# Secure64 DNS Signer

Overview of Secure64 Grant from DHS

and

Technology Preview of DNSSEC Automation Appliance

June 25, 2008

SECURE 64

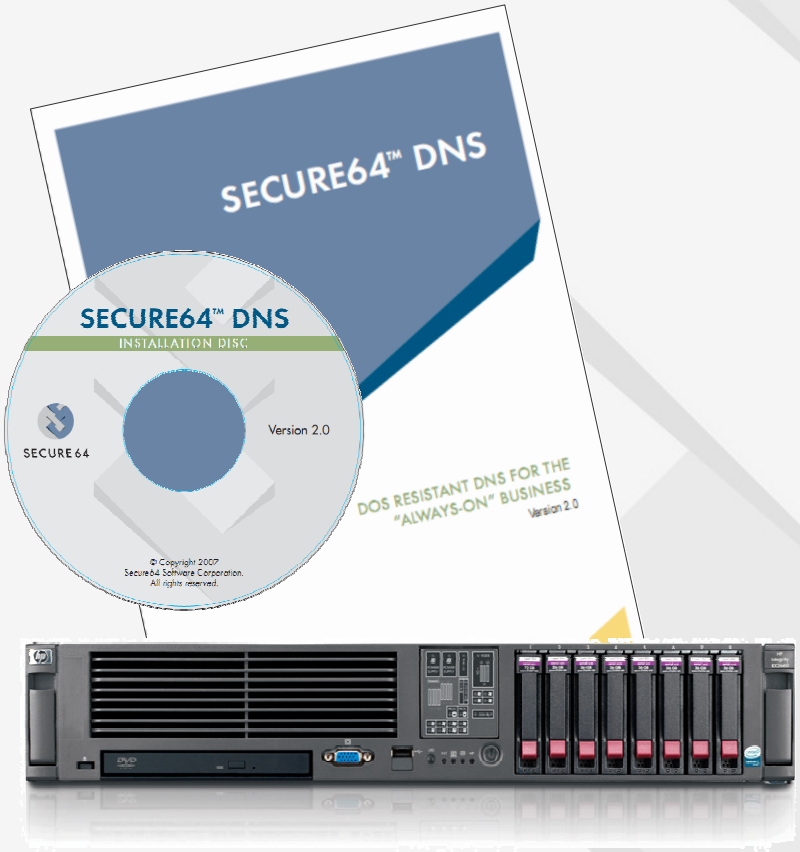
SOFTWARE CORPORATION

# DHS Grant

- Announced on May 14, 2008
- $1.2 grant to develop and commercialize DNSSEC signing solution
- Implementation in two phases
  - Phase 1 – automated signing engine
  - Phase 2 – automated parent-child communications
- Motivation – to accelerate deployment of DNSSEC in US government as well as worldwide

SECURE64

# Secure64 DNS Signer




## *DNSSEC Made Simple and Secure*

### Simple

- Automated key management, rollover, signing

### Secure

- Malware-immune OS
- FIPS 140-2 compliant (pending)

### Auditable

- Key and zone status reports, alerts

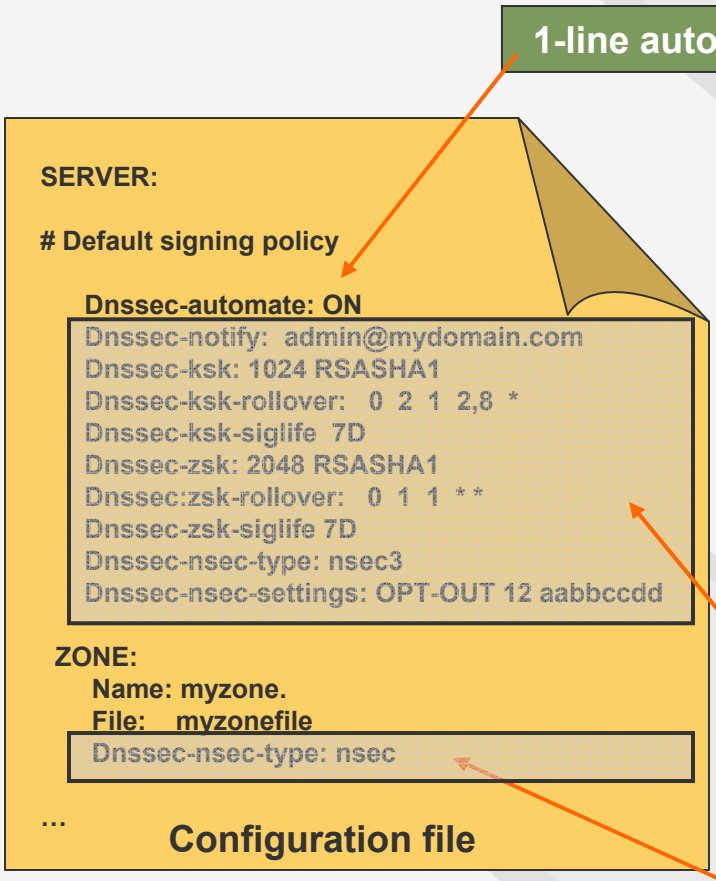
### Scalable

- High performance signing algorithms
- Incremental zone signing

Secure64 DNS Signer makes it easy to deploy DNSSEC correctly and securely

SECURE64

# Simple to Configure



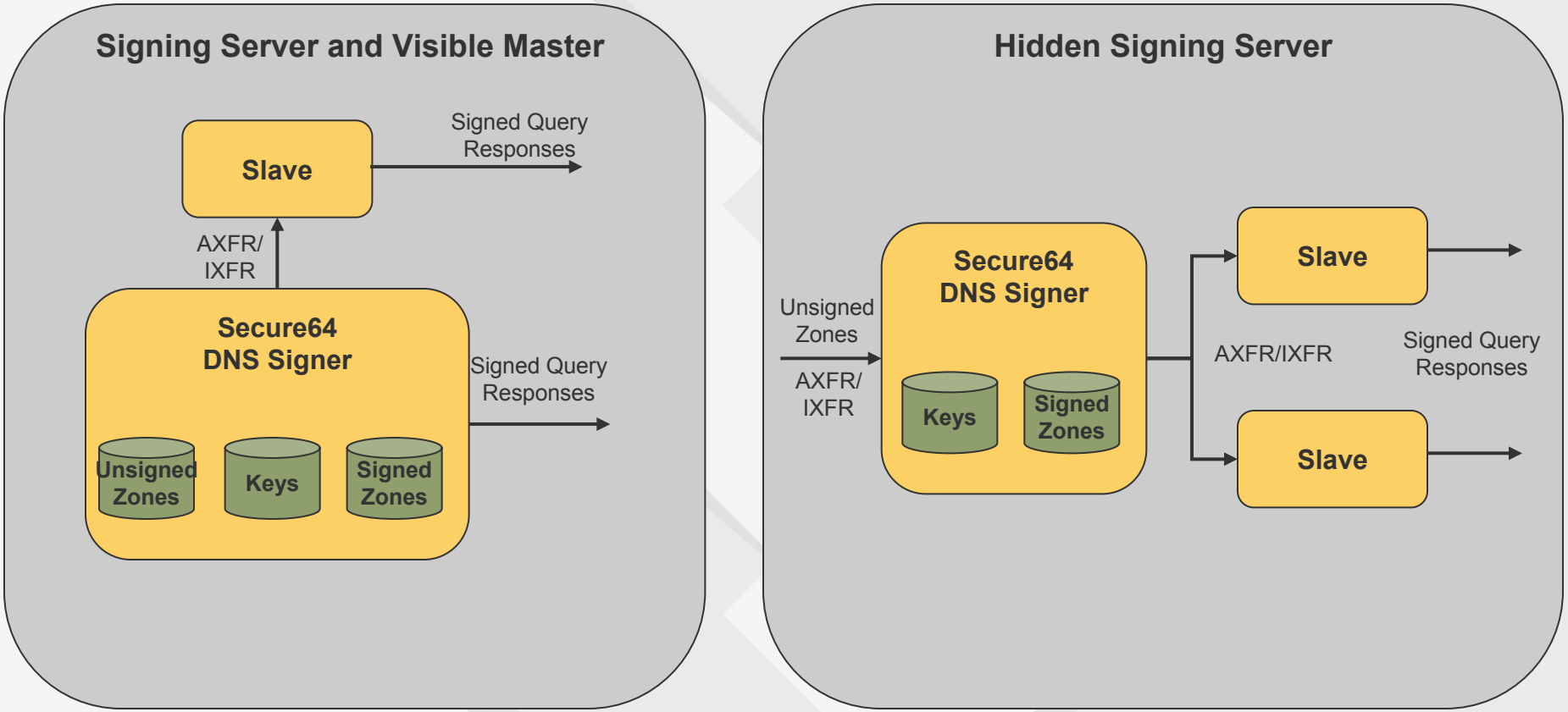

- Simply specify your signing policy or use built-in best-practice defaults
  - Key sizes, algorithms
  - signature lifetime
  - Re-signing time
  - NSEC or NSEC3
  - Notifications
  - Online or offline KSK
  - Parent-child sync (version 2)

**Optional parameters to override defaults**

**Can be applied system-wide or zone by zone**

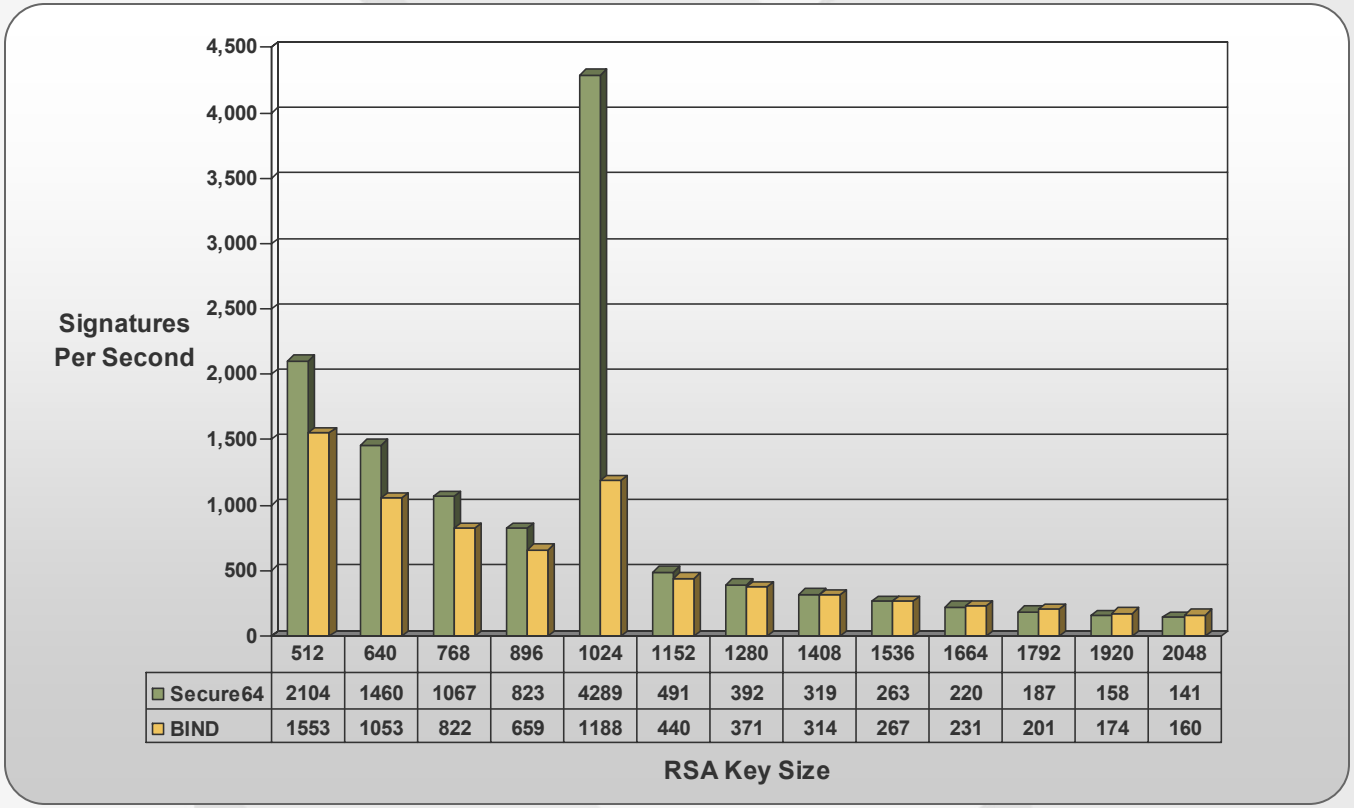
DNSSEC can be deployed in days, not months

# Simple to Deploy




Just plug it into your existing provisioning system

# Fast Signing Performance

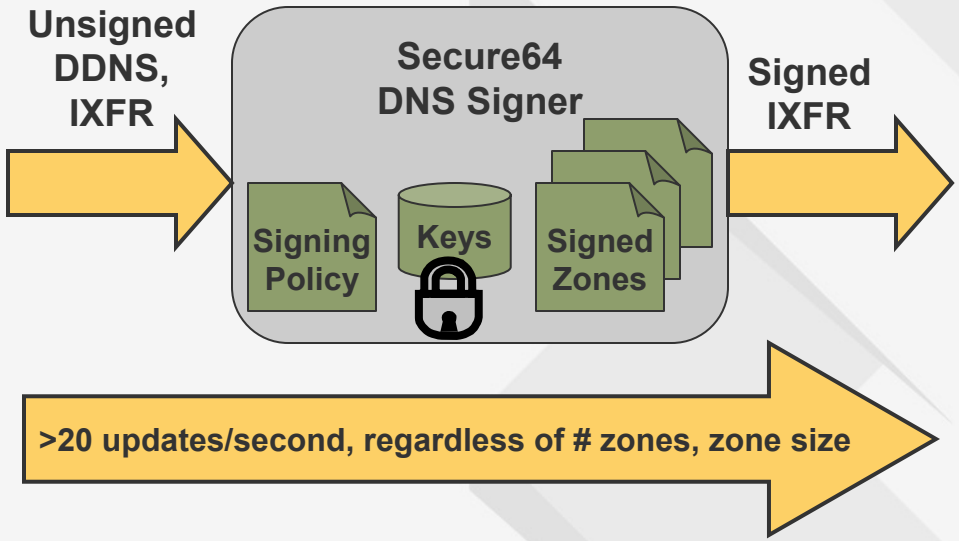



| | 512 | 640 | 768 | 896 | 1024 | 1152 | 1280 | 1408 | 1536 | 1664 | 1792 | 1920 | 2048 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Secure64 | 2104 | 1460 | 1067 | 823 | 4289 | 491 | 392 | 319 | 263 | 220 | 187 | 158 | 141 |
| BIND | 1553 | 1053 | 822 | 659 | 1188 | 440 | 371 | 314 | 267 | 231 | 201 | 174 | 160 |

**Configuration:**
HP Integrity rx2660 server, 1 dual core Itanium 1.4 Ghz processor
4 GB RAM
1 zones, 177,005 records, 344,010 signatures

Optimized code for 1024 bits outperforms many hardware cryptography accelerators

# Incremental Signing




*Challenge*

- How fast can zone changes be signed?
- Can you still meet your target update interval?

*Solution*

- Accept changes via DDNS or IXFR
- Only sign changes
- Update slaves via IXFR

Even the largest, most dynamic environments can be updated quickly

# Secure From Compromise

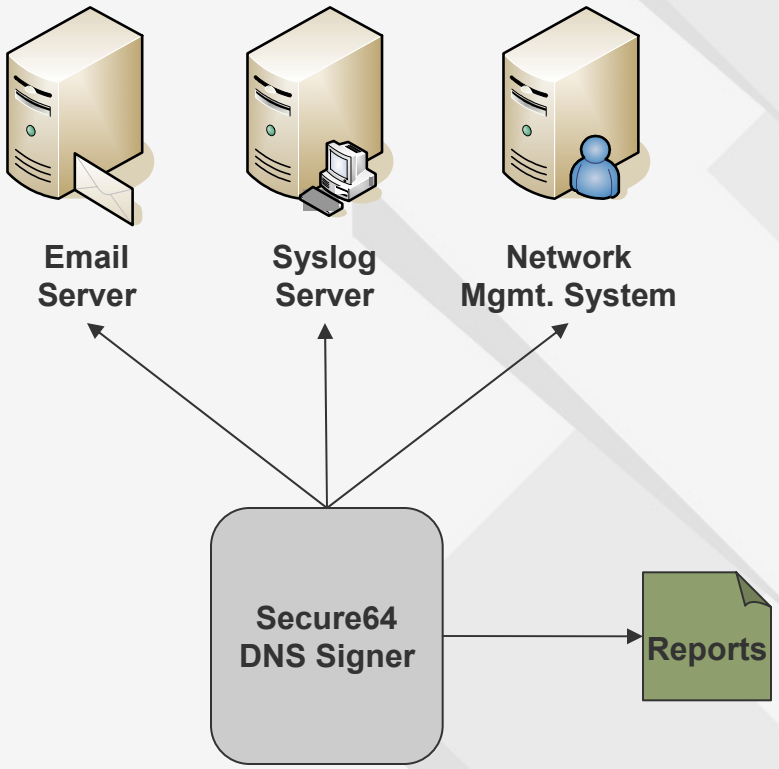

- FIPS 140-2 certification (pending)
  - Certified cryptographic algorithms
  - Role and identity-based authentication

*Plus…*


- Hardware and software chain of trust
  - TPM chip provides root trust
  - Digital signatures of firmware, software checked before executing
- Platform security
  - Immune to malware
- Key security
  - TPM provides root storage key
  - KSKs, ZSKs encrypted on disk
  - Encrypted KSKs, ZSKs stored in hardware-protected memory compartments

Provides levels of security well beyond FIPS requirements

# Easy to Audit




## Event notification

- Normal: zones signed or resigned, key rollover initiated
- Warnings: keys nearing expiration
- Errors: keys expired

## On demand reporting

- Per zone or all signed zones
- Key sizes, algorithms, inception time, expiration time, rollover time

You always know the status of your keys

# Questions?

Joe Gersch, joe.gersch@secure64.com

Mark Beckett, mark.beckett@secure64.com