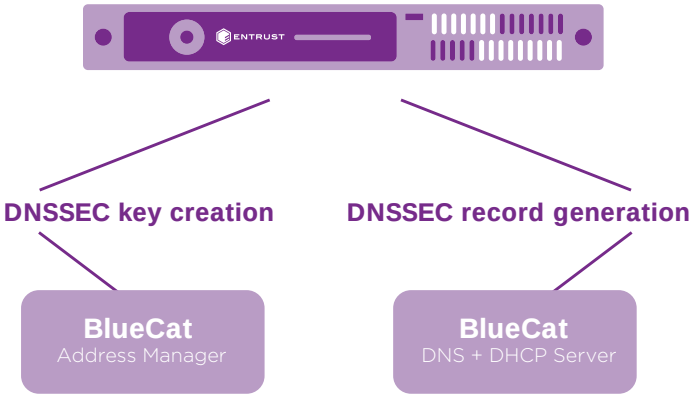
BlueCat and Entrust solution reduces cyber-threats to DNS and simplifies DNSSEC management

- Mitigate threats to e-commerce, cloud security and more with strong DNSSEC cryptography
- Simplify management and administration with BlueCat's single-click signing policies
- Reduce the overall cost of administration, key management and regulatory compliance
- Protect an organization's online identity by securing critical keys in Entrust FIPS 140-2 Level 3-certified hardware security modules (HSMs)

nCipher nShield Connect HSM

Secure key generation and storage



- DNSSEC keys are securely stored on the Entrust nShield HSM
- Compromise of the DNS server does not expose keys
- Minimal change to existing administrative setup for DNSSEC

The inherent vulnerabilities of DNS

The Domain Name System (DNS) is a critical part of the Internet's infrastructure. As the master address book, the DNS enables web sites, email addresses, VoIP services, file transfer services and a range of cloud services to communicate with each other through DNS queries that share domain name information and IP addresses.

Because the DNS was not designed with security in mind, there are inherent security vulnerabilities. Malicious individuals can alter a DNS response to engage in cache poisoning, phishing or web site spoofing, where users or services are routed to a di□erent IP address that is impersonating a legitimate site. As enterprises and governments grow increasingly reliant on the Internet for everything from communications, to commerce, to critical IT services, these vulnerabilities pose a significant threat.

DNSSEC: the new security standard

More domains are deploying DNS security extensions known as DNSSEC to address these threats. DNSSEC uses strong public key cryptography to protect the DNS core network service from attack. Adoption of DNSSEC is growing rapidly, due to continuing attacks against the DNS infrastructure and the trend toward cloud-based services.

DNS is critical to connect users and devices to applications and services in the cloud. Implementing DNSSEC poses two challenges for security conscious organizations: secure key storage and key management. Standard DNS servers are not tamper-proof. Managing DNSSEC keys can be complex, costly and time-consuming, as security teams must manually generate, administer and validate the many DNSSEC keys required by an organization.

Improve security and simplify management of DNSSEC with BlueCat and Entrust

The BlueCat and Entrust solution provides secure key storage and simplified key rollover. Organizations can easily implement and manage DNSSEC to protect the network and sensitive data. Keys are generated and secured via the Entrust nShield® Connect HSM, a high assurance device that is both physically and electronically protected against tampering. BlueCat's IP Address Management, DNS, Dynamic Host Configuration Protocol (DHCP) solutions reduce the complexity of DNSSEC with centralized key management, single-click signing policies, fully automated key rollover and emergency manual key rollover.

The BlueCat and Entrust integrated solution for DNSSEC

The BlueCat and Entrust solution combines the ultra-high security of HSM-based DNSSEC with the simplicity of fully automatic DNSSEC key rollover for all key types, as well as flexible support for a broad range of encryption algorithms. Keys are not exposed if the DNS server is compromised.

How it works:

- The BlueCat IP Address Management (IPAM) solution integrates with nShield HSMs to generate and protect DNSSEC keys
- BlueCat DNS/DHCP servers integrate with nShield HSMs to generate signed DNSSEC records
- There is virtually no change to the existing administrative setup for DNSSEC

Why use HSMs for DNSSEC?

While it's possible to deploy DNSSEC in purely software-based systems, HSMs deliver a significantly higher level of protection. They are the only proven and auditable way to protect valuable private keys. HSMs enable organizations to:

- Secure keys within carefully designed cryptographic boundaries that use robust access control mechanisms with enforced separation of duties to ensure keys are only used by authorized entities
- Ensure availability by using sophisticated key management, storage and redundancy features to guarantee keys are accessible when needed
- Improve performance, as DNS servers experience increasing signature and verification transaction volumes, Entrust HSMs reduce the DNS server CPU load

Entrust nShield HSMs: best-in-class hardware for high assurance key security

Entrust delivers best-in-class hardware security modules (HSMs) that are certified to FIPS 140-2 Level 3 for strong DNSSEC signing key security. The hardened platform,

AB A

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust o□ers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.