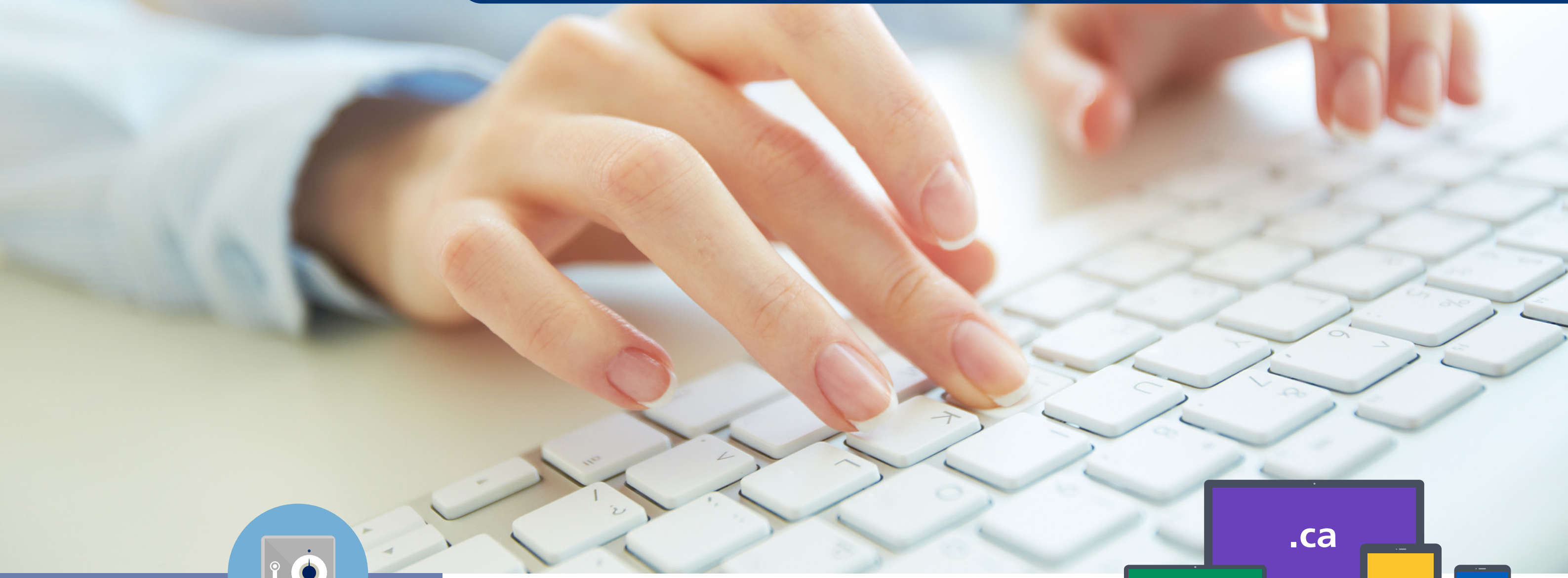
Security & Cyber



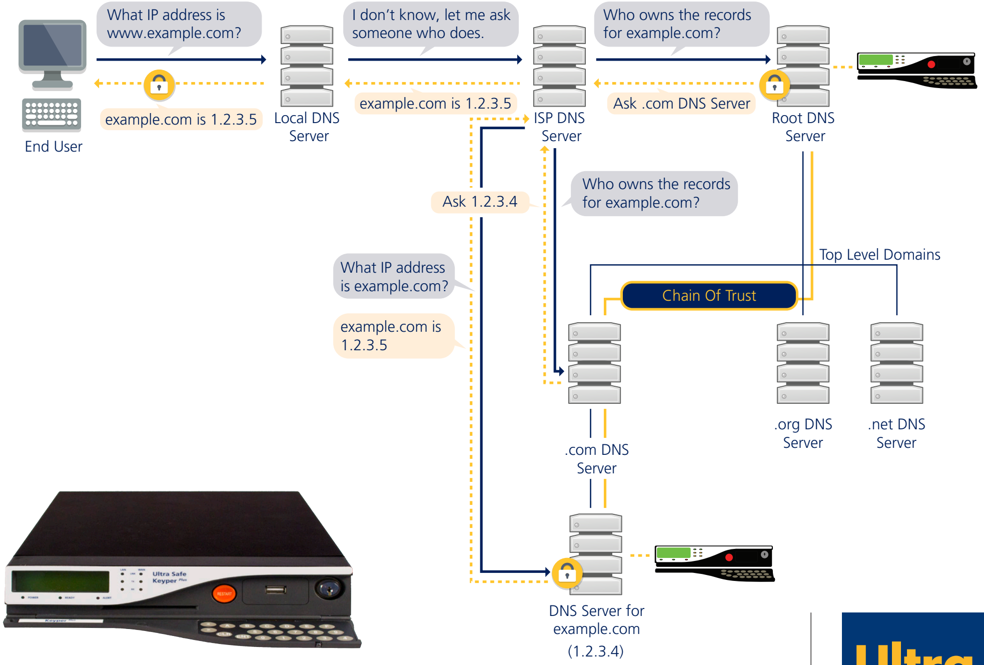
Keyper^{Plus} DNSSEC
Virtual Appliance

Key Features

- Data integrity - DNSSEC is a mechanism to verify DNS data for Top Level Domains, secondary level domains and corporate domains where trusted data security is paramount
- Compatibility - designed to be backwards compatible with the original standard DNS protocol
- Automation - automatic zone signing achievable using new inline-signing feature and automatic key rollover
- Ease of deployment - Hyper-V or VMware virtual appliance eases deployment of OS and DNSSEC into service.
- Assurance - the only standalone HSM with FIPS 140-2
- Capability - broad range of algorithms including elliptic curve
- Architecture - Built using ACCE, giving tamper protection to FIPS 140-2 Level 4
- Fault Tolerance and Scalability - Load balancing of multiple HSMs across multiple hosts and locations
- Authenticated Use of Keys - Optionally PIN activated
- Proven – AEP's Keyper HSMs are deployed in the original DNSSEC implementation for the root DNS domain, hailed by Vint Cerf as heralding a new era in Internet security. AEP's Keyper HSMs are also the foundation of the world's top level domains.

DNSSEC has arisen due to the escalating threat of attacks against the DNS infrastructure. The Keyper^{Plus} HSM from Ultra Electronics AEP can future-proof your DNSSEC deployment, keeping it not just one step ahead of criminals, but beyond their reach. Keyper^{Plus} is the most highly accredited and secure cryptographic hardware security module (HSM) on the market, capable of employing a range of algorithms including the latest Elliptic Curve Cryptography (ECC) Suite B algorithms.

Keyper^{Plus} is the world's only standalone HSM using FIPS 140-2 Level 4 validated technology for the ultimate in cryptographic assurance of signed resource records. Choosing Keyper^{Plus} gives your DNS solution a security pedigree that other HSMs cannot. Keyper^{Plus} positively wipes all Cryptographic keys when tampered, rendering the keys irrecoverable, making Keyper^{Plus} totally tamper-proof, not just tamper-resistant. Favoured by military and governmental organisations, Keyper^{Plus} is the no-compromise HSM for use where the HSM is not simply a passive deterrent but an active protector of keys and all that they secure.



AEP

Ultra ELECTRONICS

Get ahead and stay ahead

To accelerate deployment, the AEP DNSSEC solution comes with a toolkit. It enables out of the box key generation and DNS Zone signing. The toolkit gives organisations what they need to deploy their DNSSEC solution quickly, with optimum flexibility.

A comprehensive solution

The AEP DNSSEC Solution offers true random number generation for the highest quality keys, a hardened platform, key management and resilience Plus elliptic curve cryptography. The toolkit consists of a pre-installed open source software stack provided on DVD. The primary component is the ISC BIND DNS Server software based on a hardened Linux operating system. Like our Keyper^{Plus} the toolkit uses best in class technology. ISC BIND is the gold standard for DNS Servers on the Internet and supports the full DNSSEC standard and automatic key rollover. The toolkit makes a DNSSEC signing server easy to deploy into existing virtualised infrastructure.

The Full Toolkit:

■ ISC BIND DNS Server

■ CentOS (Community Enterprise Operating System) virtual server compatible with existing virtualised environments.

■ OpenSSL

■ Keyper^{Plus} drivers

■ OpenDNSSEC

Applicable markets

- ccTLDs & gTLDs - The highest level of cryptographic assurance for TLD owners
- Domain Registrars and ISPs - requirement for ICANN's 2013 Registrar Accreditation Agreement (RAA) and future customer retention
- Blue chip corporations – retain control of own DNS zones, retain ownership of cryptographic key material

The AEP DNSSEC solution is based on the AEP Keyper^{Plus} HSM, the most tamper-proof and highly accredited HSM on the market. In 2000 AEP led the way with the first fully tamper-proof HSM. AEP's Keyper^{Plus} range has employed FIPS 140-2 Level 4 validated technology for fourteen years and is relied upon the world's preeminent defence in depth strategists.

ICANN

> *"Security is a critical factor for ICANN's DNSSEC deployment, AEP's Keyper HSM & FIPS Level 4 was an easy choice"*
>
> **Richard Lamb, ICANN**

Ordering information

Product	Ordering Part Number
Keyper^{Plus} DNSSEC	KEY-PLS-DNS

Ultra
ELECTRONICS

Ultra Electronics
AEP
Knaves Beech Business Centre
Loudwater
High Wycombe
Buckinghamshire, HP10 9UT
Main Switchboard: +44 (0)1628 642 600
Email: info@ultra-aep.com
www.ultra-aep.com
www.ultra-electronics.com

Made in Britain

ISOQAR REGISTERED UKAS MANAGEMENT SYSTEMS 0026
ISO 27001

FIPS VALIDATED 140-2 TM
FIPS 140-2 Inside

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

Ultra Electronics reserves the right to vary these specifications without notice.