DNSSEC Deployment Plan

March 16, 2011

PayPal's DNSSEC Deployment Plan
(Start To Finish, Estimate 4-6 months)

- **Deploy a fully signed test domain**
  - Gain experience pushing DS keys to registrar
  - Gain experience with operations, key rotation, performance, etc.

- **Deploy signed and "validatable" DNSSEC on secondary non-mission-critical domains.**
  - These domains receive significant traffic, but substantially less than PayPal's core transactional domains

- **Deploy a fully signed and "validatable" paypal.com zone**

Deployment Considerations

- **Resolution Failure Rates**

  - PayPal uses a public secondary to serve DNS for paypal.com. During deployment we found issues with edge resolvers

  - AAAA records broke the 512-byte UDP barrier, surfacing problems with some broken clients/networks

  - Concerns that DNSSEC will cause similar breakage on core domains

- **Key Operations**

  - How robust a key management practice should we have? HSM for DNSSEC keys, or basic system controls?

- **Registrar Interaction**

  - Still TBD how/whether to automate DS key pushes