Goedel
Protogen
Omnibroker

Phillip Hallam-Baker

Comodo Inc.

3 Parts:

1. A software tool for building software tools
   - Goedel
2. A software tool for bulding Web Services
   - ProtoGen
3. A protocol & spec built with the above tools
   - Omnibroker

Meta: What is a standard

- Making standards is the process of making choices where that choice does not matter
  - Choices that matter = functionality
  - All else = Rat Hole

- I have spent too long re-litigating style issues
  - Mostly with the same people
  - Lets just pick one way folk, *please…*

How do tools help?

- It is very fast
  - Design and implement a spec in 5 days
  - Can play 'what if' during design
- The specification and code are kept in lockstep
  - Examples are validated on every document run
- The tools have a set of choices built in
  - They can be changed, but at a price
  - ProtoGen currently builds Web Services in a REST style using JSON encoding
    - Adding XML/SOAP would be about 2 weeks work on the tool
    - Same for output of production code or C or Objective C

- ***Forcing consistency improves the specification***

Omnibroker 0.1

- Original objective
  - Tunnel OCSP queries over DNS
  - Use lightweight MAC for authentication
- Architecture (c.f. Kerberos)
  - Connection Server (JSON Web Service)
    - Distributes authentication tickets
  - Query Server
    - Returns certificate status response

PKI 2.0

Its all about the Relying Party

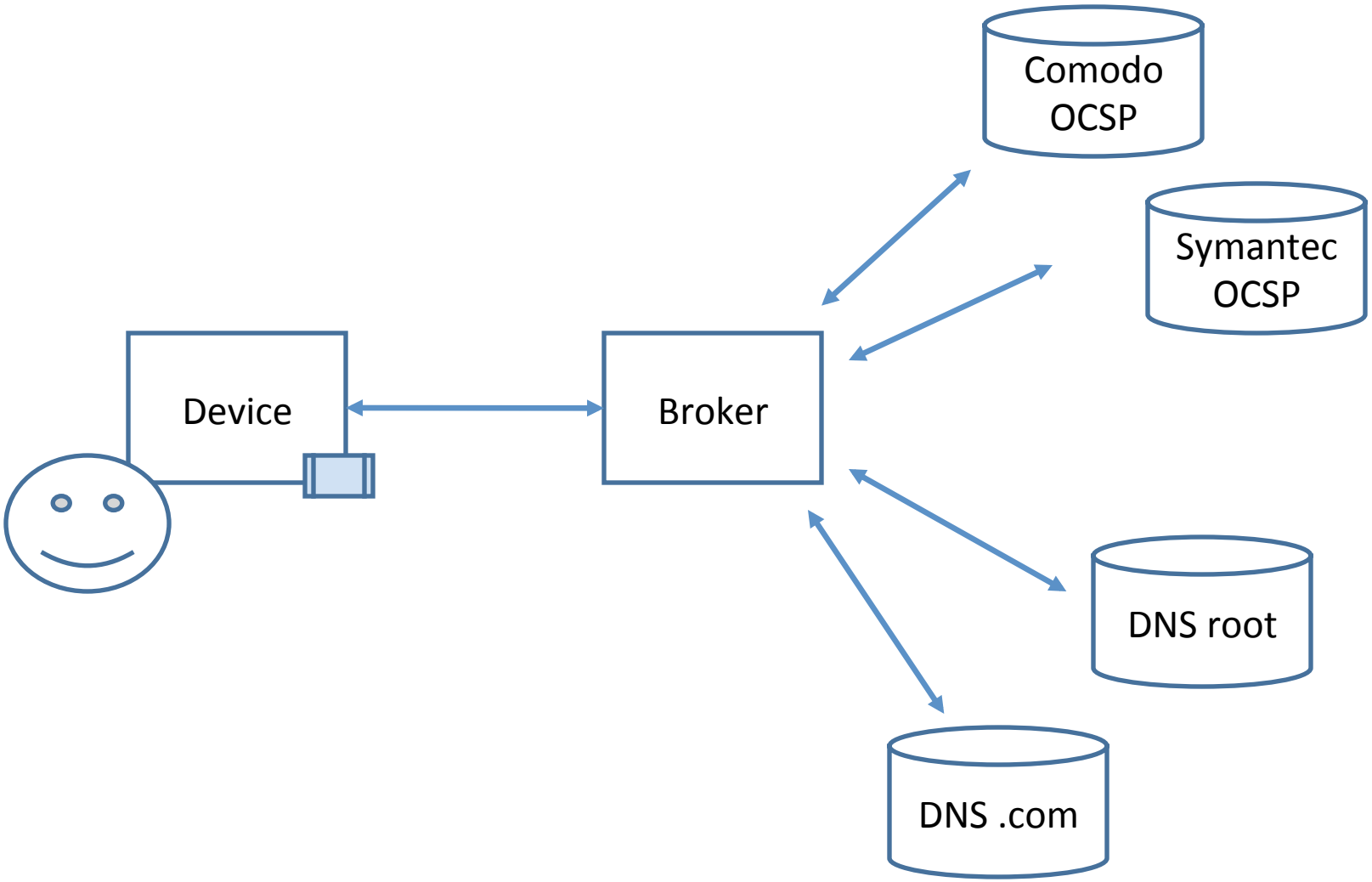
- New Architectures:
  - Perspectives
  - Convergence
  - Certificate Transparency
- New Infrastructures
  - DNSSEC
  - DANE

- Anti-Virus Perspective:
  - How do I give my customers access to these?
  - Which will win?
  - Proprietary or Open Standard?

‘++XKMS in JSON’

- XKMS:
  - “What key should I use to access host X via protocol Y”
- Trustbroker Connection query
  - “What IP address, port and transport protocol should I use to access host X via protocol Y”

Architecture



Feature Creep

- There are two ways to deal with a slippery slope, with crampons or with skis.

or

- Omnibroker uses rocket skis
  - A gateway to ***any*** trust service

Omnibroker Current Status:

- Client
  - Query: newprotocol at example.com
  - Response: IP=10.1.2.3, TLS, cert=…
- Server
  - Advertise <service description>
  - Broker performs DNS, LDAP, etc. config
- Peer to Peer
  - Endpoints are user@domain rather than domain

In development:

- Time
  - For preventing replay attacks
- Bookmark sharing
- Password storage
  - Because humans cannot remember strong passwords
- Authentication
  - Get token for strong authentication protocols
    - E.g. SAML, Oauth, OpenID
- Confirmation
  - Better than 2-factor authentication

Call for interest

- BOFs in Atlanta?
  - Protocol Compiler
  - Omnibroker
- Code is on GitHub
  - Repositories are Godel, ProtoGen, Omnibroker
  - MIT Licensed