THALES

www.thales-esecurity.com

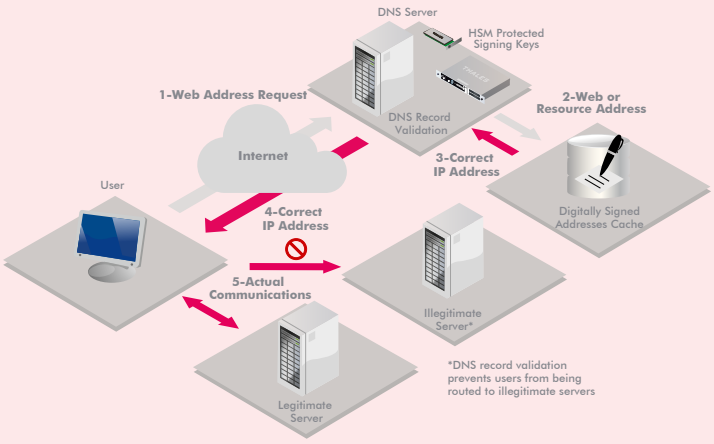
THALES DELIVERS HIGH ASSURANCE SIGNING SOLUTION TO ENHANCE SECURITY FOR BIND

Solution Benefits

- Mitigate threats to the DNS by implementing ISC BIND support for DNSSEC
- Protect keys in Thales FIPS 140-2 Level 3 certified HSMs
- Simplify key management operations with unique Thales Security World architecture
- Reduce overall cost of administration, key management and regulatory compliance

Thales e-Security

ISC – Thales Solution for High Integrity DNSSEC Verification

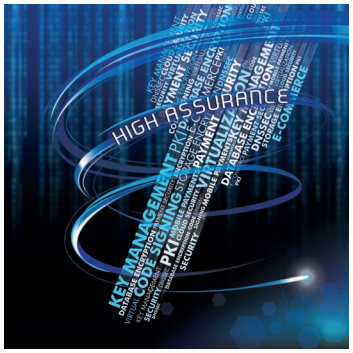


The Problem: Threats to the DNS

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.



ISC - Thales Solution for High Integrity DNSSEC Verification

The Solution: Simplify key management and improve DNSSEC security with ISC and Thales

Internet Systems Consortium (ISC) and Thales e-Security 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 Thales nShield hardware security modules (HSMs). These high assurance HSMs prevent physical and electronic tampering, and offer the strongest protection for DNSSEC keys. Thales 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 Thales 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

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

Thales HSMs: Best-in-class hardware for high assurance key security

Thales HSMs are certified to FIPS 140-2 Level 3 for strong security. The hardened platform, including a model optimized for elliptic curve cryptography, enables organizations to:

- **Safeguard and manage sensitive keys** used for cryptographic operations for a wide range of applications
- **Protect DNSSEC deployments** as well as other critical security systems including public key infrastructures (PKIs), identity management, databases, and code signing
- **Simplify key management** with Thales Security World key management architecture that automates burdensome and risk-prone administrative tasks, guarantees key recovery and eliminates single points of failure and expensive, manually-intensive backup processes

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.

Follow us on:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Unit 4101, 41/F, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com