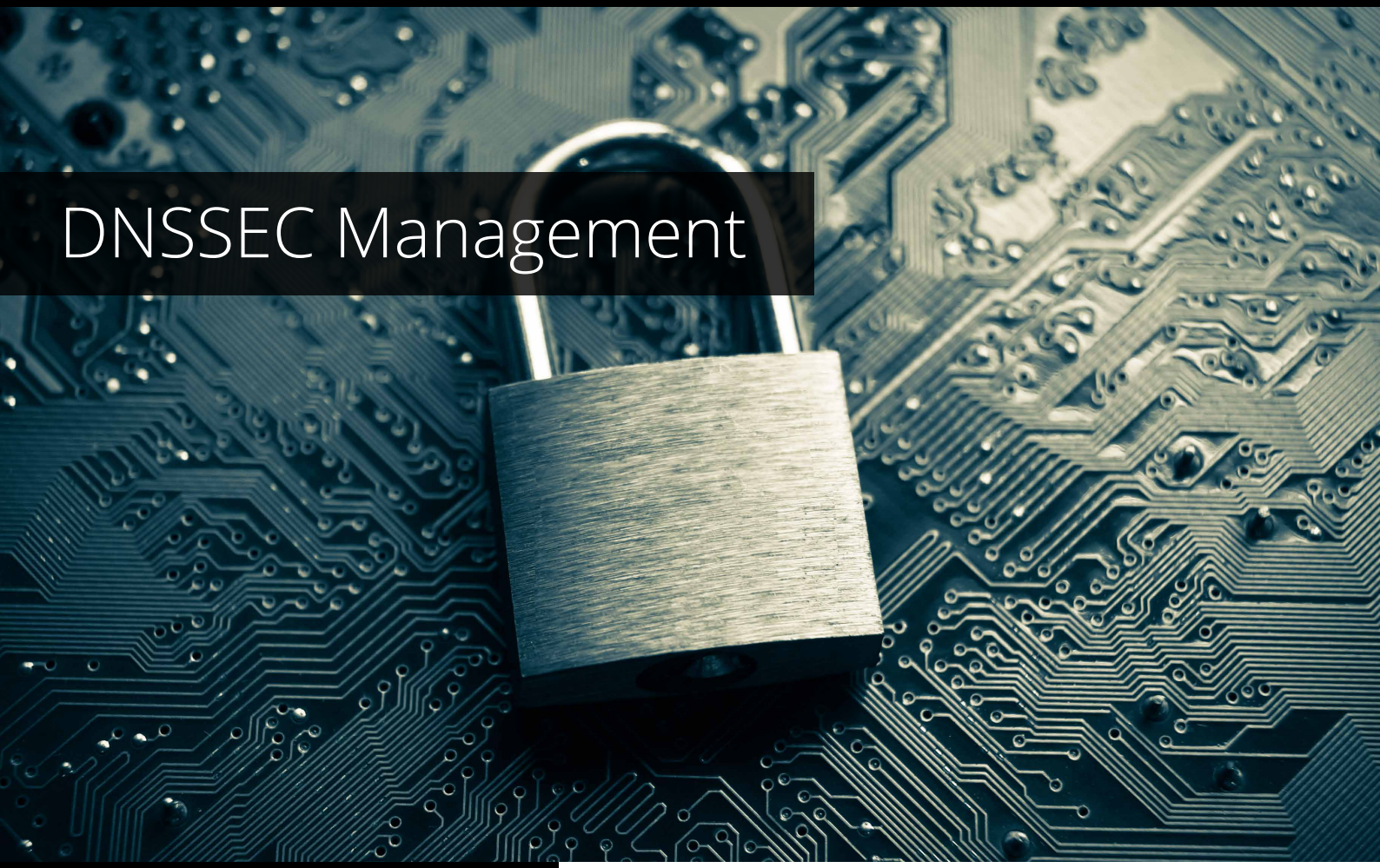
efficient iP™

Datasheet

DNSSEC Management



Highlights

- Vereinfachte Signatur der Zonen
- Automatisches Generieren, Verwaltung und Rollover von Signing Keys (ZSK und KSK)
- Garantierte Vertraulichkeit der DNSSEC Keys mit SOLIDserver™ KeyRing
- Automatische Verwaltung des asymmetrischen kryptografischen Hauptschlüssels und von DNSSEC Resource Records, Trust Anchors und Delegation Signers
- NSEC und NSEC3 unterstützt durch die Anwendung von Denial of Existence
- DLV (DNSSEC Lookaside Validation)

Der DNS-Dienst ist einer der wichtigsten Dienste des Internets und der Netzwerkdienste des Unternehmens und erlaubt die Verknüpfung der Domainnamen mit den IP Adressen. Ohne DNS können Schlüsselapplikationen nicht funktionieren: Webportale, E-Mail, Instant-Messaging, Anwendungen und Internetprotokolle benötigen einen DNS, damit sie funktionieren. Wegen dieser großen Bedeutung ist der DNS ein Dienst, der vor Bedrohungen aller Art geschützt werden muss, egal ob es sich um bösartige Angriffe oder versehentliche Konfigurierungsfehler handelt.

In den vergangenen Jahren haben verschiedene Schwachstellen die Risiken im Bereich der DNS Sicherheit aufgezeigt. Dan Kaminsky hat gezeigt, dass der Cache eines Name Servers leicht vergiftet werden kann und den Angreifern die Möglichkeit gibt, die Benutzer auf eine nicht offizielle Webseite umzuleiten. Die IP Adresse, die einer Domain zugeordnet ist, welche von Nutzern aufgerufen wird, kann im DNS Cache von einem Hacker verändert werden, um die Benutzer so auf die Webseite des Hackers umzuleiten. Dann kann der Hacker die vertraulichen Zugangsdaten und Passwörter abgreifen, bevor er die Nutzer auf die echte Webseite weiterleitet. Es gibt viele weitere Beispiele, die die Bedeutung der Datenintegrität von DNS Servern zeigen und sich alle auf Vorfälle im alltäglichen Gebrauch beziehen.

Die Open Source Community hat Patches und neue Versionen veröffentlicht, um die Schwachstellen zu eliminieren und die Risiken zu senken. Die wirksamste Lösung zum Schutz vor Cache Poisoning Angriffen ist aber die Implementierung und Umsetzung der DNSSEC Sicherheitsmaßnahmen.

Die Vorteile der DNSSEC Sicherheitserweiterungen

Wichtig ist in diesem Zusammenhang, dass die DNSSEC (DNS Security Extensions) das DNS Protokoll nicht verändert, da es sich bei den DNSSEC um Erweiterungen des DNS handelt. Die DNSSEC können deshalb mit Standard DNS Caches verwendet werden. Ein DNS Client, der keine DNSSEC verwendet, kann mit einem DNS Server kommunizieren, der DNSSEC verwendet und umgekehrt.

DNSSEC ist ein Mechanismus, der die Validierung und Authentifizierung des Ursprungs und der Integrität der DNS Daten ermöglicht. Die DNSSEC Sicherheitsmaßnahmen basieren auf asymmetrischen kryptografischen Schlüssen, die zwischen autoritativen Name Servern und dem DNS Client oder Resolver ausgetauscht werden. Alle generierten Keys befinden sich in der DNS Zone mit neuen RR Typen (Resource Record). Jede signierte Zone und jedem RR sind zwei kryptografische Schlüssel zugeordnet, die auch als «Schlüsselpaar» bezeichnet werden:

- **Vertraulicher privater Schlüssel:** Dieser Schlüssel wird verwendet, um die Authentizität und Integrität der Daten durch Signieren der Resource Records Sets zu signieren. Dieser Schlüssel ist vertraulich.
- **Öffentlicher Schlüssel:** Dieser Schlüssel wird verwendet, um die Daten zu entschlüsseln, die mit dem privaten Schlüssel verschlüsselt worden sind, um die Authentizität und Integrität der Daten zu prüfen.
- Der öffentliche und der private Schlüssel sind miteinander verbunden, es ist aber nicht möglich, den anderen Schlüssel zu finden, wenn man nur einen der beiden Schlüssel kennt.
- Das Signieren der Daten mit einem öffentlichen Schlüssel belegt, dass die Daten vom authentischen privaten Schlüssel signiert worden sind.

Wenn ein DNS Client DNS Datensätze anfragt, die in einer signierten DNS Zone gehostet sind, erhält der DNS Client den angefragten RR und eine digitale Signatur des RR, die vom kryptografischen Schlüssel erstellt wird. Der Client prüft daraufhin die Gültigkeit der Signatur, indem er den öffentlichen Schlüssen des DNS Servers anfordert, der die Zone hostet, welche die Signatur validieren soll. Die Validierung vom DNS Server als «True Source» erfolgt dann mithilfe der «Trust Anchors».

DNSSEC bietet in folgenden zwei Schlüsselbereichen Vorteile:

- **Authentifizierung des Ursprungs:** Stellt sicher, dass die DNS Antwort vom offiziellen DNS Server kommt, von dem die Antwort erwartet wird.
- **Prüfung der Integrität:** Stellt sicher, dass die DNS Zonendaten nicht durch einen Dritten verändert worden sind, da dafür der private Schlüssel erforderlich ist.

EfficientIP Lösung für DNSSEC

EfficientIP liefert eine komplette Lösung für eine einfache Implementierung und Pflege der DNSSEC Sicherheitserweiterungen. Das Schlüsselmanagement wurde vereinfacht, um das Rollout der DNSSEC zu beschleunigen.

SOLIDserver™ ist Teil der einzigartigen 360° Sicherheitstechnologie von EfficientIP zum Schutz vor Floods (Volumetric Attacks) und vor Exploit und Stealth Attacks für öffentliche und private DNS Infrastrukturen.

SOLIDserver™ gibt Ihnen die Möglichkeit, Ihren DNSSEC Einsatz von einer zentralen Stelle aus zu verwalten, mit voller Kontrolle über die Durchsetzung Ihrer Regeln über ein benutzerfreundliches Web-Interface. SOLIDserver™ eliminiert die Komplexität und das Fehlerrisiko, das durch Kommandozeilenvorgänge und lästige Aufgaben entsteht.

Asymmetrischer kryptografischer Schlüssel

- RSA/MD5, DSA, RSA/SHA1, RSA/SHA256, RSA/SHA512, DSA/SHA1/NSEC3, RSA/SHA1/NSEC3
- 512 bis 4096 Bits für SHA Keys und 512 bis 1025 für DSA

DNSSEC Resource Records

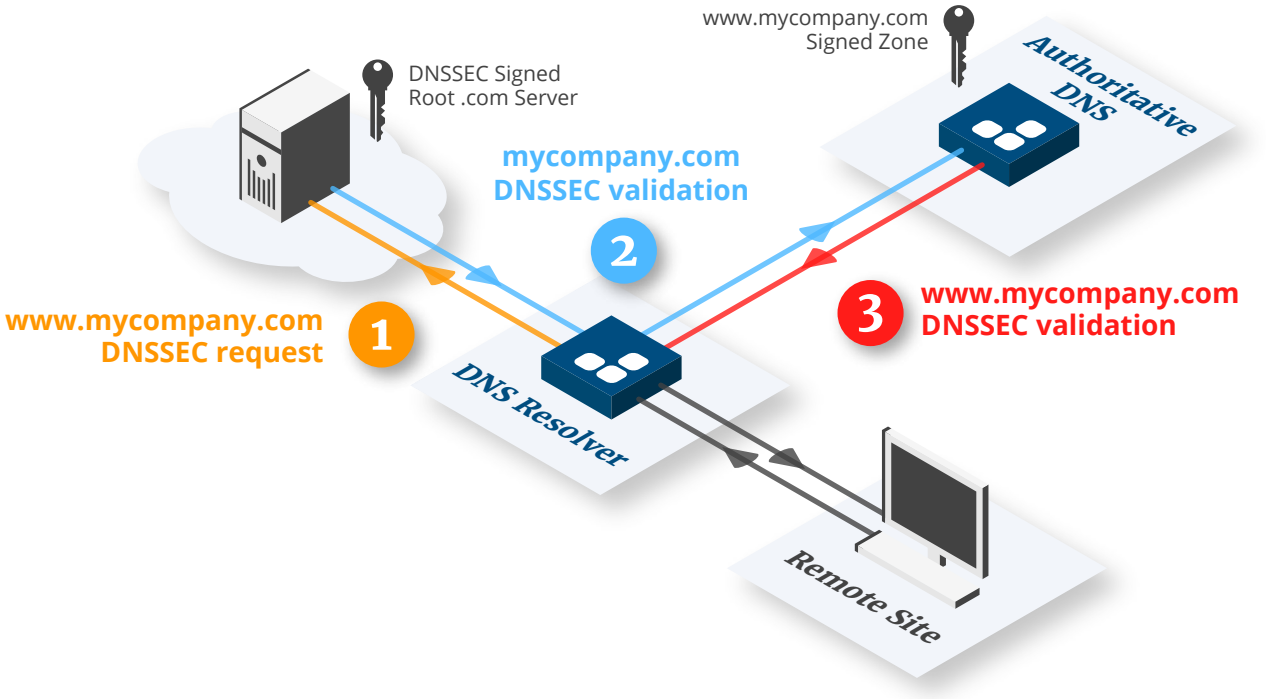
SOLIDserver™ unterstützt alle erforderlichen Resource Records für die Umsetzung und Bereitstellung der DNSSEC, einschließlich Resource Record Signature (RRSIGs), DNSKEY, Next Secure Records (NSEC) und Next Secure 3 Records (N3SEC).

Management der Zone Signing Keys (ZSK)

- Automatisches Signieren der Zone und Neusignieren nach Durchführung von Änderungen an den Zonendaten.
- Automatischer ZSK Rollover (Default = 30 Tage)
- Duale Signatur für das Prozessmanagement vom Key Rollover
- Verwaltung von Gültigkeitszeitraum und TTL Konformität
- Extraktion vom privaten Schlüssel
- Automatisierung mit vorsigniertem Schlüssel
- Warnung bei Ablauf des Schlüssels

Management der Key Signing Keys (KSK)

- Überschneidende Zonen-Signaturen für das Prozessmanagement vom Key Rollover
- Verwaltung von Gültigkeitszeitraum und TTL Konformität
- Alarm bei Erreichen vom Grenzwert der Verfallszeit
- Footprint Key Export für Trust Anchors und Delegation Signers (DS)
- Export vom Trusted Key
- Warnung bei Ablauf des Schlüssels



Unterstützt NSEC und NSEC3 durch die Anwendung von Denial of Existence

DLV: DNSSEC Lookaside Validierung

Delegation Signers

- Automatische DS Erstellung auf dem SmartArchitecture™ Level
- Import vom Key

Trust Anchors

- Export vom Key
- Automatische Konfiguration
- Export vom Footprint

EfficientIP ist vollumfänglich kompatibel mit RFCs in Verbindung mit 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
33 Ubi Avenue 3
08-25 Vertex Building, Singapore 408868
+65 6678 7752