MarkMonitor®

# DNSSEC

**Matt Serlin**
**VP Domain Management**

# Actual Usage By Clients

- Several clients have expressed interest in signing zones
- Very few clients have actually deployed DNSSEC
- Dominated with e-commerce clients
  - Clients that are security aware
  - Clients that see a real security hole in DNS
  - Clients that experienced DNS redirection attacks
- Clients are being cautious about signing zones:
  - Partly due to lack of understanding
  - Partly due to possible increased risk:
    - » If there is a mismatch between the DS record supplied to the registry and the signed records on the zone, it may not resolve.
    - » Must actively maintain keys before they expire (you could set the expiration date out very far, but that would defeat the purpose).
    - » Additional complexity during transfers, either unsign or maintain two sets of keys.
    - » Benefit only available where recursive DNS has DNSSEC enabled.
    - » Clients not concerned or aware of redirected sites.

# MarkMonitor Implementation

- Currently we have less than 200 signed zones (i.e. we have provided DS records to the registry)
- Clients maintain zone signing and key rollover
- We have > 20 tlds that clients can provide DS records directly
- Difficult when registries use non-standard extensions for the addition of DS records
  - E.g .cz uses keysets which is unique
  - Sometimes takes a while for the registry to expose both API and web DS functionality, even after they sign their tld root.