SECURE64®

Secure64® DNS SIGNER™

DNSSEC made simple and secure

DATA SHEET

The DNS is a fundamental, mission-critical internet service. All website visits, email communications and virtually all IP-based communications begin with a DNS query. Yet despite the fact that the DNS is such an essential service, the basic DNS protocol cannot guarantee the accuracy of its responses; in fact, the DNS can and has been compromised by attackers to provide damaging, counterfeit responses.

Domain Name System Security Extensions (DNSSEC) adds essential trust to the DNS, providing certainty that DNS responses came from an authorized source and have not been altered in transit. This increased level of trust thwarts many of the DNS hijacking attacks used to commit fraud, including pharming, cache poisoning and redirection, and increases consumer confidence in the security of their online transactions.

But DNSSEC adoption has been hampered by its inherent complexity and the high cost of implementing and maintaining a solution to securely and correctly sign DNS zone data.

Secure64 DNS Signer makes implementing DNSSEC simple and secure. DNS Signer fully automates all of the time consuming DNSSEC key management and signing processes. Unlike other commercial or open-source solutions, DNS Signer runs on SourceT, the Secure64 malware-immune, Genuinely Secure micro OS. This allows it to safely keep signing keys online in a FIPS 140-2 level 2 certified software crypto module without requiring expensive and slow Hardware Security Modules.

DNS SIGNER

DNS SIGNER

KEY BENEFITS

- Implements DNSSEC quickly and easily
- Eliminates implementation errors
- Reduces implementation and maintenance costs
- Scales to hundreds of thousands of zones and millions of records
- Minimizes disruption to current DNS infrastructure

KEY FEATURES

- Fully automated key management
- Fast, incremental zone signing
- Active/failover architecture
- FIPS 140-2 level 2 compliant
- DNS Signer in the middle architecture

Simple to Deploy

Fully automated

Secure64 DNS Signer completely automates the processes required to implement DNSSEC, including key generation, key storage, key rollover, zone signing and re-signing. With DNS Signer, implementing DNSSEC zone signing is as simple as adding a single statement to the configuration file, regardless of the number of zones.

On demand key generation

DNS Signer automatically generates keys for each zone, saving time compared to other systems that require manual key generation for each zone to be signed.

Standards-compliant

DNS Signer supports all of the RFCs and best practices required to deploy DNSSEC safely, correctly and completely. This includes support for RSA SHA-1, RSA SHA-256 and RSA SHA-512 signing algorithms, 1024-2048 bit key lengths, and full support for both NSEC and NSEC3.

Simple yet configurable

DNS Signer uses a set of “best practice” signing defaults but also allows the overriding of any of these settings to confirm to an organization’s requirements.

Plug-in architecture

DNS Signer can be easily inserted into an existing DNS infrastructure using a “DNS Signer-in-the-middle” architecture in which it receives unsigned zone transfers from the existing master, signs the zones, and updates the existing slaves.

Secure Solution

Protected data

Because DNS Signer runs on the Secure64 Genuinely Secure micro OS, SourceT, it is immune to malware and resistant to network attacks. These characteristics protect the DNS data from compromise.

Protected keys

Signing keys are kept in a FIPS 140-2 level 2 certified crypto module, protecting the keys from compromise.

Protection from cryptanalysis attack

DNS Signer automatically generates unique keys for each zone. This minimizes the risk of key compromise through cryptographic analysis, since there are fewer data points for an attacker to analyze. It also limits the potential damage from a successful attack since each zone uses its own keys.

Protected zone transfers

DNS Signer supports ACLs and TSIG on zone transfers, ensuring the integrity of transferred data.

Business Continuity

Active/failover architecture

DNS Signer can be deployed in an active/failover architecture to ensure signature and key rollover continuity in the event of a hardware or network failure.

Alerting and reporting

DNS Signer automatically generates notifications for all signing and key management events (including normal, warning and error events), using syslog alerts and/or SNMP traps. In addition, DNS Signer generates on-demand reports identifying all signed zones and the status of keys utilized for signing.

Scalable Performance

Fast signing performance

DNS Signer employs high speed cryptographic algorithms, which provide over 4,000 RSA operations per second with a 1024 bit key.

Pre-generated keys

Key generation can be a time consuming operation that slows down the key rollover process, especially when rolling keys for many zones. DNS Signer can maintain a pool of pre-generated keys that are available for use immediately, refreshing the pool in the background when CPU cycles are available.

IXFR and AXFR support

DNS Signer supports both incremental and full zone transfers both in and out in order to minimize the impact of zone transfers on the network.

Dynamic zone addition/deletion

Zones can be dynamically added or deleted; these changes are quickly propagated to slave servers, meeting even the most stringent Service Level Agreements.

Efficient zone signing

When receiving an incremental zone transfer, DNS Signer regenerates only those signatures affected by the changes and transfers just the changed records to the slaves rather than the entire zone.

DNS SIGNER

PERFORMANCE

- 4,200 signatures/second/core (RSA SHA-1with 1024 bit key)
- Hundreds of thousands of zones
- Millions of records

SECURITY

- Genuinely secure micro OS
- TPM chip for high entropy and root key security
- Encrypted private key storage
- Secure SSH2 CLI
- Role-based access control
- Password, certificate, LDAP or RADIUS authentication
- CLs on notify and zone transfers
- TSIG signed zone transfers

CERTIFICATIONS/COMPLIANCE

- FIPS 140-2 level 2
- IPv6 Ready Phase 2 Gold
- NIST SP 800-53
- NIST SP 800-81

HARDWARE HP Integrity servers

- HP Integrity iLO management processor
- Integrated TPM security chip
- Redundant power supplies, fans, disks available
- Call Secure64 for specific models and configurations

Learn more about Secure64 DNS solutions at **www.secure64.com**

Secure64 Software Corporation

303-242-5890

www.secure64.com