VeriSign's DNSSEC Signing Service

Matt Larson, Vice President, DNS Research

ICANN 40 DNSSEC Workshop
16 March 2011

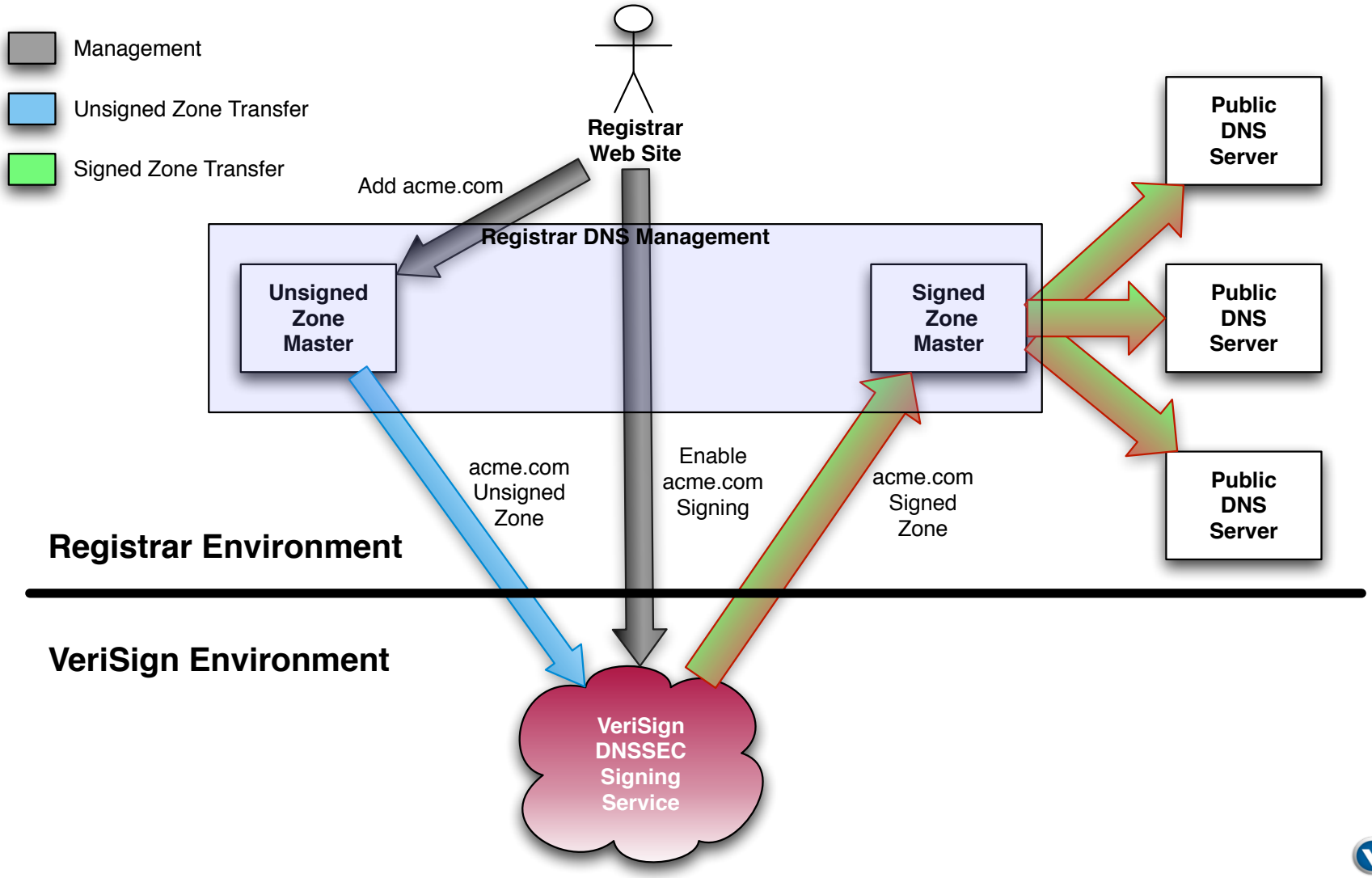
VERISIGN

Verisign's DNSSEC Signing Service

- Converts unsigned zones into signed zones
  - "Bump in the wire" architecture
  - VeriSign signs the zone and the customer hosts it
- Requires no manual effort after setup
  - …and setup takes minutes, not days
- Provides:
  - Entire zone signing
  - Key rollover management
  - Notifications of significant zone-signing events
  - 99.9% uptime
  - Tight SLAs for signing after zone updates
    - Designed for < 10 minutes
    - In production, current stats show 60-90 seconds
  - No sharing of keys between zones

VERISIGN

DNSSEC Signing Service Architecture



DNSSEC Signing Service Details

- Management via SOAP web service or web-based GUI
- Entire zone re-signed with each update
  - All RRSIGs have all same inception and expiration
  - Signature validity of 14 days, refresh at 7 days
- More details:
  - 2048-bit RSA KSK, 1024-bit RSA ZSK
  - ZSK rollover: every 3 months with 1-week pre-/post-publish
  - KSK rollover: every 2 years with 2-month pre-/post-publish
  - RSA/SHA-256
  - NSEC or NSEC3
  - Keys stored in FIPS 140-2 Level 3 HSM

VERISIGN

DNSSEC Signing Service Pricing

- Available to ICANN-accredited registrars
- Free trial period
- $2/domain per year for non-VeriSign TLDs

VERISIGN