ISC - Entrust solution for high integrity DNSSEC verification
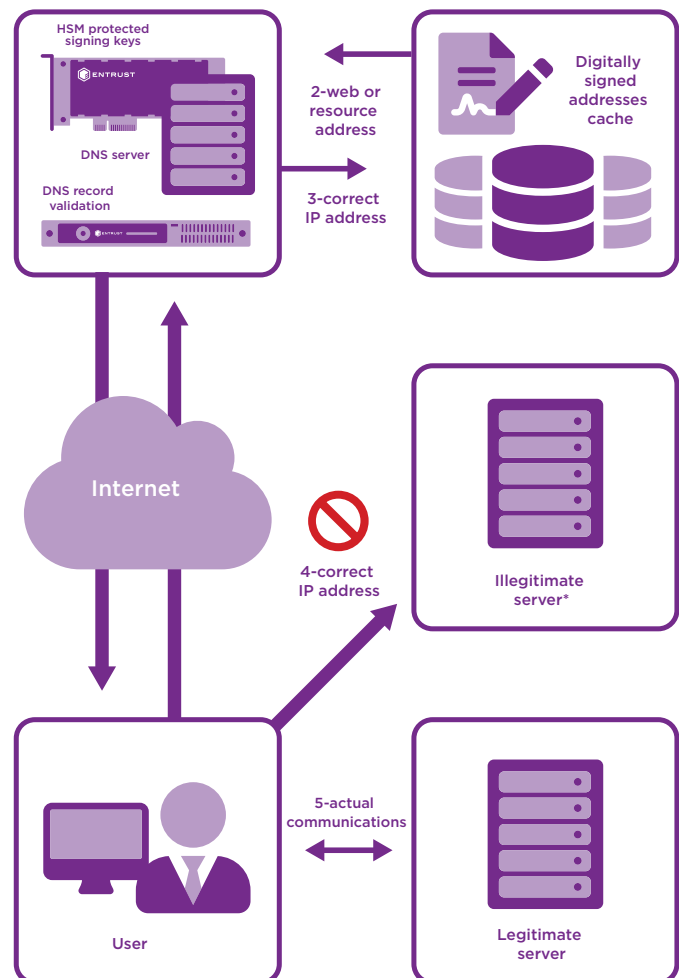
Entrust delivers high assurance signing solution to enhance security for BIND

HIGHLIGHTS

- Mitigate threats to the DNS by implementing ISC BIND support for DNSSEC

- Protect keys in Entrust FIPS 140-2 Level 3 certified HSMs

- Simplify key management operations with unique Entrust Security World architecture

- Reduce overall cost of administration, key management and regulatory compliance

HSM protected signing keys

DNS server

DNS record validation

2-web or resource address

3-correct IP address

Digitally signed addresses cache

Internet

4-correct IP address

Illegitimate server*

5-actual communications

User

Legitimate server

ISC - Entrust solution for high integrity DNSSEC verification

The problem: threats to the DNS

The domain name system (DNS) is a critical part of the infrastructure of the Internet. As a master address book, the DNS enables web site, email, VoIP, file transfer and cloud services to communicate through queries that share domain name information and IP addresses. The DNS however was not designed with security in mind and therefore can be vulnerable and subject to attack. Malicious individuals can alter a DNS query to engage in cache poisoning, phishing or web site spoofing, where users or services are routed to an IP address that is impersonating a legitimate site. As enterprises and governments grow increasingly reliant on the Internet for communications, commerce, and critical IT services, these vulnerabilities pose a significant threat.

The challenge: addressing these threats with DNSSEC

Many domains are deploying DNS security extensions (DNSSEC) to address these threats. DNSSEC is a security standard that uses strong public key cryptography to protect the DNS core network service from attack. While implementing DNSSEC enhances security, it can bring challenges: secure key storage and key management. Standard DNS servers are not tamper-proof and managing DNSSEC keys can be complex, costly and time consuming. Security teams must manually generate, administer and validate the many DNSSEC keys required by an organization.

The solution: simplify key management and improve DNSSEC security with ISC and Entrust

Internet Systems Consortium (ISC) and Entrust have partnered to create an integrated DNSSEC solution for BIND, the open source software most widely used for providing DNS protocols for the Internet. BIND implements the full DNSSEC standard, addressing issues in the DNS protocol. For enhanced security, BIND is integrated with Entrust nShield® hardware security modules (HSMs). These high assurance HSMs prevent physical and electronic tampering, and offer the strongest protection for DNSSEC keys. Entrust HSMs not only generate and protect DNSSEC keys, but also, through the market-leading Security World key management architecture, simplify and automate the complex tasks of managing these keys.

Why use Entrust HSMs with BIND for DNSSEC?

While it is possible to deploy DNSSEC in purely software-based systems, HSMs deliver an enhanced level of protection, providing a proven and auditable way to protect valuable private signing keys. HSMs enable organizations to:

- Secure keys within carefully designed cryptographic boundaries, using robust access controls

- Enforce separation of duties to ensure keys are used only by authorized entities

- Ensure availability by using sophisticated key management, unlimited storage, secure backup and recovery, and built-in redundancy features to guarantee keys are accessible when needed

- Improve performance as DNS servers experience increased transaction volumes

LEARN MORE AT ENTRUST.COM/HSM

ISC - Entrust solution for high integrity DNSSEC verification

An integration guide describing tested configurations and associated procedures to use ISC BIND with Entrust HSMs is available here.

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations.

Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

About ISC

Internet Systems Consortium, Inc. (ISC) is a non-profit 501(c)(3) corporation dedicated to supporting the infrastructure of the universal connected self-organizing Internet. ISC software is open source. ISC's widely-imitated Managed Open Source process ensures software quality while keeping it completely open and available. ISC operates high-reliability global networks of DNS root servers (F-root) and authoritative DNS servers both for non-profit and commercial enterprises. ISC is actively involved in Internet protocol and standards development, particularly in the areas of DNSSEC and IPv6. ISC is supported by donations from generous sponsors, by program membership fees, and by increasing revenues from for-profit subsidiaries.

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

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 offers 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.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com