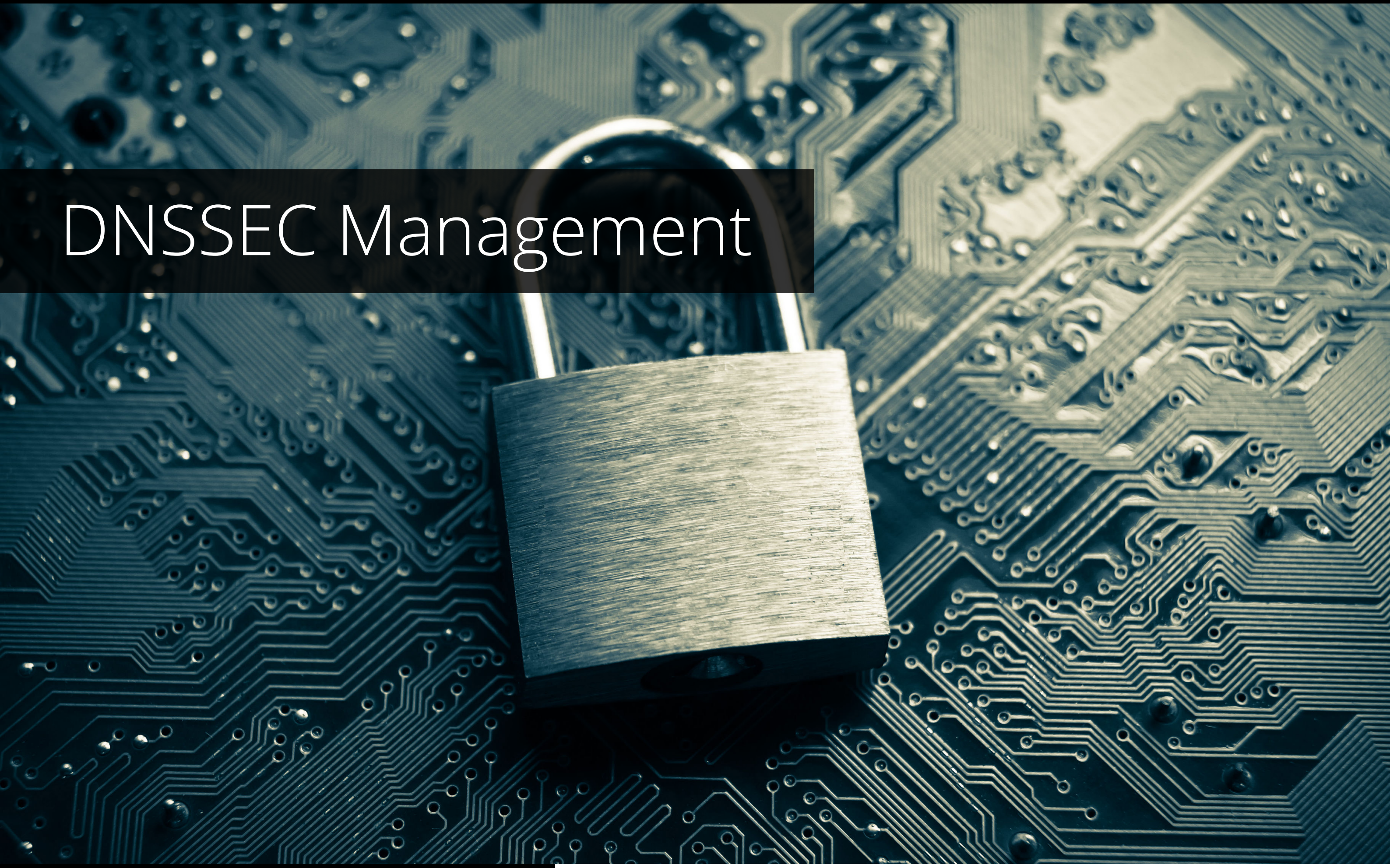
efficient iP®

Datasheet

DNSSEC Management



Highlights:

- Simplified signature of zones
- Automated signing keys (ZSK and KSK) generation, management and roll over
- Guaranteed DNSSEC keys confidentiality with SOLIDserver™ KeyRing
- Automated Management of asymmetric cryptography key, DNSSEC Resource Records, Trust Anchors, and Delegation Signers
- NSEC and NSEC3 supported applying denial of existence
- DLV (DNSSEC Lookaside Validation)

The DNS service is one of the most important Internet and corporate network services, allowing the mapping of domain names to IP addresses. Without DNS, key applications simply do not work: web portals, e-mail, instant messaging, applications and internet protocols all rely on DNS to perform their operations.

Given this importance, DNS is a service which must be secured against all kinds of threats, whether malicious attacks or unintentional misconfigurations.

Over recent years, several vulnerabilities have illustrated the risks around DNS security. Dan Kaminsky demonstrated that the cache of a name server can easily be poisoned, enabling attackers to redirect users to a non-official website. The IP address associated to a domain requested by users can be modified in the DNS cache by a hacker, in order to redirect users to the hacker's website. Then the hacker can steal confidential login and password data before redirecting users to the real website. There are many other examples which illustrate the importance of DNS data integrity, all related to everyday use.

The open source community has released patches and new versions to remediate vulnerabilities and mitigate risks. But the most effective solution to the cache poisoning threat is to implement and deploy DNSSEC.

DNSSEC Principles

An important point to underline is that DNSSEC (DNS Security Extensions) does not modify DNS protocol. DNSSEC is an extension of DNS. Thus, it is possible to use DNSSEC through standard DNS caches. A DNS client which does not use DNSSEC can interact with a DNS server which uses DNSSEC (and vice versa).

DNSSEC is a mechanism enabling the validation and authentication of the origin and integrity of DNS data. DNSSEC mechanisms are based on asymmetric cryptography keys exchanged between the authoritative Name server and DNS client or resolver. All keys generated are contained within the DNS zone with new RR types (resource record). Each signed zone and RR is associated with two cryptography keys, also known as a "key pair":

- **Confidential private key:** This key is used to sign data authenticity and integrity by signing the Resource Records Sets. This key is confidential.
- **Public key:** This key is used to decrypt data that was encrypted with the private key to verify data authenticity and integrity.
- Public and private are linked, but it is not possible to find the other key by knowing only one of them.
- The data signed with a public key proves that it has been signed by the authentic private key.

When a DNS client requests DNS records hosted in a signed DNS zone it receives the requested RR and a digital signature of the RR created by the cryptographic key. The client checks the validity of the signature by requesting the public key of the DNS server hosting the zone which should validate the signature. The validation of the DNS server as a "true source" is then performed thanks to "Trust Anchors".

DNSSEC delivers benefits in two key areas:

- **Origin authentication:** ensures that the DNS answer is delivered by the official DNS server which is supposed to deliver the answer
- **Integrity checking:** ensures that the DNS zone data has not been modified by a third party, as it would require the private key to do so

EfficientIP Solution for DNSSEC

EfficientIP provides a complete solution to easily deploy and maintain DNSSEC. Key management has been simplified to help accelerate rollout of DNSSEC.

SOLIDserver™ is part of EfficientIP's unique 360° security technology to protect against volumetric, exploit and stealth attacks for both public and private DNS infrastructures.

SOLIDserver™ enables you to manage your DNSSEC deployment from a centralized point, with full control over enforcement of your standards through a user-friendly Web interface. SOLIDserver™ eliminates complexity and the risk of errors due to command-line operations, as well as tedious tasks.

Asymmetric Cryptography Key

- RSA/MD5, DSA, RSA/SHA1, RSA/SHA256, RSA/SHA512, DSA/SHA1/NSEC3, RSA/SHA1/NSEC3
- From 512 to 4096 bits for SHA keys and 512 to 1025 for DSA

DNSSEC Resource Records

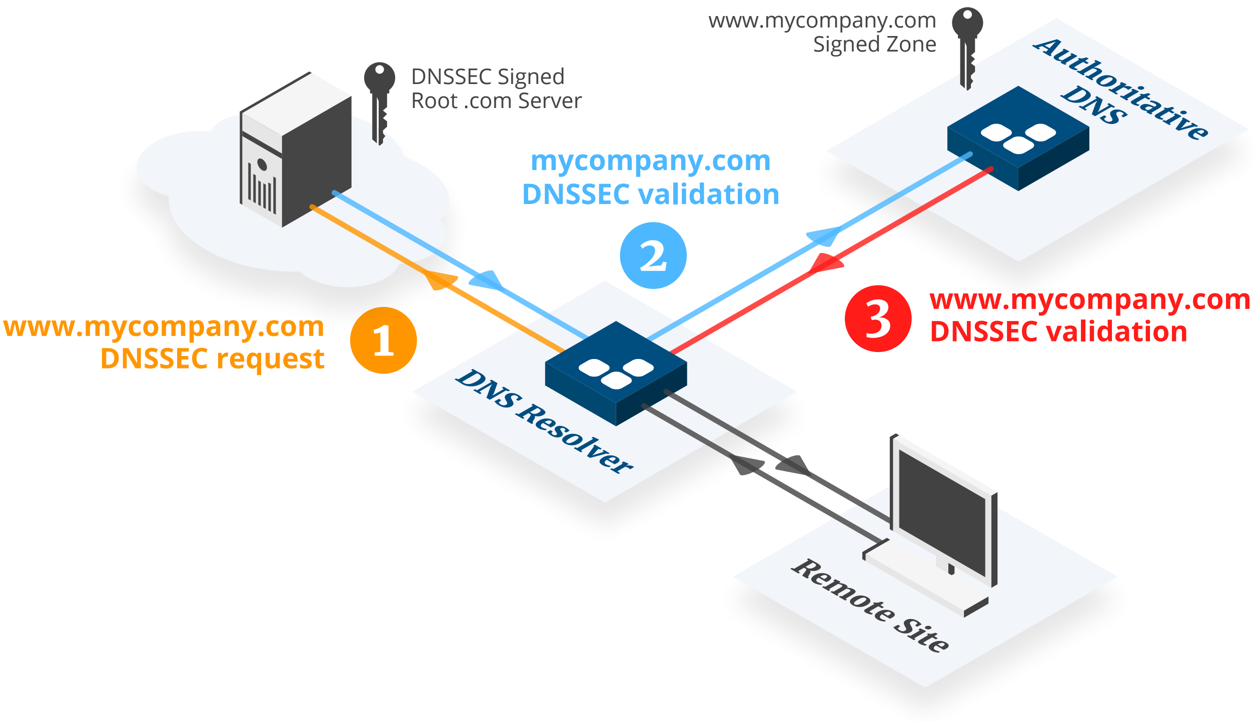
SOLIDserver™ supports all required resource records to deploy and provide DNSSEC including Resource Record Signature (RRSIGs), DNSKEY, Next Secure Records (NSEC) and Next secure 3 Records (N3SEC).

Zone Signing Keys (ZSK) Management

- Automated zone signing and re-signing after modifications of zone data
- Automated ZSK rollover (30 days by default)
- Dual signature for key rollover process management
- Validity period and TTL conformity management
- Private key extraction
- Pre-signed key automation
- Alert on key expiration

Key Signing Keys (KSK) Management

- Overlapped zone signature for key rollover process management
- Validity period and TTL conformity management
- Expiration time threshold alert
- Footprint key export for Trust Anchors and Delegation Signers (DS)
- Trusted key export
- Alert on key expiration



Supports NSEC and NSEC3 applying denial of existence

DLV: DNSSEC Lookaside Validation

Delegation Signers

- Automated DS creation at the SmartArchitecture™ level
- Key importation

Trust Anchors

- Key exportation
- Automated configuration
- Footprint exportation

EfficientIP is fully compliant with RFCs related to DNSSEC

- RFC 4033, DNS Security Introduction and Requirements
- RFC 4034, Resource Records for the DNS Security Extensions
- RFC 4035, DNSSEC Protocol Modifications
- RFC 4641, DNSSEC Operational Practices
- RFC 4956, DNS Security (DNSSEC) Opt-In
- RFC 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence RFC 4033

efficient iP®

REV: C-190103

As one of the world's fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility. Institutions across a variety of industries and government sectors worldwide rely on our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752