VeriSign DNS Initiatives

Matt Larson
mlarson@verisign.com
Principal Engineer/DNS Architect

Registrar Constituency Meeting
ICANN/Rome
March 2, 2004

VeriSign DNS Initiatives

- Real-time update of zone data
- DNS Security Extensions (DNSSEC)
- IPv6 support

ATLAS

- Advanced Transaction Lookup and Signaling System
- Authoritative name server developed by VeriSign
  - Very high performance
  - Economic scaling
  - Real-time updates to geographically distributed sites
  - (Really a distributed directory with multi-protocol support)
- The only name server that can handle the demands of *.com* and *.net*
- ATLAS deployed starting in November 2002

Real-time Updates

- *.com/.net* zones historically updated twice per day
- ATLAS supports real-time updates
  - Less than one minute from RRP to DNS at all 13 *.com/.net* name server locations
- Real-time updates in “shadow mode” testing now
- Deployment expected in Q4 2004

DNS Security Extensions (DNSSEC)

- DNSSEC uses public key cryptography and digital signatures to provide:
  - Data origin authentication
    - E.g., "Did this DNS response really come from *a.gtld-servers.net?*"
  - Data integrity
    - E.g., "Did an attacker—a man-in-the-middle—modify this DNS response?"
- Bottom line: DNSSEC offers protection against spoofing of DNS data

VeriSign®

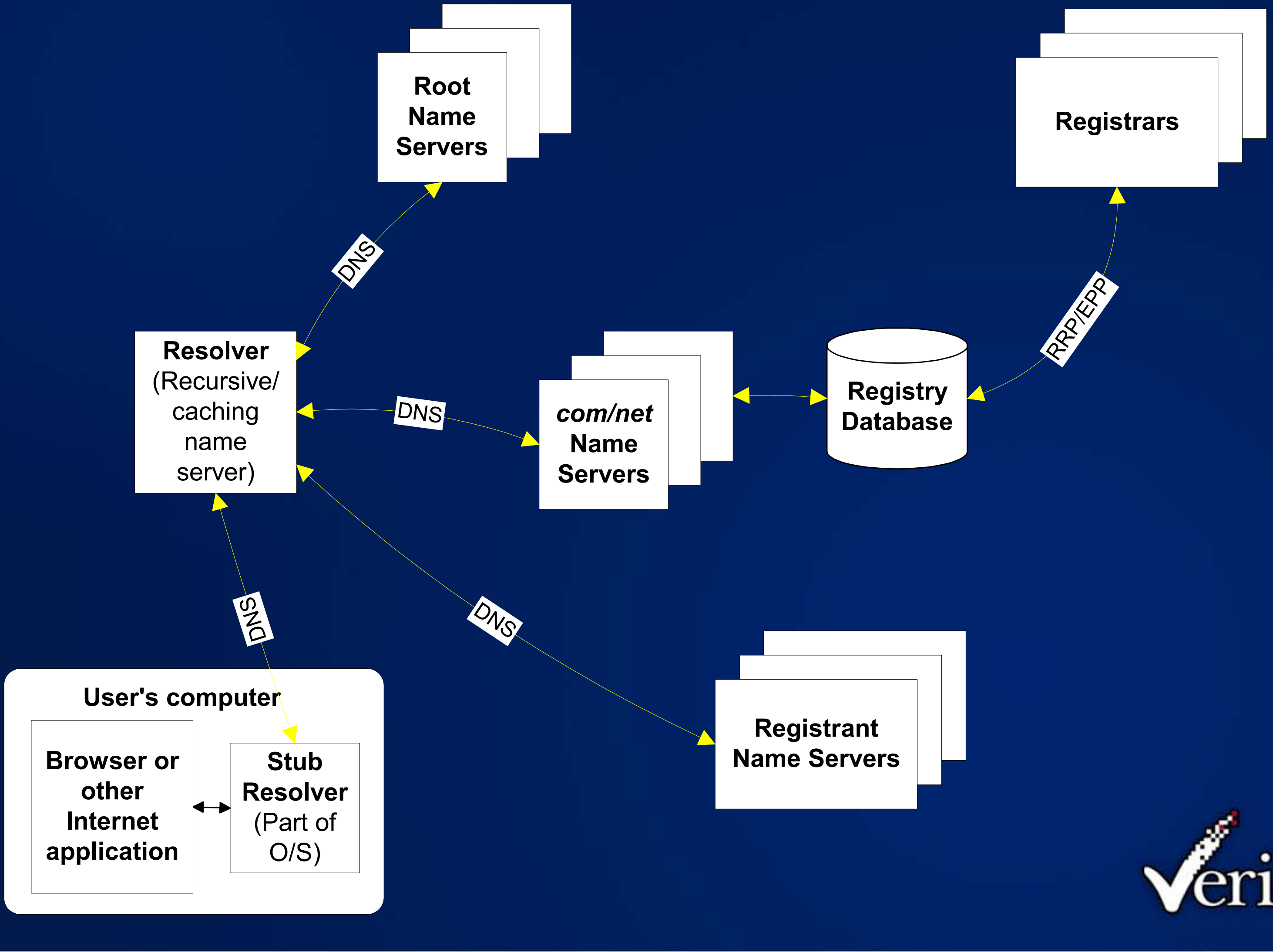
What DNSSEC Does Not Do

- **DNSSEC does not:**
  - **Provide any confidentiality for DNS data**
    - I.e., no encryption
    - Assumption: The data in DNS is public
  - **Address attacks against the name server itself**
    - Denial of service
    - Implementation vulnerabilities
    - Etc.

DNSSEC for Registrant/Registrar/Registry

- Registrant generates a public/private key pair for a zone
- Registrant signs the zone with the private key
- Registrant sends the zone's public key to the registrar
- Registrar sends registrant's key to the registry
- Registry puts registrant's key in the TLD zone
- Registry signs the TLD zone
- Registry publishes signed TLD zone

Changes for DNSSEC



Please Give Us Your Feedback

- VeriSign is soliciting feedback to gauge the community's awareness of and interest in DNSSEC

- What opinions do you have on DNSSEC in *.com/.net*?
- Are your customers interested in DNSSEC?

VeriSign’s IPv6 Efforts to Date

- “AAAA” record is IPv6 equivalent of IPv4 “A” record
- Support for AAAA registration in *.com/.net* registry since May 2002
  - For registrants with name servers using IPv6 transport
- Only a few registrars support AAAA provisioning at this time
- Very few AAAA records in *.com/.net* so far

Root Server Testbed Network

- Separate network of root servers to test new concepts and technology
- Current test areas:
  - IPv6
  - DNSSEC
  - IDN
- Participants (all are IPv4 root operators):
  - VeriSign Research, ISI, EP.NET, WIDE, Autonomica
- See *www.rs.net* for more information

IPv6 Going Forward

- **Planning on native IPv6 transport for *.com/.net* name servers**
  - I.e., *.com*/*.net* name servers reachable over IPv6
  - Obtaining IPv6 microallocations from ARIN
    - 13 *.com*/*.net* name servers and two root name servers
- **Waiting for IPv6 demand**
- **What do you hear from your customers about IPv6?**

Questions?

- We would appreciate your comments and feedback on these initiatives.
- Please send comments and feedback to Matt Larson, *mlarson@verisign.com.*