IE Domain Registry Ltd

DNSSEC Practice Statement for the IE ccTLD

Version: 1.0

Date: 29th November 2014

Document Control

Document Information and Security

Conducted by	Responsible for facts	Responsible for document
Security Officer	Security Officer	Security Officer

Security classification	File name
Open	IEDR-DPS-v1.0

Author	Position
Billy Glynn	Security Officer

Approved By

Date	Name	Function
29th October 2014	David Curtin	CEO
29th October 2014	Michael Begley	Technical Services Manager

Audits

Date	Version	Name	Description
29th Oct 2014	v1.0	Billy Glynn	Policy and Practice Statement (DPS)

Contents

1. INTRODUCTION

This document is the DNSSEC Practice Statement (DPS) for the IE zone. It states the practices and provisions that are in use in by IEDR in providing DNSSEC signing for the IE ccTLD zone.

1.1. Overview

The Domain Name System (DNS) Internet Protocol was originally designed with virtually no security in its specifications.

DNS has several distinct classes of vulnerabilities which may be exploited. These DNS vulnerabilities provide a real and present danger to Internet security and have the potential to erode consumer confidence in transacting online or lead to serious financial losses.

Domain Name System Security Extensions (DNSSEC) is a set of Internet Engineering Task Force (IETF) standards that provides data origin authentication and data integrity verification to the DNS, through the use of public key cryptographic signatures. Public key cryptography uses asymmetric key algorithms of mathematically related key pairs in the form of a private key and a published public key. The combination of the key pair enables the verification of the authenticity of a DNS message through the creation of a digital signature of the DNS data, using the secure private key. This signature can in turn be verified by a recipient security aware resolver, using the already published public key from the pair.

This DPS is specifically applicable to all DNSSEC related operations performed by IEDR for the IE zone.

1.2. Document name and identification

Document Title:	DNSSEC Practice Statement for the IE ccTLD
Document Filename:	IEDR-DPS_v1.0.pdf
Document Version:	1.0
Document Last Updated:	2014-10-29
Document URL:	https://www.iedr.ie/dnssec/IEDR-DPS_v1.0.pdf

1.3. Community and applicability

1.3.1. IE ccTLD Registry

The IEDR is the registry for IE Internet Domain Names and maintains the database of IE registered Internet names.

The IEDR is an independent not-for-profit organisation that manages the IE country code Top Level Domain (ccTLD) namespace in the public interest of the Irish and global Internet communities. The IE Domain Registry Limited is not a governing or regulatory body, but provides a public service for the IE namespace on behalf of the Internet community, and is defined as a public company under the Irish Companies Acts.

The IEDR is responsible for generating cryptographic key material, for protecting the confidentiality of the private component of key material and for publishing the public component of relevant key pairs for use as DNSSEC trust anchors.

IEDR is responsible for signing the IE DNS zone file using DNSSEC.

1.3.2. IE Registrars

Accredited IE Registrars are companies, organisations or individuals who have demonstrated the knowledge, experience and the expertise in managing IE domains as agents of registrants.

IE Registrars are responsible for requesting changes in the IE registry on behalf of IE Registrants. IE Registrars are responsible for the secure identification and transmission of IE Registrant DNS and DNSSEC information to the IE Registry such that the IE Registry can apply the requisite changes to its database. In the context of DNSSEC, such information would be of the form of Delegation Signer (DS) resource records for a given domain.

1.3.3. IE Registrants

IE Registrants are any party that has an Internet domain name ending in IE registered. IE Registrants are responsible for generating, protecting and maintaining their own DNSSEC key material. However, they may entrust an IE Registrar to provide such services on their behalf.

IE Registrants are responsible for ensuring that their DNSSEC keys are managed in an appropriate manner and to perform key rollover when the keys are suspected to be compromised or have been lost.

1.3.4. Relying Party

A relying party is the entity that makes use of DNSSEC signatures such as DNSSEC validator's and other DNSSEC enabled applications. The relying party is responsible for maintaining appropriate trust anchors. Relying parties must not use IE DNSKEYs as their secure entry point in to the IE zone. Moreover, relying trust parties must ensure that they use the root zone anchor as their secure entry point in to the DNSSEC chain of trust for IE.

1.4. Specification administration

1.4.1. Specification administration organization

IE Domain Registry Ltd

4th Floor

Harbour Square

Crofton Road

Dun Laoghaire

Co. Dublin

Ireland

Registered No: 315315.

VAT No: IE 6335315V

1.4.2. Contact information

Telephone: + 353 1 2365400 (lines open 9am – 5:30pm)

Email: registrations@iedr.ie

1.4.3. Specification change procedures

IEDR reserves the right to change, amend or revoke this DPS without prior notice. Material changes will be announced on the IEDR website. IEDR will provide reasonable notice of significant changes. Only the most recent version of this DPS is applicable.

2. PUBLICATION AND REPOSITORIES

Information relating to DNSSEC in the IE ccTLD will be published at: https://www.iedr.ie/dnssec/

2.1. Repositories

Information relating to DNSSEC in the IE ccTLD is published at:

https://www.iedr.ie/dnssec/

2.2. Publication of public keys

A cryptographic hash of the public component of the IE KSK will be published in the root zone.

3. OPERATIONAL REQUIREMENTS

3.1. Meaning of domain names

A domain name is a unique identifier in the DNS as described in RFC1024 and RFC1035. An IE domain name is a unique name that is registered in the IE ccTLD and delegated in the IE ccTLD zone.

3.2. Identification and authentication of child zone manager

IEDR as the operator of the IE ccTLD manage the registry database and zone for all IE second level domain (SLDs) names. All SLDs holders contact details and credentials (or their agents) are maintained by IEDR to enable secure electronic communication and processing of change requests.

3.3. Registration of delegation signer (DS) resource records

IEDR accepts DS records for SLDs through secure communication channels. Those DS records are submitted by Registrants or Registrars on behalf of Registrants. DS records are validated against the SLD zone DNSKEY KSK resource record. This validation forms part of IEDR pre-registration pre-modification checks. The acceptance of a DS record for a SLD activates DNSSEC for that domain as of the next IE zone reload.

3.4. Method to prove possession of private key

Registrants are not required to prove possession of private keys.

3.5. Removal of DS resource records

3.5.1. Who can request removal

The removal of a DS resource record can be requested by a registrant or their registrar.

3.5.2. Procedure for removal request

The removal request of a DS resource record is received, validated and processed as per any other name server or glue removal request.

3.5.3. Emergency removal request

There is no provision for a registrant to be able to make an emergency removal request of a DS resource record from the IE zone. All DS record removals must be processed through standard IE Registrar/Registrant channels using standard procedures.

4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

4.1. Physical controls

4.1.1. Site location and construction

IEDR has two operational and geographically dispersed data centres. The two sites serve as a backup to each other. The state-of-the-art operational centre facility provides IEDR with a dedicated, fully redundant environment for its mission critical equipment, providing the highest degree of protection and power. IEDR data centre operator's business processes are ISO 9001:2008 certified and it holds the ISO 27001 Information Security certification.

4.1.2. Physical access

The IEDR's Primary Data Centre facility is a Tier IV class facility which employs industry standard mechanisms to restrict access to the various levels of the facility.

- Biometric access control system
- Motion sensitive CCTV cameras using the latest IP technology
- Business Park 24 x 7 external security
- Full control on private premises
- Data centre 24 x 7 manned security
- Security footage available for customer viewing upon request
- Multiple state-of-the-art security technologies to complement the above.

4.1.3. Power and air conditioning

Every element of the electrical infrastructure is in place to a minimum of N+1 with N+2 being standard in many core areas. Power density is 1kw per sq.m and 1.2kw per sq.m respectively. There are multiple redundant generators that can deliver unlimited power to satisfy each sites requirements. In addition, fully redundant power feeds (A & B) to each client's cabinet(s) with a delivery of 32 individual power outlets per cabinet are totally metered. Each of these feeds is fed direct from totally independent Power Distribution Units (PDU's), Uninterruptible Power Supplies (USP's), Generators and Transformers.

4.1.4. Water exposures

IEDR has taken reasonable precautions to minimize the impact of water exposure to our systems.

4.1.5. Fire prevention and protection

Optical and ionisation sensors are fitted to the ceiling void and to the floor. Very Early Smoke Detection Appliance (VESDA) detects smoke levels over 1ppm, broken down by zone. Fire suppression systems use low-pressure inert gases, which do not harm people or equipment. In addition, exhaust hoses are built into ceilings and floors and have sufficient capacity to fill the room twice.

4.1.6. Media storage

Media containing production software, as well as media containing data, audit, archive and backup information is stored within the main IEDR facility and in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorised personnel.

4.1.7. Waste disposal

All information-carrying media which may contain sensitive information are destroyed in a secure manner, either by IEDR or by a contracted party.

4.1.8. Off-site backup

IEDR regularly and routinely replicate backups of critical data, audit data and other sensitive information to a backup facility. That facility has multiple-tiers of physical access control and is geographically and administratively separate from IEDR's other facilities.

4.2. Procedural controls

4.2.1. Trusted roles

IEDR have four trusted roles in the context of DNSSEC, namely:

1. System Administrator (SA).
2. Security Officer (SO).
3. Auditor (AU).
4. Safe Keeper (SK).

All roles are tightly bound to the IEDR hierarchy. The Security Officer (SO) role is performed by a member of the IEDR management team. The Auditor (AU) role is performed by an employee that is appointed by the IEDR management team. The Safe Keeper (SK) role is the CEO, or someone delegated by the CEO. No one person can occupy more than one role.

4.2.2. Number of persons required per task

DNSSEC related tasks include HSM activation, HSM operations and key operations. IEDR apply the *m* of *n* rule which mandates that a minimum of *m* people from each role are required from the set of *n* persons defined in each role.

4.2.3. Identification and authentication for each role

Only IEDR staff members may be assigned to a role. Role assignees are identified to another trusted person prior to logical access.

4.2.4. Tasks requiring separation of duties

Physical access to the safe and HSM operations requires one person from each trusted role.

4.3. Personnel controls

4.3.1. Qualifications, experience, and clearance requirements

All IEDR personnel participating in the operation of IE DNSSEC systems have a demonstrable proficiency in their assigned role and where necessary have undergone training.

4.3.2. Background check procedures

IEDR routinely validate job references and interview past employers upon recruitment of new employees.

4.3.3. Training requirements

IEDR routinely provides employees with on-the-job training upon recruitment and on an on-going basis. Such training ensures that employees can carry out DNSSEC procedures, processes and administration competently and appropriately.

4.3.4. Job rotation frequency and sequence

All personnel assigned trusted roles will be exercised in their roles by rotation to ensure that all personnel have practical experience of that role.

4.3.5. Sanctions for unauthorized actions

IEDR would immediately suspend the credentials of any person suspected of unauthorised actions beyond their role. That suspension of credentials would be promptly followed by an investigation.

4.3.6. Contracting personnel requirements

All contracted personnel would be subject to the same requirements as IEDR employees.

4.3.7. Documentation supplied to personnel

IEDR DNSSEC operations and practices are documented in Standard Operating Procedures (SOPs). Those procedures are supplied to personnel assigned to a DNSSEC role.

4.4. Audit logging procedures

4.4.1. Types of events recorded

IEDR manually or automatically record events in logs which may include, but are not limited to:

- Safe access.
- HSM events.
- Key management events.
- Physical access to facilities.
- Successful and unsuccessful remote access.

4.4.2. Frequency of processing log

Logging events are continuously monitored and recorded.

4.4.3. Retention period for audit log information

IEDR retain audit log information for as long as necessary to fulfil the audit requirements as set out in section 7 of this document.

4.4.4. Protection of audit log

All audit log data are stored securely to protect against unauthorised access or manipulation.

4.4.5. Audit log backup procedures

All electronic log information is backed up daily. All IEDR log information is stored securely for seven years. All manual logging information is scanned and stored electronically after completion of each auditable DNSSEC task. Physical logs are stored permanently in a fire-proof safe.

4.4.6. Audit collection system

Electronic log information is transferred in real-time to the dedicated log collection system. Manual log information is scanned and stored electronically after completion of each auditable DNSSEC task. The physical logs are stored permanently in a fire-proof safe.

4.4.7. Vulnerability assessments

Every anomaly detected during a DNSSEC task is recorded and requires further analysis and investigation. IEDR continuously monitors and evaluates information sources relating to DNSSEC and DNS vulnerability reports from vendors and community groups, and collaborates with other TLD operators in evaluating the domain name system environment. In addition, all systems are monitored on a 24/7 basis for disruptions and unexpected events.

4.5. Compromise and disaster recovery

4.5.1. Incident and compromise handling procedures

All actual and suspected events that impact on any IEDR services are investigated to ascertain a root cause. IEDR has standard operating procedures for;

- investigation of incidents,
- remedying actions,
- communication and reporting to stakeholders and
- actions to prevent the reoccurrence of such incidents.

4.5.2. Corrupted computing resources, software, and/or data

IEDR's zone generation and signing system implements automatic controls which is designed to ensure that invalid, incomplete or otherwise corrupted data will never be published to the authoritative slave servers. The system is designed to halt operations and to alert the administrators to investigate the anomaly and optionally switch to the fail-over facility.

In any case where corrupted computing resources, software, and/or data causes, or could have caused a disruption of operations which could/would not be recovered from using the normal fail-over procedures, that event will be viewed upon as an incident, and the incident handling procedures will be activated.

4.5.3. Entity private key compromise procedures

If there is suspicion that a key has been compromised IEDR would enact standard operating procedures that include emergency key rollover where a new ZSK or KSK will be generated and the old key will be removed from the key set as soon as its signatures have expired or timed out.

4.5.4. Business continuity and IT disaster recovery capabilities

IEDR maintain an extremely high level of availability, security and resilience, which incorporates several levels of firewall, high-availability network architecture and systems, as well as an always-ready disaster recovery and business continuity plan (tested biannually). Further to this is the strong philosophy of external audit and review by third parties on a regular basis.

4.6. Entity termination

If the Registry must discontinue DNSSEC for the IE zone for any reason and return to an unsigned position, this will take place in an orderly manner in which the general public will be informed. If operations are to be transferred to another party, the Registry will participate in the transition so as to make it as smooth as possible.

5. TECHNICAL SECURITY CONTROLS

5.1. Key pair generation and installation

5.1.1. Key pair generation

Key generation takes place in a hardware security module (HSM) that meets the FIPS 140-2 Level 3 certification. Key generation is planned and carried out by trained and specifically assigned personnel in trusted roles. Key generation takes place when necessary and must be performed by the SO, SA, AU and SK. These people are present during the entire operation. Key generation follows a standard operating procedure which includes logging, part of which is done electronically and part of which is done manually on paper by the AU.

5.1.2. Public key delivery

The public component of the appropriate KSK is exported from the signing system and verified by the SO and SA. The SA is responsible for ensuring that the keys that are published are the same as those that were generated. The hash of the public key is delivered to IANA using the method mandated from time to time. No other publication of public keys will be made.

5.1.3. Public key parameters generation and quality checking

Public key parameters are defined and controlled by IEDR's DNSSEC KASP (Key and Signing Policy). The public key parameters are validated during the automated zone signing and distribution process.

5.1.4. Key usage purposes

The keys used for signing the IE zone will not be used for any other purpose, or outside of the signing system.

5.2. Private key protection and cryptographic module engineering controls

All cryptographic operations are performed in the hardware security module and no private keys are ever found unprotected outside HSM. Private Key material is not exportable from the HSMs.

5.2.1. Cryptographic module standards and controls

IEDR uses hardware security modules (HSM's) validated to the requirements of FIPS 140-2 level 3.

5.2.2. Private key (m-of-n) multi-person control

IEDR has implemented standard operating procedures for the operations performed on private keys. *M of n* control is mandatory for private key operations.

5.2.3. Private key escrow

Private keys are not escrowed.

5.2.4. Private key backup

The IEDR key archive is encrypted and backed up on a clustered HSM. Backups of those HSMs are encrypted and stored in a fire-proof safe.

5.2.5. Private key storage on cryptographic module

Private Key material is stored on a FIPS 140-2 Level 3 HSM. The private component of the key pairs is not exportable from the HSM in an unencrypted manner. A HSM backup may be made to an encrypted token such that a HSM may be restored in the event of a disaster or when a cluster of HSMs is being setup.

5.2.6. Private key archival

Private keys which have reached the expired state will be deleted and are not archived.

5.2.7. Private key transfer into or from a cryptographic module

The private component of the key pairs is not exportable from the HSM in an unencrypted manner. A HSM backup may be made to an encrypted token such that a HSM may be restored in the event of a disaster or when a cluster of HSMs is being setup. IEDR has standard operating procedures for the restoration of a HSM.

5.2.8. Method of activating private key

An IEDR assigned SO may activate a private key. Activation is enabled by providing a valid SO PIN. Once the key is activated, the key is active for a defined time period as specified in the IEDR Key and Signing Policy (KASP).

5.2.9. Method of deactivating private key

HSMs are locked if the IE signing system is either turned off or rebooted.

5.2.10. Method of destroying private key

Keys that have entered the expired state will be automatically removed from the key store at each site.

5.3. Other aspects of key pair management

5.3.1. Public key archival

Public keys are not archived after their operational period has expired.

5.3.2. Key usage periods

When a key has been rolled over and superseded with a new key, it enters its expired state. A key moved into the expired state will never be re-used to sign resource records or for any other purpose.

5.4. Activation data

5.4.1. Activation data generation and installation

The HSM's are activated by the Security Officer, using individual passwords, selected by the SO.

5.4.2. Activation data protection

Security Officers are required to memorise their respective activation data and to not expose or share it with others.

5.4.3. Other aspects of activation data

The security module implements mechanisms to counter password guessing attacks.

5.5. Computer security controls

All critical components of IEDR's systems are placed in the organizations secure facilities in accordance with 4.1. Access to the server's operating systems is limited to individuals that require

this for their work, meaning system administrators. All access is logged and is traceable at the individual level.

5.6. Network security controls

IEDR's production servers are logically separated into security zones using filtering devices. Filters are configured according to the least-privilege principle allowing only the necessary communication paths to flow over the filtering device.

During master key management operations, systems are always disconnected from any communications network.

5.7. Timestamping

All systems synchronises time from a trusted internal source using NTP.

5.8. Life cycle technical controls

5.8.1. System development controls

All source code is stored in a version control system. The source code archive is regularly backed up and copies are stored separately in a fireproof safe.

5.8.2. Security management controls

Configurations of all systems are centrally managed and revision controlled. The authenticity and integrity of software components are verified using digital signatures before being installed onto the server platform.

5.8.3. Life cycle security controls

Critical software components are either sourced from suppliers using a procurement process, or based on open-source products.

For each of these categories of products there is a Quality Assurance (QA) process which includes rigorous testing and continuous follow-up of any stability or security issues uncovered during the products life-cycle.

6. ZONE SIGNING

6.1. Key lengths, key types and algorithms

Currently the IE KSK uses the RSA algorithm and has 2048 bit modulus (key length) while the ZSK also uses the RSA algorithm and has a 1024 bit modulus.

6.2. Authenticated denial of existence

The IE zone is not publicly available. As such, zone enumeration is ensured using the NSEC3 standard. Accordingly, authenticated denial of existence is attested using the SHA-1 algorithm.

6.3. Signature format

The KSK signatures will be generated by encrypting SHA-256 hashes using RSA [RFC5702].

6.4. Key roll-over

The ZSK will be rolled over to a new key every 6 months. No standby keys are used.

The KSK will be rolled over to a new key every 3 years or when required. No standby keys are used, and the roll-over process will not take into account the timings specified in [RFC5011].

6.5. Signature life-time and re-signing frequency

Signatures will have 14 days validity, with 1 hour inception and 1 hour of jitter applied to the signature life-time. Resigning takes place during every rebuild which occur daily at every other odd UTC hour.

6.6. Verification of resource records

IEDR verifies that all resource records are valid in accordance with the current standards prior to delegation.

6.7. Resource records time-to-live

These values are determined by the IEDR DNSSEC key and signing policy (KASP). The DNSKEY TTL is 3,600, the SOA is 172,800. The DS TTL is 3,600 and the NSEC3 TTL is 86,400. The RRSIG inherits the TTL from the resource record that it signs.

7. COMPLIANCE AUDIT

Before the end of 2012, IEDR intend to select and procure an appropriate DNSSEC consultancy expert to conduct a compliancy audit review of the IE DNSSEC infrastructure and the statements made in this DPS document. The subsections of section 7 cannot be filled out until that process has been completed. This document will be revised in due course when IEDR have selected such an auditor. Any update to this document will be made via the channels outlined earlier in this document.

7.1. Frequency of entity compliance audit

[To Be Determined]

7.2. Identity/qualifications of auditor

[To Be Determined]

7.3. Auditor's relationship to audited party

[To Be Determined]

7.4. Topics covered by audit

[To Be Determined]

7.5. Actions taken as a result of deficiency

[To Be Determined]

7.6. Communication of results

[To Be Determined]

8. LEGAL MATTERS

8.1. Fees

IEDR do not charge any fees for the provision of DNSSEC services.

8.2. Privacy of Personal Information

The IEDR Privacy Statement is available here.

8.3. Limitation of Liability

DNSSEC registrations are subject to the IEDR's normal terms and conditions and DNSSEC registrants that use DNSSEC services are obliged to enter into an Agreement with the IEDR. The agreement contains clauses in relation to limitation of liability as follows:-

"a) Nothing in the Agreement shall be taken to exclude or limit IEDR's liability for death or personal injury caused by its negligence under applicable law.

b) IEDR limits its liability for physical damage to tangible property caused by its negligence to the sum of €25,000 for any event or series of connected events. Damage to or loss of data shall not constitute physical damage to tangible property.

c) Subject to a) above, all representations, terms, conditions and all warranties whether express or implied by statute, law or otherwise including under s 39 of the Sale of Goods and Supply of Services Act 1980, relating to the provision of the Services and the operation of the IEDR systems and the data in them are excluded to the maximum extent permissible by law;

d) IEDR will not be liable to the DNSSEC Registrant whether under contract law, tort or under statute arising from any breach by IEDR of the provisions of this Agreement including without limitation breach in relation to the provision of the DNSSEC Services, for: di) indirect or consequential loss; dii) any loss of profit, revenue, loss of business or contracts; or loss of expected savings or goodwill; diii) any mistake or missing information in the register; div) any loss of registration or use of a domain name, or both dv) or default by IEDR in registration or renewal (for whatever reason and whether temporary or otherwise), of the domain name; or dvi) any; error concerning identity of a registrant; or dvii) technical problems or faults with the Site or inability to access the Site; or dviii) third party claims in respect of a domain name; or dix) acts or omissions of the Registrar regarding the application, registration or renewal of domain names which may result in the non-registration or deletion of a domain name.

e) IEDR exclude any liability whatsoever to the Registrar and any DNSSEC Registrant to whom the Registrar provides services to, as a result of any failure or inaccuracy, delay or error in the operation of the IEDR Site, systems or the information in them.

f) IEDR's liability to the Registrar under this Agreement for any direct loss or damage in any 365 day period or part thereof for any breach or series of breaches whether or not connected to this Statement, shall be limited to an amount corresponding to the fees IEDR received from the Registrar in that period or 5,000 Euro whichever is lower.

g) The DNSSEC Registrant shall indemnify and keep IEDR indemnified in full on demand against any claim (and the resulting costs, including legal fees, loss or expense) originating from the use or registration of a domain name that infringes the rights of a third party.

This Agreement shall be governed by the laws of the Republic of Ireland."