SECURE64®

DATA SHEET

Secure64® DNS SIGNER™

DNSSEC Made Simple and Secure

FEATURES & BENEFITS:

- Fully automated key management
- Fast, incremental zone signing
- Active/failover architecture
- FIPS 140-2 and FIPS 140-3 certified
- Support for Secure64 and third-party DNS servers
- Optional Hardware Security Module (HSM) for increased security

Industry-Leading Security

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.

Despite the improved security, 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.

Running on X86 based Linux, Secure64 Signer provides an open architecture for customers with the ability to provide signing services for non Secure64 Authorative servers.

Secure64 Signer has the ability to connect to an optional Hardware Security Module for enhanced security, FIPS compliance, and secure storage of DNSSEC keys.

SECURE64®

DATA SHEET

Secure64® DNS SIGNER™

DNSSEC Made Simple and Secure

Product Highlights

Simple, Fully Automated Deployment

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 RSASHA1, RSASHA256, RSASHA512, ECDSAP256SHA256, ECDSAP384-SHA384, ED25519 and ED448s, 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.

Protected Keys

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

Protection From Cryptanalysis

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.

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 or redirected.

Fast Signing Performance

DNS Signer employs high speed cryptographic algorithms, which provide over 2,330 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.

SECURE64®

DATA SHEET

Secure64® DNS SIGNER™

DNSSEC Made Simple and Secure

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.

Performance:

RSA-1024: 970 signatures per second
- 2230 verifications per second

RSA-2048: 470 signatures per second
- 1448 verifications per second

ECDSAP256SHA256: 590 signatures per second
- 547 verifications per second

Hundreds of thousands of zones

Millions of records

Security:

Encrypted private key storage
Password, certificate, LDAP or RADIUS authentication

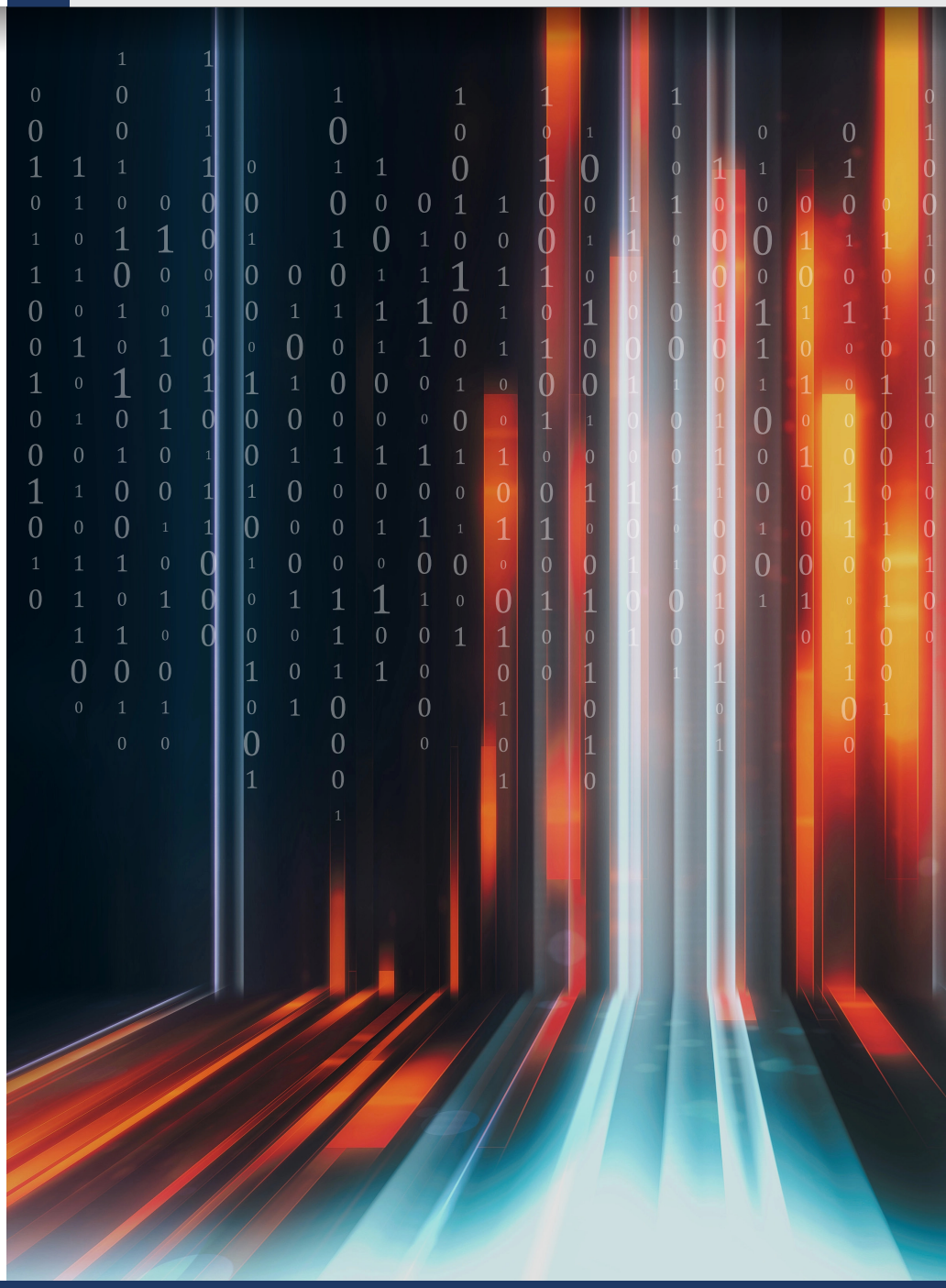
CLs on notify and zone transfers
TSIG signed zone transfers

Certifications/Compliance:

FIPS 140-2 and FIPS 140-3

NIST SP 800-53

NIST SP 800-81



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

SECURE64®

303.242.5890 | www.secure64.com