

# DNSSEC Made Simple and Secure

Internetdagarna  
November 5, 2009



**SECURE64**

SOFTWARE CORPORATION

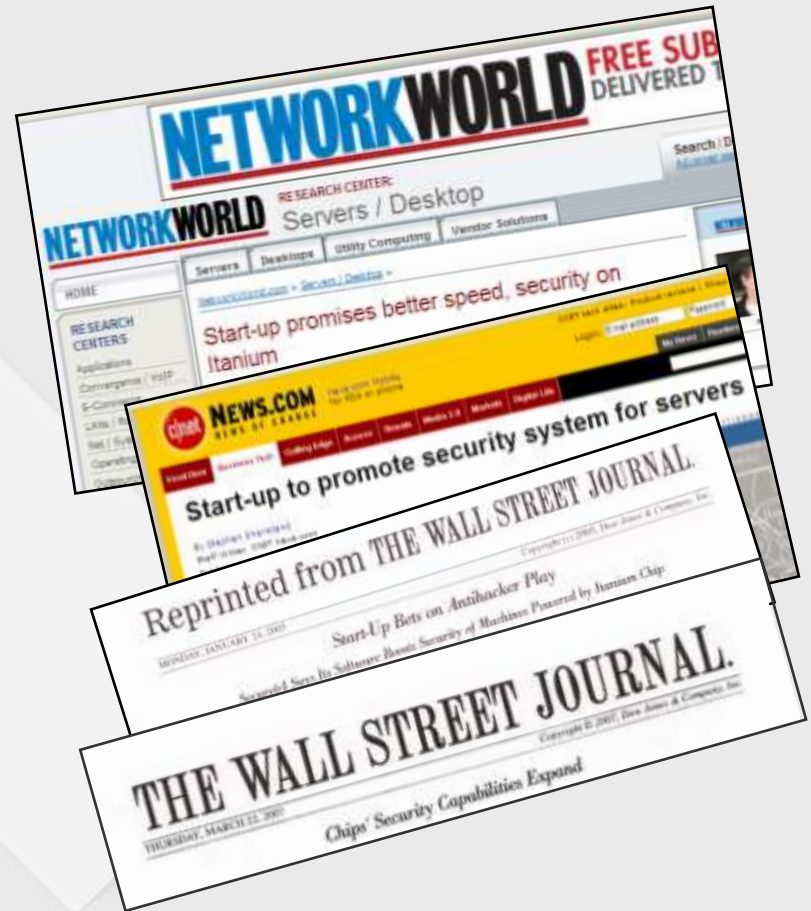
# Secure64 Software Corporation

Privately funded, Colorado-based corporation, founded in 2002

Focused on making the DNS trustworthy and secure

Secure64 products: 'DNS Authority' & 'DNS Signer'

Partially funded by the US Department of Homeland Security



# DNSSEC Deployment Challenges

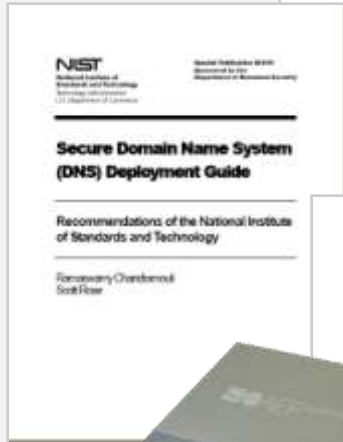
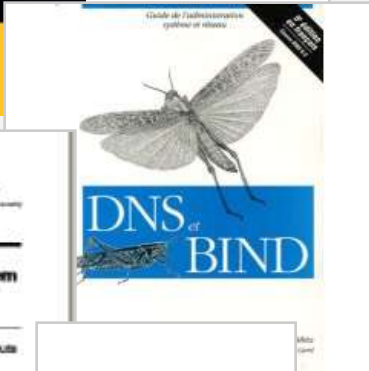
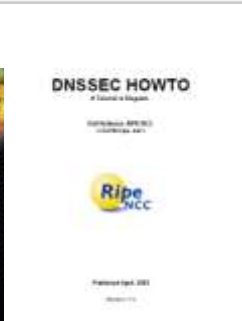
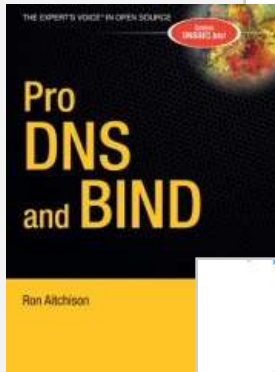
Complexity

Security

Disaster Recovery

Scalability

Auditability



# Secure64 DNS Signer



***Funded by  
DHS Grant***



## ***DNSSEC Made Simple and Secure***

- Automated key management, rollover, signing, re-signing

## **Secure**

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

## **Built-in failover**

- Backup/restore from failover server

## **Scalable**

- High performance signing algorithms
- Incremental zone signing

## **Auditable**

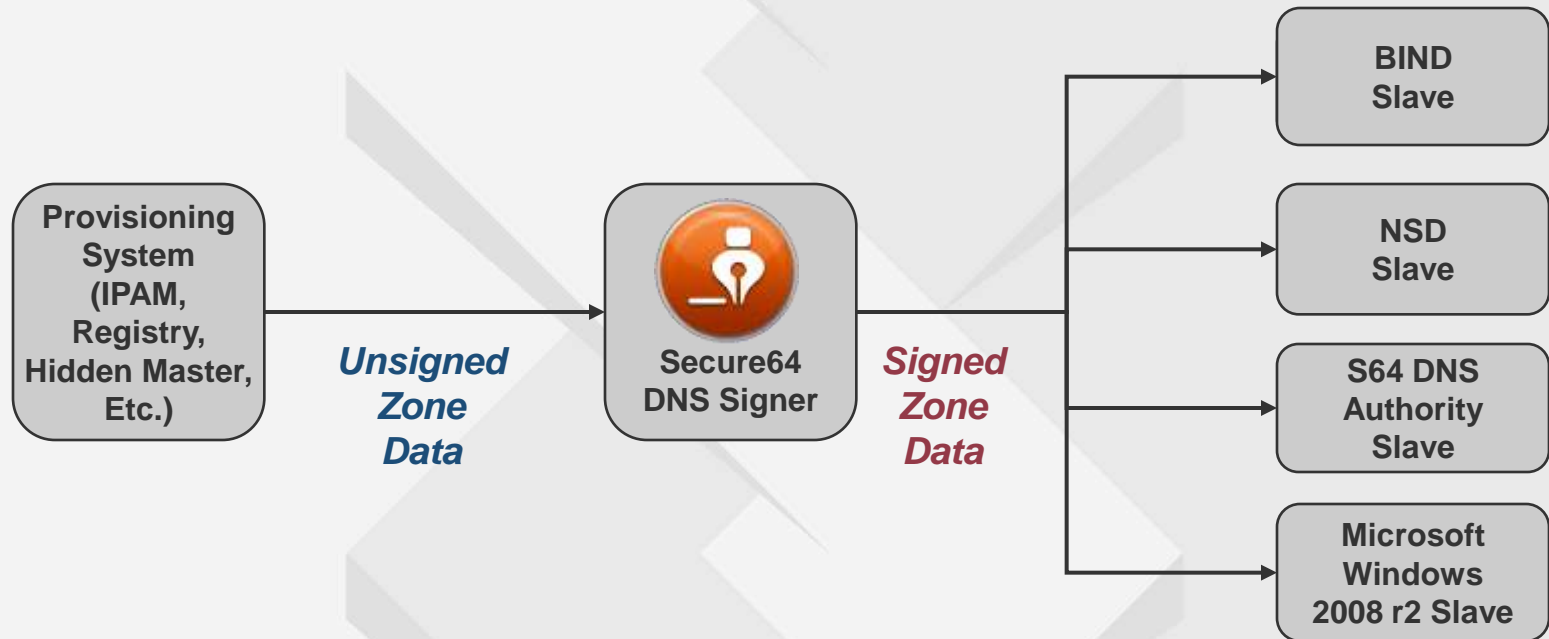
- Key and zone status reports, alerts

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



SECURE64

# Compatible With Current Infrastructure



Just plug it into your existing DNS infrastructure

# Simple to Configure

```
SERVER:

# Default signing policy

Dnssec-automate: ON
Dnssec-ksk: 1024 RSASHA1
Dnssec-ksk-rollover: 0 2 1 2,8 *
Dnssec-ksk-siglife: 7D
Dnssec-zsk: 2048 RSASHA1
Dnssec-zsk-rollover: 0 1 1 * *
Dnssec-zsk-siglife: 7D
Dnssec-nsec-type: nsec3
Dnssec-nsec-settings: OPT-OUT 12 aabbccdd

ZONE:
  Name: myzone.
  File: myzonefile
  Dnssec-nsec-type: nsec

...

Configuration file
```

1-line automation

Optional parameters  
to override defaults

Can be applied system-wide  
or zone by zone



DNSSEC can be deployed in days, not months

# Secure From Compromise

Protects the keys ↓	Component	Security Measure	Other Signing Products	Secure64 DNS Signer*
	Crypto Module	FIPS Certification	None or Level 1 (ask)	Level 2
	Application	Digital Signature Validation		✓
	Operating System	Digital Signature Validation		✓
	Hardware	Trusted Boot from TPM		✓

Protects the data {

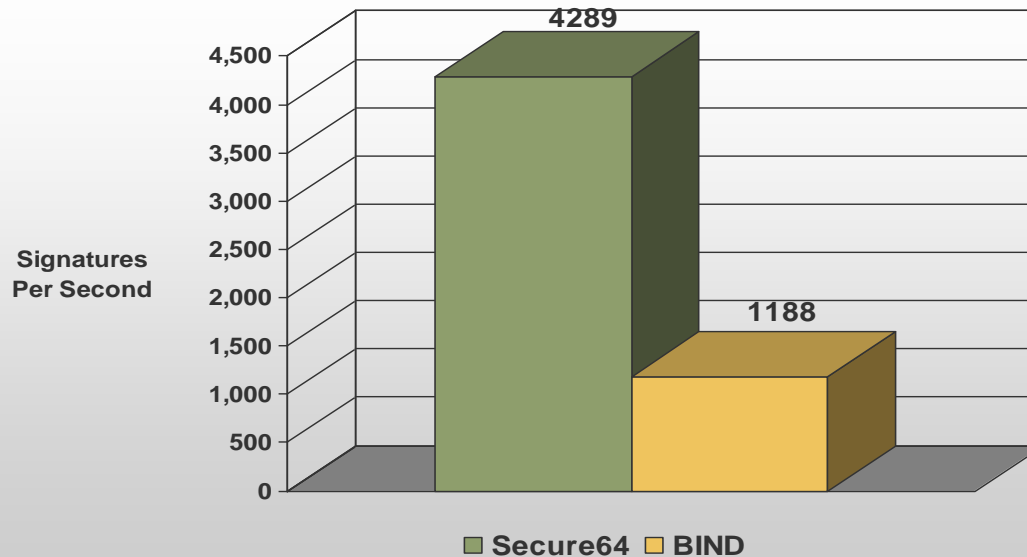
\* Certification currently "In Coordination" status at NIST



Protect both signing keys and DNS data from compromise



# Fast Signing Performance



## Configuration:

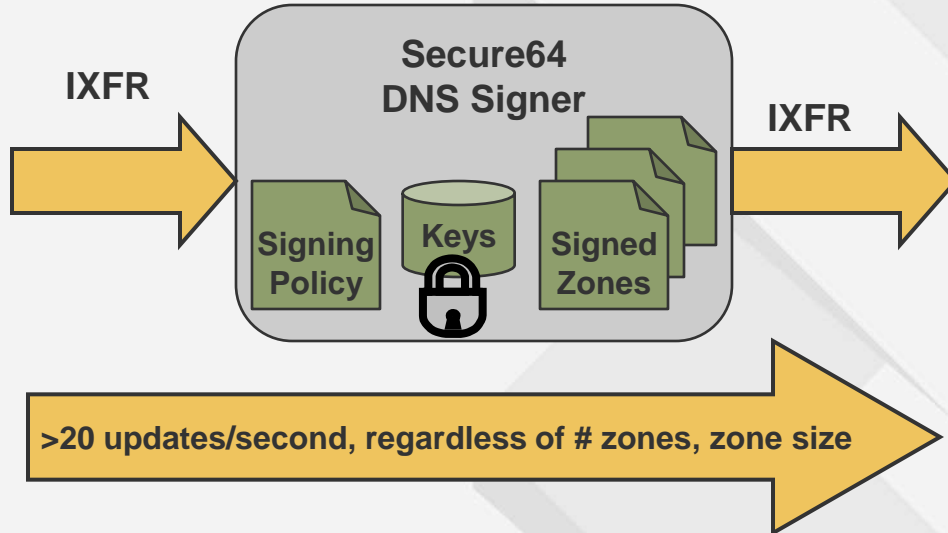
HP Integrity rx2660 server, 1 dual core Itanium 1.4 Ghz processor, 4 GB RAM  
1 zones, 177,005 records, 344,010 signatures, 1024 bit RSA SHA1 algorithm

Optimized code for 1024 bits outperforms many hardware cryptography accelerators





# Incremental Signing



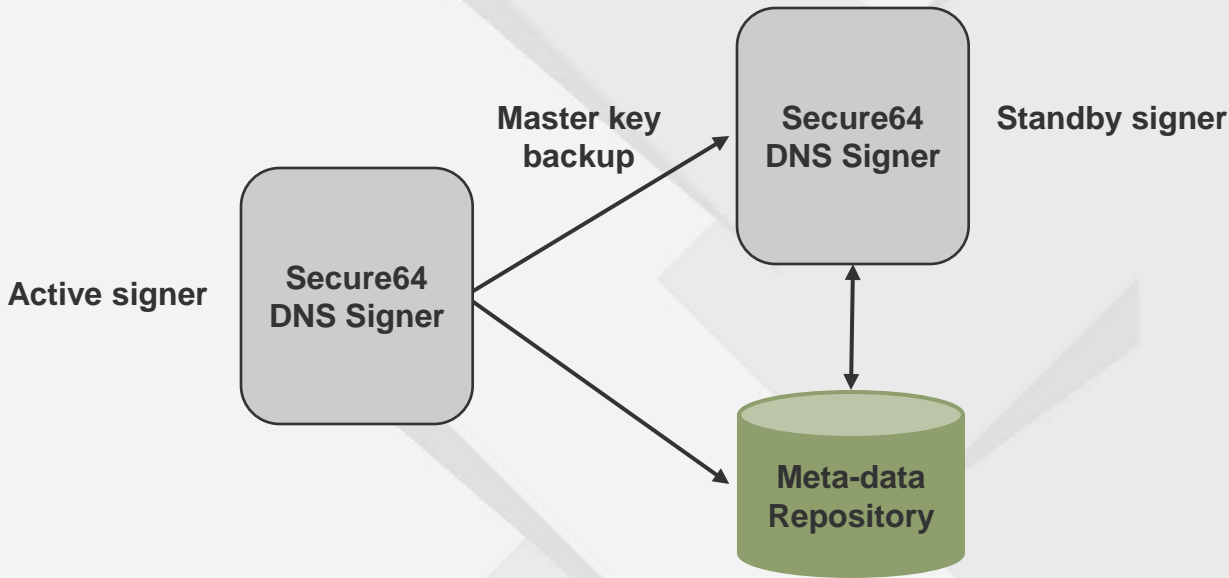
## Easily Handles...

- Dynamic updates
- Hundreds of thousands of zones
- Millions of records

Even the largest, most dynamic environments can be updated quickly



# Secure Key Backup and Restore



## Meta-data Repository

- Encrypted with master key
- Automatically updated after every re-signing event
- Contains KSKs, ZSKs, system state
- Stored on any networked device

## Master key

- Backed up to another trusted platform
- Communication is encrypted
- Restores meta-data repository to any other trusted platform

Failover architecture ensures signing continuity



# Why Secure64 DNS Signer?

## For management

- Faster implementation
- Reduced operating cost
- Reduced risk

## For staff

- Simple. No long learning curve or DNS disruption
- Timely. Deploy in days, not months
- Correct. Eliminates errors that can take you offline
- Secure. Protects the signing keys and the data

## For users

- Internet is safer to access



versus



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



# Recent Success Stories



## Dept of Interior

- Signing for all 9 Interior agencies



## ES.net

- Network backbone operator for Dept of Energy



## Dept of Commerce

- Selected to sign doc.gov



## .org

- Signing .org domain
- 15 million records
- Updates 1/minute



## Dept of Labor

- Signing for all agencies



## Qwest

- Essential part of secure DNS infrastructure



## .uk

- Part of signing infrastructure at .uk

# Thank You!

**For more information, contact:**

Mark Beckett  
VP Marketing  
Secure64 Software Corporation  
[Mark.beckett@secure64.com](mailto:Mark.beckett@secure64.com)  
+1 (303) 242-5899

Or visit our booth at Internetdagarna



SECURE64