NIST
National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

Cyber and Network Security Program

What to Ask Vendors about DNSSEC

FOSE 2011

July 20th 2011

Presented by Scott Rose, NIST

scottr@nist.gov

DNSSEC

The Basics

- Do your products have FIPS 140 certification?
  - Does it generate keys of the appropriate size and algorithms?
- Can the product be used to automate management of key material?
- Can the product generate both NSEC and NSEC3 signed zones?
- Can I sign/serve/manage multiple zones using this product?
- How quickly can I expect newly specified features/ algorithms to appear?

Not so Basic - Servers

- Does it work in your network infrastructure?
  - i.e. what are you using now?
- How do you update zone data using your product?
- Can you use an HSM for key management with your product?
- What about logging/debugging tools?
  - i.e. Look for potential FISMA needs on config/logging controls.

Not So Basic – Recursive Caches

- How do I configure trust anchors?
- Can I configure more than one?
- Is there a feature to automate trust anchor updates?
  - i.e. using RFC 5011 or some other means
- Any other security features?
  - i.e. blacklisting/whitelisting, port randomization, etc.
- What logging/debugging tools are available?
  - i.e. keep any relevant FISMA controls in mind.