DNSSEC Practice Statement

Contents

1. INTRODUCTION 5
   - 1.1. Overview 5
   - 1.2. Document name and identification 5
   - 1.3. Community and Applicability 5
     - 1.3.1. Registry 5
     - 1.3.2. Registrar 5
     - 1.3.3. Registrant 6
     - 1.3.4. Relying Party 6
     - 1.3.5. Internal Auditor 6
     - 1.3.6. Applicability 6
   - 1.4. Specification Administration 6
     - 1.4.1. Specification administration organization 6
     - 1.4.2. Contact Information 7
     - 1.4.3. Specification change procedures 7
2. PUBLICATION AND REPOSITORIES 7
   - 2.1. Repositories 7
   - 2.2. Publication of key signing keys 7
   - 2.3. Access controls on repositories 7
3. OPERATIONAL REQUIREMENTS 7
   - 3.1. Meaning of domain names 7
   - 3.2. Activation of DNSSEC for child zone 8
   - 3.3. Identification and authentication of child zone manager 8
   - 3.4. Registration of delegation signer (DS) resource records 8
     - 3.4.1. Who can request registration 8
     - 3.4.2. Procedure for registration request 8
     - 3.4.3. Emergency Registration Request 8
   - 3.5. Method to prove possession of private key 8
   - 3.6. Removal of DS record 8
     - 3.6.1. Who can request removal 9
     - 3.6.2. Procedure for removal request 9
     - 3.6.3. Emergency removal request 9
4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS 9
   - 4.1. Physical Controls 9
     - 4.1.1. Site location and construction 9
     - 4.1.2. Physical access 9
     - 4.1.3. Power and air conditioning 9
     - 4.1.4. Water exposures 9
     - 4.1.5. Fire prevention and protection 10
     - 4.1.6. Media storage 10
     - 4.1.7. Waste disposal 10
     - 4.1.8. Off-site backup 10
   - 4.2. Procedural Controls 10
     - 4.2.1. Trusted roles 10
     - 4.2.2. Number of persons required per task 10
     - 4.2.3. Identification and authentication for each role 10
     - 4.2.4. Tasks requiring separation of duties 10
   - 4.3. Personnel Controls 10
     - 4.3.1. Qualifications, experience, and clearance requirements 11

4.3.2. Background check procedures 11
4.3.3. Training requirements 11
4.3.4. Retraining frequency and requirements 11
4.3.5. Job rotation frequency and sequence 11
4.3.6. Sanctions for unauthorized actions 11
4.3.7. Contracting personnel requirements 11
4.3.8. Documentation supplied to personnel 11
4.4. Audit Logging Procedures 12
4.4.1. Types of events recorded 12
4.4.2. Frequency of processing log 12
4.4.3. Retention period for audit log information 12
4.4.4. Protection of audit log 12
4.4.5. Audit log backup procedures 12
4.4.6. Audit collection system 12
4.4.7. Notification to event-causing subject 12
4.4.8. Vulnerability assessments 12
4.5. Compromise and Disaster Recovery 13
4.5.1. Incident and compromise handling procedures 13
4.5.2. Corrupted computing resources, software, and/or data 13
4.5.3. Entity private key compromise procedures 13
4.5.4. Business Continuity and IT Disaster Recovery Capabilities 13
4.6. Entity termination 13
5. TECHNICAL SECURITY CONTROLS 14
5.1. Key Pair Generation and Installation 14
5.1.1. Key pair generation 14
5.1.2. Public key delivery 14
5.1.3. Public key parameters generation and quality checking 14
5.1.4. Key usage purposes 14
5.2. Private key protection and Cryptographic Module Engineering Controls 14
5.2.1. Cryptographic module standards and controls 14
5.2.2. Private key (m-of-n) multi-person control 14
5.2.3. Private key escrow 14
5.2.4. Private key backup 14
5.2.5. Private key storage on cryptographic module 15
5.2.6. Private key archival 15
5.2.7. Private key transfer into or from a cryptographic module 15
5.2.8. Method of activating private key 15
5.2.9. Method of deactivating private key 15
5.2.10. Method of destroying private key 15
5.3. Other Aspects of Key Pair Management 15
5.3.1. Public key archival 15
5.3.2. Key usage periods 15
5.4. Activation data 15
5.4.1. Activation data generation and installation 15
5.4.2. Activation data protection 16
5.4.3. Other aspects of activation data 16
5.5. Computer Security Controls 16
5.6. Network Security Controls 16
5.7. Timestamping 16
5.8. Life Cycle Technical Controls 16
5.8.1. System development controls 16
5.8.2. Security management controls 16

5.8.3. Life cycle security controls 17
6. ZONE SIGNING 17
6.1. Key lengths and algorithms 17
6.2. Authenticated denial of existence 17
6.3. Signature format 17
6.4. Zone signing key roll-over 17
6.5. Key signing key roll-over 17
6.6. Signature life-time and re-signing frequency 17
6.7. Verification of zone signing key set 17
6.8. Verification of resource records 18
6.9. Resource records time-to-live 18
7. COMPLIANCE AUDIT 18
7.1. Frequency of entity compliance audit 18
7.2. Identity/qualifications of auditor 18
7.3. Auditor's relationship to audited party 18
7.4. Topics covered by audit 18
7.5. Actions taken as a result of deficiency 18
7.6. Communication of results 18
8. LEGAL MATTERS 18
8.1. Limitations of liability 18
8.2. Governing law and jurisdiction 19

1. INTRODUCTION

This document is a statement of security practices of the applied for registry that are applied in the DNSSEC operations for the FIRMDALE top level domain names.

This document conforms with the RFC-draft DNSSEC Policy & Practice Statement Framework (draft-ietf-dnsop-dnssec-dps-framework-05).

1.1. Overview

DNSSEC (DNS Security Extensions) is a set of specifications that enable the authentication of DNS data and also make it possible to ensure that content has not been modified during transfer.

DNSSEC are described in the follow RFCs.

- RFC 4033 DNS Security Introduction and Requirements
- RFC 4034 Resource Records for the DNS Security Extensions
- RFC 4035 Protocol Modifications for the DNS Security Extensions

1.2. Document name and identification

Document title: DNSSEC Practice Statement
Version: 0.1
Created on: 30 August, 2011
Effective on: TBD

1.3. Community and Applicability

The associated entities and their roles are described in this section.

1.3.1. Registry

The Registry administrates the registrations and resolutions of the applied for FIRMDALE domain names. The Registry is responsible for generating key pairs and protecting the confidentiality of the private component of the Key Signing Keys and Zone Signing Keys. The Registry is also responsible for securely signing all authoritative DNS resource records in the applied for FIRMDALE zone. The Registry is responsible for the registration and maintenance of the applied for FIRMDALE DS resource records in the root zone.

1.3.2. Registrar

A Registrar is the party that is responsible for the administration and management of domain names of behalf of the Registrant. The Registrar handles the registration, maintenance and management of a Registrants domain name and is ICANN acredited.

The Registrar is responsible for securely identifying the Registrant of a domain. The Registrar is responsible for adding, removing or updating specified DS records for each domain at the request of the Registrant.

The relation between the Registry and a Registrar is regulated in the Registry-Registrar Agreement between the applied for FIRMDALE registry and the applied for FIRMDALE registrars.

1.3.3. Registrant

A Registrant is an entity who has registered the applied for FIRMDALE domain name(s). Registrants are responsible for generating and protecting their own keys, and registering and maintaining the DS records through the Registrar during registration, modification or transfer of domain names.

To enables the authentication and data integrity verification for the registered domain names, the Registrant composes the digital signatures on Registrant's zone using their own keys.

The Registrant is responsible for issuing an emergency key rollover if keys are suspected of being compromised or have been lost.

1.3.4. Relying Party

The relying party is the entity relying on DNSSEC such as validating resolvers and other applications. The relying party is responsible for configuring and updating the appropriate DNSSEC trust anchors.

1.3.5. Internal Auditor

Internal auditor is an entity within the applied for FIRMDALE registry who audits whether the applied for FIRMDALE DNSSEC Service is operated along with the applied for FIRMDALE DPS or not.

1.3.6. Applicability

This DPS is only applicable to the applied for FIRMDALE Root Zone. Each link in the chain of trust may have entirely different requirements that can affect the end entity, and is not governed by this DPS. Each entity shall determine the level of acceptable risk in their environment.

1.4. Specification Administration

1.4.1. Specification administration organization

The applied for FIRMDALE registry

1.4.2. Contact Information

Postal address: 21 Golden Square, London, W1F 9JN
Facsimile number: +44 (0)20 7581 1867
Email address: IT@firmdale.com
Attention: IT Department

1.4.3. Specification change procedures

Amendments to this DPS are either made in the form of amendments to the existing document or the publication of a new version of the document. This DPS and amendments to it are published at the applied for FIRMDALE registry websites. Only the most recent version of this DPS is applicable.

The applied for FIRMDALE registry reserves the right to amend the DPS without notification for amendments that are not designated as significant. It is in the sole discretion of the applied for FIRMDALE Registry to designate changes as significant, in which case the applied for FIRMDALE Registry will provide notice. Any changes will be approved by the applied for FIRMDALE Registry management and may be effective immediately upon publication.

2. PUBLICATION AND REPOSITORIES

2.1. Repositories

URL to the repository will be advice later.

2.2. Publication of key signing keys

The DS record of the applied for FIRMDALE zone are registered into and published in the root zone

2.3. Access controls on repositories

Information published at the applied for FIRMDALE website is available to the general public and is protected against unauthorized adding, deletion or modification of the content on the website.

3. OPERATIONAL REQUIREMENTS

3.1. Meaning of domain names

DNSSEC provides mechanisms for securing that the origin of the DNS data is consistent with the information in the registry. It does NOT provide any way of determining the legal entity behind the domain name, or the relevance of the domain name itself.

3.2. Activation of DNSSEC for child zone

DNSSEC is activated by at least one DS record for the zone being sent from the Registrar to the Registry and thus being published in the DNS, which established a chain of trust to the child zone. The Registry presumes that the DS record is correct and will not perform any specific controls.

3.3. Identification and authentication of child zone manager

The applied for FIRMDALE Registry does not identify and authenticate the child zone manager. Registrar is responsible to comply with the Registrar agreement contracted between the Registry and the Registrar.

3.4. Registration of delegation signer (DS) resource records

The Registry accepts DS records through the system interface from each Registrar. The DS record must be valid and sent in the suitable format. More than one DS records (up to 10) can be registered per domain name.

3.4.1. Who can request registration

The Registry accepts DS records registration from authenticated Registrars only.

3.4.2. Procedure for registration request

Registrars are authenticated before using the system interface. Registrars register the DS record(s) to the Registry through the system interface via EPP or Web. The Registry will add the DS records in the applied for FIRMDALE zone.

3.4.3. Emergency Registration Request

Not Applicable

3.5. Method to prove possession of private key

The Registry does not conduct any controls with the aims of validating the Registrant as the manager of a private key. The Registrar is responsible for conducting the controls that are required and those deemed necessary.

3.6. Removal of DS record

A DS record is deregistered by sending a request from the Registrar to the Registry. The removal of all DS records will deactivate the DNSSEC security mechanism for the zone in question.

3.6.1. Who can request removal

The Registry removes DS records for a Registrant based on the request from Registrar. Registrar should confirm the intentions of the registration with the Registrant before requesting the removal.

3.6.2. Procedure for removal request

Registrars are authenticated before they are allowed to use the system interface. Registrars request the removal of DS record(s) to the Registry through the system interface via Web or EPP. The Registry will remove the DS records in the applied for FIRMDALE zone.

3.6.3. Emergency removal request

Not applicable.

4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

4.1. Physical Controls

4.1.1. Site location and construction

The Registry installs and operate important equipments related to the applied for FIRMDALE top level domain names in multiple fully operational and geographically dispersed locations. All equipments are protected within a physical perimeter with access control. Both sites have equipped with facility protection in terms of physical security, power supply, air conditioning, fire and water protection.

4.1.2. Physical access

Physical access to the protected environment is limited to authorized personnel. Entry is logged and the environment is continuously monitored.

4.1.3. Power and air conditioning

Power is provided to the sites through separate sources. In the event of power outages, power is provided by UPS until the backup power systems have begun to generate electricity.

4.1.4. Water exposures

The sites implements water protection and detection mechanisms.

4.1.5.Fire prevention and protection

The sites are equipped with fire detection and extinguishing systems.

4.1.6.Media storage

The Registry's guidelines for information classification define the requirements imposed for the storage of sensitive data.

4.1.7.Waste disposal

Disposed storage media and other material that may contain sensitive information are destroyed in a secure manner.

4.1.8.Off-site backup

Certain critical data is also securely stored using a third-party storage facility. Physical access to the storage facility is limited to authorized personnel.

4.2. Procedural Controls

4.2.1.Trusted roles

Trusted roles are held by persons that are able to affect the zone file's content, the generation or use of private keys. The trusted roles are:
1. Systems Administrator, SA
2. Support Manager, SM
3. The applied for registry CEO, CEO

4.2.2.Number of persons required per task

At any given time, there must be at least two individuals within the organization per trusted role indicated in 4.2.1. Key generation requires two people to be present. None of the aforementioned operations may be performed in the presence of unauthorized people.

4.2.3.Identification and authentication for each role

Permissions to use the equipments are authorized for each role. Authentication are required before the use of equipments are allowed.

4.2.4.Tasks requiring separation of duties

The trusted roles in 4.2.1 above may not be held simultaneously by one and the same person.

4.3. Personnel Controls

4.3.1. Qualifications, experience, and clearance requirements

Persons who have the trusted roles in 4.2.1 above are limited to full time employees of the Registry.

4.3.2. Background check procedures

The evaluation of background checks is conducted by the HR function at the applied for FIRMDALE registry. The background checks include the following:

- Confirmation of previous employment
- Check of professional references
- Confirmation of the highest or most relevant educational degree obtained
- Check of credit/financial records to the extent allowed by national laws for the individual's country of residence
- Search of criminal records (local, state or provincial, and national)
- Search of driver's license records

4.3.3. Training requirements

The Registry gives training to personnel in charge of the DNSSEC Service. Before the person is taking up the role, the required trainings for the roles are provided. When there is changes to the operation, trainings associated with the changes are provided.

4.3.4. Retraining frequency and requirements

The Registry provides trainings as necessary, such as when there is major change in the operation, systems and organization.

4.3.5. Job rotation frequency and sequence

The responsibility for conducting operations is rotated on each occasion between the people who hold a trusted role.

4.3.6. Sanctions for unauthorized actions

Sanctions resulting from unauthorized actions are regulated by the HR function at the applied for FIRMDALE registry.

4.3.7. Contracting personnel requirements

In certain circumstances, the applied for FIRMDALE registry may need to use contractors as a supplement to full-time employees. These contractors are managed according to the applied for FIRMDALE Registry Security Policy.

4.3.8. Documentation supplied to personnel

The Registry and IT operations supply the documentation necessary for the individual employee to perform their work task in a secure and satisfactory manner.

4.4. Audit Logging Procedures

4.4.1. Types of events recorded

The following events are included in logging:

- Key management activities, such as key generation, key rolling, key activation, and signing and exporting keys
- Remote access, successful and unsuccessful
- Privileged operations
- Entry to a facility

Log entries include the following elements:

- Date and time of the entry
- Identity of the entity
- Activity of the entry

4.4.2. Frequency of processing log

Logs are continuously monitored through automated control and sufficiently frequently through manual controls to detect any anomalies.

4.4.3. Retention period for audit log information

Log information is stored in systems for not less than 3 years.

4.4.4. Protection of audit log

All electronic log information is stored at the protected operations facilities. The logging system is protected against unauthorized viewing and the manipulation of information.

4.4.5. Audit log backup procedures

All electronic log information is securely back up on daily basis and is stored separately from the system in a secure location.

4.4.6. Audit collection system

The application and system scripts will generate and collect audit logs. The audit logs will be backup to tape according to the backup plan.

4.4.7. Notification to event-causing subject

No notice is required to be given to the individual, organization, device, or application causing a log event.

4.4.8. Vulnerability assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Security vulnerability assessments are performed, reviewed, and revised triggered by error logged in the events log.

4.5. Compromise and Disaster Recovery

4.5.1. Incident and compromise handling procedures

All incidents are handled in accordance with the Registry's incident handling procedures. The incident handling procedure includes investigating the cause of the incident, what effects the incident has had or may have had, measures to prevent the incident from recurring and forms to further report this information.

An incident that involves suspicion that a private key has been compromised leads to the immediate rollover of keys pursuant to the procedures indicated in chapter 4.5.3.

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

In the event of corruption, the incident management procedures shall be initiated and appropriate measures shall be taken.

4.5.3. Entity private key compromise procedures

Suspicion that a private key has been compromised or misused leads to a controlled key rollover as follows:
If a zone signing key is suspected to be compromised, it will immediately be removed from production and stopped being used. A new ZSK will be generated and the old key will be removed from the key set as soon as its signatures have expired or timed out.

If a KSK is suspected of having been compromised, a new key will be generated and put into immediate use, in parallel with the old key. The old KSK will remain in place and be used to sign key sets until such time as it can be considered sufficiently safe to remove the key taking into account the risk for system disruptions in relation to the risk that the compromised key presents.

4.5.4. Business Continuity and IT Disaster Recovery Capabilities

The Registry has a IT disaster recovery plan that ensures that operation-critical production can be switched over between the two operation facilities. The facilities are equivalent in terms of physical and logistical protection. Information is replicated between the facilities.

4.6. Entity termination

If the Registry must discontinue DNSSEC for any reason and return to an unsigned position, this will take place in an orderly manner. 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

The key generation takes place in signing systems managed by trained personnel in trusted roles. Key generation takes place when necessary and is performed by two personnel simultaneously.

5.1.2. Public key delivery

The public component of each generated KSK is exported from the signing system and verified by the SM and SA. The SM is responsible for publishing the public component of the KSK in a secure manner. The SA is responsible for ensuring that the keys that are published are the same as those that were generated.

5.1.3. Public key parameters generation and quality checking

The Registry periodically confirms that generation of signing key is conducted with appropriate parameters and is with the correct key length.

5.1.4.Key usage purposes

The Registry uses the signing keys only for generating signatures for the applied for FIRMDALE zone and does not use them for any other purposes.

5.2. Private key protection and Cryptographic Module Engineering Controls

5.2.1.Cryptographic module standards and controls

The keys are encrypted using standard cryptographic algorithm in the HSM.

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

During the HSM activation, at least 2 person with trusted role need to be present to be enrolled as such and activate the HSM. One System Administrator is required to get logical access. Multi-person control will be applied during the creation of a key backup and restoration.

5.2.3.Private key escrow

The private key is not escrowed.

5.2.4.Private key backup

The private key are backup into separate signing systems that are installed in the protected facilities.

5.2.5.Private key storage on cryptographic module

Private key are stored in encrypted format in the HSM.

5.2.6.Private key archival

Private keys that are no longer used are not archived in any other form than as backup copies.

5.2.7.Private key transfer into or from a cryptographic module

The key will be stored in an encrypted form in a portable media when a transfer is needed.

5.2.8.Method of activating private key

The private key is activated by SM and is observed by CEO. The active status of keys continues until the usage period is finished.

5.2.9.Method of deactivating private key

The private keys are deactivated upon system shutdown.

5.2.10. Method of destroying private key

Private keys are not destructed. After their useful life, they are removed from the signing system.

5.3. Other Aspects of Key Pair Management

5.3.1.Public key archival

Public keys are not archived.

5.3.2.Key usage periods

Keys become invalid as they are taken out of production. Old keys are not reused.

5.4. Activation data

5.4.1.Activation data generation and installation

Each personnel with trusted roles are responsible to create their own activation data (passphrase) according to the requirements set out in the applied for FIRMDALE Registry Security Policy.

5.4.2. Activation data protection

Each personnel is responsible for protecting their activation data in the best reasonable possible way. On the suspicion of compromised activation data, the personnel must immediately change it.

5.4.3. Other aspects of activation data

In the event of an emergency, there is a sealed and tamper evident envelope in a secure location that contains activation data.

5.5. Computer Security Controls

All critical components of the Registry's systems are placed in the protected 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

The Registry has sectioned networks that are divided into various security zones with secured communications in-between. Logging is conducted in the firewalls. Transmission of classified information is protected with suitable method (e.g. encryption).

5.7. Timestamping

The Registry retrieves time from NTP servers. Time stamps are used for log information and validity time for signatures.

5.8. Life Cycle Technical Controls

5.8.1. System development controls

The Registry controls the processes of system developments. The development model includes specifying the functional and security requirements, as well as systematic testing and regression tests.

5.8.2. Security management controls

The Registry has adopted an Information Security Policy. The Registry regularly conduct risk assessment and implement preventive measures, detective measures and corrective actions. The Registry also conducts regular security audits of the system.

5.8.3. Life cycle security controls

The signer system is designed to require a minimum of maintenance. Updates critical to the security and operations of the signer system will be applied after formal testing and approval using CMMI standards. The origin of all software and firmware will be securely authenticated by available means.

6. ZONE SIGNING

6.1. Key lengths and algorithms

The key length of KSK is 2048 bits and that of ZSK is 1024 bits.
The algorithm for both KSK and ZSK is RSASHA256 specified in RFC 5702.
The algorithm is defined by the protocol standards by IETF.

6.2. Authenticated denial of existence

For authenticated denial of existence, NSEC3 records with Opt-Out flag specified in RFC 5155 is adopted.

6.3. Signature format

The signature format is RSA/SHA-256 specified in RFC 5702.

6.4. Zone signing key roll-over

ZSK rollover is carried out on a monthly basis by the pre-publish method described in RFC 4641.

6.5. Key signing key roll-over

KSK rollover is carried out on an annual basis by the double signature method described in RFC 4641.

6.6. Signature life-time and re-signing frequency

RR sets are signed with KSKs with validity period of = 15 days
RR sets are signed with ZSKs with validity period of = 10 days

Resigning frequency using KSKs is = 90 day
Resigning frequency using ZSKs is = 30 day

These values are for reference only and may be changed without prior notice.

6.7. Verification of zone signing key set

To ensure signatures and the validity period of keys, security controls are conducted against the DNSKEY prior to publishing zone information on the Internet. This is done by verifying the chain from DS in the parent zone to KSK, ZSK and the signature over the zones SOA.

6.8. Verification of resource records

The Registry verifies that all resource records are valid in accordance with the current protocol standards prior to distribution.

6.9. Resource records time-to-live

DNSKEY = 24 hours
NSEC3 and NSEC3PARAM = 1 hour
DS = NS TTL = 1 hour
RRSIG = inherits TTL from the RRset

These values are for reference only and may be changed without prior notice.

7. COMPLIANCE AUDIT

7.1. Frequency of entity compliance audit

The Registry conducts security audit regularly every year.

7.2. Identity/qualifications of auditor

The auditor shall be able to demonstrate proficiency in IT security, DNS and DNSSEC.

7.3. Auditor's relationship to audited party

An internal auditing manager shall be appointed for the audit.

7.4. Topics covered by audit

The applied for FIRMDALE DPS is covered by the audit.

7.5. Actions taken as a result of deficiency

The result will be followed up aiming to correct any discrepancy with the applied for FIRMDALE DPS.

7.6. Communication of results

A written report will be submitted to the applied for FIRMDALE Registry management for the record and to follow up.

8. LEGAL MATTERS

The Registry has no legal responsibility for the matters described in the applied for FIRMDALE DPS.

8.1. Limitations of liability

The relevant section of the Registrar Agreement regulates the limitations of liability between the Registry and the Registrar.

8.2. Governing law and jurisdiction

The applied for FIRMDALE DPS shall be governed by and interpreted in accordance with the laws of Malaysia. The parties hereby submit to the exclusive jurisdiction of the courts of Malaysia.