanisms
  • E.164 Phone Numbers
    • Historically: Country, Area, Provider, Subscriber
    • Currently: ?
  • X.500 names
    • ?
  • ISBNs
    • Group, Publisher, Title, check
  • PKIs (Certificates)
    • Issuer, Subject, Subject Key, Attributes

• Identity as a “bestowed token”
Choices, Choices, Choices

Disorganised Namespaces

• Low overhead access to uniqueness above all else
• Public Keys or Hash value of a Public Key
  • Block of bits without internal structure
  • Robustly provable provenance (via private key)
  • No implicit association to object instances
  • Can be replicated at will without dilution of its uniqueness
  • No structured search, no defined resolution

• Identity as a “proof of possession”
Identity Resolution Issues

• Use of an “Identity” is to resolve it into useable attributes and values
• We can look at identity and resolution of identity as related, but distinct, concepts
• Is the identity resolution function:
  • Absolute or relative to the query?
  • Absolute or relative to the identity token issuer?
  • Dynamic or static?
  • Configured or negotiated?
  • Deterministic?
  • Temporal?
  • Assured to terminate?
  • Assuredly valid?
  • Assuredly secure?
Identity Schema

“Conventional”
• Construct a compound object that combines external identification realms of the identity issuer and the means to resolve the token in the context of the issuer
Identity Schema

“Compound Referential”

- Use a series of identity elements with a set of resolution mechanisms

- DNS: Resolve the DNS string using conventional DNS resolution
- Service: Resolve the following parts in the context of a Named applications
- Args: Pass these arguments to the local instance of application
- Quals: Apply these qualifiers to the application outcome
Identity Schema

“Ephemeral”

• Use an opportunistic identity as a means of resolving uniqueness in a limited context
Identity Scopes

Is identity:

• What I call myself?
• What I call myself in relation with others?
• What I call myself in relation with others today?
• What you call me?
• What they use to call me?
• All of the above?
• None of the above?
Upper-Level Issues of Identity Realms

• The significant effort and cost of supporting a new global unique token distribution system as an identity system
• The unintended side-effects of reusing some other existing token set as an identity component
• The issue of the relationship between identity and resolution mechanisms
• The overhead of identity resolution for application-level transactions
• The security issues in maintaining integrity of identity and integrity of resolution
百花齊放，百家爭鳴 *

• One identity scheme will not comfortably suit all forms of use:
  • Information as objects vs information as an outcome of collaboration
  • Associating the metadata with the object, not the identifier
  • Disassociation of attribute discovery from the identity space
  • Disassociation of object identification from object instantiation
  • Bestowing attributes and permissions to an identified instance

• We use a collection of URLs, URIs, DNS names, DOIs, Digital Passes, Certificates, Keys
  • Each have their areas of application, relative strengths and weaknesses

• And this collection of identity schemes will probably keep on expanding over time!

* Let a hundred flowers bloom: let a hundred schools of thought contend
  Mao Zedong, 1956
Thank You!

Questions?