GMO REGISTRY

DNSSEC Practice Statements

Table of Contents

1 Introduction 3
1.1 Overview 4
1.2 Document Name and Identification 4
1.3 Community and Applicability 4
1.3.1 Registry 4
1.3.2 Registrars 4
1.3.3 Registrants 5
1.3.4 DNS Operators 5
1.3.5 Relying Party 5
1.3.6 Applicability 5
1.4 Specification Administration 5
1.4.1 Specification Administration Organisation 5
1.4.2 Contact Information 6
1.4.3 Specification Change Procedures 6
2 Publication and Repositories 6
2.1 Repositories 6
2.2 Publication of public keys 6
3 Operational Requirements 6
3.1 Meaning of Domain Names 6
3.2 Identification and Authentication of Child Zone Manager 7
3.3 Registration of delegation signer (DS) resource records 7
3.4 Method to Prove Possession of Private Key 7
3.5 Removal of Delegation Signer Record 7
3.5.1. Who can request removal 7
3.5.2 Procedure for removal request 7
3.5.3 Emergency removal request 8
4 Facility, Management and Operational Controls 8
4.1 Physical Controls 8
4.1.1 Site Location and Construction 8
4.1.2 Physical Access 8
4.1.3 Power and Air Conditioning 8
4.1.4 Water Exposure 9
4.1.5 Fire Prevention and Protection 9
4.1.6 Media Storage 9
4.1.7 Waste Disposal 9
4.1.8 Off-Site Backup 9

4.2 Procedural Controls 9
4.2.1 Trusted Roles 9
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 10
4.3.2 Background Check Procedures 11
4.3.3 Training Requirements 11
4.3.4 Job rotation frequency and sequence 11
4.3.5 Sanctions for unauthorized actions 11
4.3.6 Contracting personnel requirements 11
4.3.7 Documentation supplied to personnel 11
4.4 Audit Logging Procedures 11
4.4.1 Types of Events Recorded 11
4.4.2 Frequency of Processing Log Information 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 Vulnerability Assessments 13
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 15
5.2.3 Private Key Escrow 15
5.2.4 Private Key Backup 15
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 16
5.4 Activation Data 16
5.4.1 Activation Data Generation and Installation 16
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 17
5.8 Life Cycle Technical Controls 17
6 Zone Signing 17
6.1 Key Lengths and Algorithms 17
6.2 Authenticated Denial of Existence 17
6.3 Signature Format 18
6.4 Key Roll-over 18
6.5 Signature Lifetime and Re-Signing Frequency 18
6.6 Verification of Resource Records 19
6.7 Resource Records Time-to-Live 19
7 Compliance audit 19
7.1 Frequency of entity compliance audit 19
7.2 Identity and qualifications of auditor 20
7.3 Auditor's relationship to audited party 20
7.4 Topics covered by audit 20
7.5 Actions taken as a result of deficiency 20
7.6 Communication of results 20
8 Legal matters 20
Appendix A 21

1 Introduction

This DNSSEC Policy Statement (DPS) is a statement of security practices and provisions made by GMO Registry, Inc (“GMO”) in relation to the Domain Name System Security Extensions (DNSSEC) for TLDs.

This DPS conforms to the template included in *draft-ietf-dnsop-dnssec-dps-framework-07*[1], dated March 8, 2012.

The approach described here is modeled closely on the corresponding DPS procedures published for the Swedish TLD by the "*Stiftelsen för Internetinfrastruktur*" (.SE The Internet Infrastructure Foundation)[2] and the DPS procedures published for the Canadian TLD by the *Canadian Internet*

Registration Authority (CIRA)[3].

1.1 Overview

The Domain Name System (DNS) is described in RFC 1034[4] and RFC 1035[5]. DNSSEC is an extension to the DNS that allows data retrieved from the DNS to be authenticated. DNSSEC as intended for use for names in the TLD domain is specified in RFC 4033[6], RFC 4034[7], RFC 4035[8],RFC 5155[9] and RFC 5702[10]. DNS Resource Records secured with DNSSEC are signed cryptographically using asymmetric public/private key pairs. The public keys corresponding to private keys used to sign data are published in the DNS itself as signed resource records (DNSKEYs). One or more trust anchors for TLD zones are published in the DNS as Delegation Signer (DS) Resource Records in the root zone. Trust in signatures published in the TLD zone can consequently be inferred from trust in signatures in the root zone created by the root key[11]. DS Resource Record updates to the root zone for TLD will conform to the process as described by IANA[12].

1.2 Document Name and Identification

Document Name:	GMO DPS Statement for TLD
Version:	1.0
Last Modification:	2013-02-26
Document Available From:	https://www.gmoregistry.com/
Contact:	Yoshitake Tamura

1.3 Community and Applicability

The following functional subsets of the community to which this document has applicability have been identified, based on the use of a Registry-Registrar-Registrant model.

1.3.1 Registry

GMO operates the registry for various TLDs. GMO is responsible for the management of the registry, and consequently for the registration of domain names under the top-level domains. GMO is responsible for generating all DNSSEC cryptographic key material, including signing the TLD zones.

1.3.2 Registrars

A registrar is a party responsible for requesting changes in the registry on behalf of registrants. Each registrar is responsible for the secure identification of the registrant of a domain name under its
sponsorship. Registrars are responsible for adding, removing or updating Delegation Signer (DS) records for each domain at the request of the domain's registrant.

1.3.3 Registrants

Registrants are responsible for generating and protecting their own keys, and registering and maintaining corresponding DS records through a registrar. Registrants are responsible for emergency key rollover if the keys used to sign their domain names are suspected of being compromised or have been lost.

1.3.4 DNS Operators

The registrant may outsource their technical responsibility to a third-party DNS Operator.

1.3.5 Relying Party

The relying party is the entity that makes use of DNSSEC signatures, such as DNSSEC validators and
other applications. The relying party is responsible for maintaining appropriate trust anchors. Relying
parties who choose to make use of TLD-specific trust anchors must stay informed of any relevant DNSSEC-related changes or events in the TLD domain. Relying parties who make use of a root zone trust anchor should not need to make trust anchor changes in response to events in the TLD registry, since trust anchors are securely added to the root zone as DS records.

1.3.6 Applicability

Each registrant and relying party is responsible for determining an appropriate level of security for their domain and DNSSEC infrastructure. This DPS applies exclusively to the TLD zone. With the support of this DPS, registrants and relying parties can determine an appropriate degree of trust in the TLD zone and assess their own risk accordingly.

1.4 Specification Administration

This DPS is updated as appropriate to reflect modifications in systems or procedures and to keep up with best practices in the industry in response to new development within the Internet Engineering Task Force community, as well as to respond to new threats based on cryptographic research.

1.4.1 Specification Administration Organisation

GMO Registry, Inc.
Cerulean Tower,
26-1 Sakuragaokacho,
Shibuya ku,
Tokyo,
JAPAN

1.4.2 Contact Information

Technical Director: Yoshitake Tamura:
GMO Registry, Inc.
Cerulean Tower,
26-1 Sakuragaokacho,
Shibuya ku,
Tokyo,
JAPAN
Email: system@gmoregistry.com

1.4.3 Specification Change Procedures

Changes to this DPS will result in new revisions of the entire document. The current version of this
document is available at https://www.gmoregistry.com/.

GMO may amend the DPS without notification for changes that are not considered significant. Changes are designated as significant at GMO's discretion. GMO will provide reasonable notice of significant changes. All changes to this DPS will be approved by GMO and be effective immediately upon publication.

2 Publication and Repositories

Notifications relevant to DNSSEC at GMO will be distributed by e-mail to registrars and the DNS-OARC dns-operations mailing list.

2.1 Repositories

GMO publishes DNSSEC-related information at https://www.gmoregistry.com/.
Information published in the GMO DNSSEC repository is intended to be available to the general public.

2.2 Publication of public keys

GMO publishes Key Signing Key (KSK) for the TLD zone as DS records in the root zone.
History key information will be published at https://www.gmoregistry.com/.

3 Operational Requirements

3.1 Meaning of Domain Names

A domain name is a unique identifier in the DNS, as described in RFC 10349 and RFC 103510. For the
purposes of this document a domain name is a name registered under the TLD top-level

domain, and
corresponds to a delegation from the TLD zone to name servers operated by or on behalf of the domain name's registrant.

3.2 Identification and Authentication of Child Zone Manager

DNSSEC for a child zone is activated by publishing a signed DS record for that zone. The addition of a DS record to the TLD registry for the corresponding domain name, establishes a chain of trust from the TLD zone to the child zone.

Identification and authentication of each child zone manager is the responsibility of the sponsoring registrar for the domain name.

3.3 Registration of delegation signer (DS) resource records

The TLD registry accepts DS records through an EPP interface according to RFC 5910[13] and via the Registrar Console. Syntactically valid DS record will be accepted by the registry, and no checks will be performed as to the accuracy of the trust anchor with respect to the child zone's KSK. This is done specifically to allow pre-publishing of DS records for keys that are stored off-line.

3.4 Method to Prove Possession of Private Key

The sponsoring registrar for a domain name is responsible for authenticating the registrant as the manager of the domain name. This manager is assumed to have control, or have delegated control of the private key.

3.5 Removal of Delegation Signer Record

DS records are removed from the TLD registry using an EPP interface according to RFC 5910[13] and the Registrar Console. The removal of all DS records for a domain name will remove the chain of trust between the TLD zone and the child zone.

3.5.1. Who can request removal

The registrant for a domain name has the authority to request removal of a DS record, subject to identical authentication as required for modifications of NS records. The sponsoring registrar must comply with requests from the registrant, regardless of the standing between the two parties.

3.5.2 Procedure for removal request

The registrant of a domain name requests the domain's sponsoring registrar to remove the DS record. The registrar transmits this request to the TLD registry using EPP or the Registrar

Console. Once the transaction has been successfully received and processed by the TLD registry, the DS record will be removed from the TLD zone when the following revision of the TLD zone is distributed (within the hour).

3.5.3 Emergency removal request

There is no provision for a registrant to be able to make an emergency removal request of the TLD registry. All DS record removals must be executed through the domain's sponsoring registrar.

4 Facility, Management and Operational Controls

4.1 Physical Controls

GMO has implemented a Security Policy, which supports the security requirements of this DPS. Compliance with these policies is included in Section 7 Compliance Audit.

4.1.1 Site Location and Construction

GMO has established two fully-operational and geographically-dispersed operation centers. Each site serves as a back-up to the other. Both sites are protected by multiple tiers of physical security that deters, prevents and detects unauthorized access attempts. Each site contains a full set of equipment necessary to sign the TLD zone, and verify the signed zone. All signing components are placed within locked cabinets. A third site is used to store off-line HSMs and associated portable media, within a secure container.

4.1.2 Physical Access

Physical access to operation centers is restricted to authorized personnel. All entry to both operation
centers is logged and the environment is continuously monitored. Access to locked cabinets is further restricted to personnel with trusted roles.

The physical security system includes additional tiers of key management security which serves to protect both online and offline storage of HSMs and keying material.

Offline HSMs are protected through the use of locked cabinets. Access to HSMs and keying material are restricted in accordance to GMO's segregation of duties requirements. The opening and closing of cabinets in these tiers is logged for audit purposes.

4.1.3 Power and Air Conditioning

Operation centers are equipped with multiple power sources, including battery and generator support to ensure an uninterrupted supply. Operation centers are cooled with redundant air conditioning systems to ensure a consistent, stable operating environment.

4.1.4 Water Exposure

Both operation centers implement flood protection and detection mechanisms.

4.1.5 Fire Prevention and Protection

Operation centers are equipped with fire detection and extinguishing systems.

4.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within the operation centers. Secure off-site storage facility with appropriate physical and logical controls are leveraged to restrict access to authorized personnel and protect media from accidental damage.

4.1.7 Waste Disposal

Sensitive media and other material that may contain sensitive information are destroyed in a secure
manner, either by GMO or by a contracted party.

4.1.8 Off-Site Backup

GMO performs regular backups of critical data, audit logging data and other sensitive information. An off-site facility is leveraged for storage of backup media. Physical access to the storage facility is limited to authorized personnel. The storage facility is geographically and administratively separate from GMO's other operational facilities.

4.2 Procedural Controls

4.2.1 Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control
operations that may materially affect DNSSEC content via access to registry database servers, signing servers, validation servers and HSMs.

Trusted Persons include; but are not limited to:

- DNS Operations personnel
- Security personnel
- System administration personnel
- Executives that are designated to manage infrastructure

GMO considers the categories of persons identified in this section as Trusted Persons as having a trusted position. Trusted positions are assigned to GMO staff personnel, and relate

to the publication of trust anchors and the generation and use of private keys. The trusted roles are:

- **"SA"** System Administrator
- **"SO"** Security Officer
- **"WI"** Witness

There must be at least two different individuals assigned to each positin.

4.2.2 Number of Persons Required per Task

HSM Activation and Deactivation: 3 persons (1 SA, 1 SO, 1 WI)
Key Generation: 3 persons (1 SA,1 SO,1 WI)
Distribution of encrypted Key Archives to: 2 persons (1 SA or SO, 1 WI)
Signing Components: 2 persons (1 SA and 1 SO or WI)

GMO has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties and multiple trusted persons are required to perform sensitive tasks.
The most sensitive tasks related to the cryptographic hardware (HSM or Hardware Security Module) and related key material will require multiple trusted persons.

4.2.3 Identification and Authentication for Each Role

Only GMO staff members who have signed a GMO employment agreement may hold a trusted person role of SO or SA. The role of WI can be filled with any person of good standing. Valid identification must be provided before credentials for system access are provided.

4.2.4 Tasks Requiring Separation of Duties

Tasks requiring separation of duties includes, but are not limited to, the generation, implementation or destruction of DNSSEC key material. No two trusted roles may be held by a single individual.

Designated audit personnel may not participate in the multi-person control for the ZSK or KSK. Systems Administrators have exclusive physical access to DNSSEC operational equipment. Security Officers and Witnesses have no such access. Security Officers hold credentials for HSM activation. Systems Administrators hold no such credentials. A witness is a person in good standing with no ties to the operations, or IT aspects of the company. The witness has the ability to question the procedure at all stages of DNSSEC procedures.

4.3 Personnel Controls

4.3.1 Qualifications, Experience and Clearance Requirements

Candidates for any trusted role must demonstrate appropriate background knowledge and

qualifications.

4.3.2 Background Check Procedures

Background checks for candidates for SA and SO roles are carried out by the Human Resources department at GMO, and follow normal procedures for background checks on new hires. A successful background check is required for such role to be assigned. The witness has to be a person in good standing.

4.3.3 Training Requirements

GMO provides its personnel with training upon hire as well as on-going training as needed to perform their job responsibilities competently and satisfactorily.

4.3.4 Job rotation frequency and sequence

SA and SO roles are rotated within the Operations teams so that a single individual does not perform the same role twice in a row.

4.3.5 Sanctions for unauthorized actions

Any unauthorized action taken by a staff member will result in disciplinary action and possible criminal prosecution.

4.3.6 Contracting personnel requirements

Personnel hired by GMO as contractors are subject to background checks and confidentiality agreements. Contractors must demonstrate appropriate background knowledge and qualifications.

4.3.7 Documentation supplied to personnel

Personnel will be supplied with documentation required for their trusted role, including this DPS policy, audits performed in the past, plus all system administration documentation relevant to the DNSSEC signing solution.

4.4 Audit Logging Procedures

GMO implements automatic log collection from GMO computer systems, for the purposes of monitoring and analysis in the event that a security violation is suspected. Paper documentation relating to the execution of procedures is also collected for the purposes of auditing performance of those procedures.

4.4.1 Types of Events Recorded

GMO manually or automatically logs critical events related to KSK and ZSK management:

- Key generation, backup, storage, recovery, archival and destruction
- Cryptographic device life cycle management events.
- Key activation and deactivation, rollover events, algorithm changes
- Receipt and validation of signed public key material.

GMO manually or automatically logs critical events related to system security and management:

- Facility visitor entry/exit.
- Successful and unsuccessful system access events
- Security system actions performed by trusted personnel including software updates
- System crashes, hardware failures and other anomalies
- Networking equipment events including firewalls, IDS, routers, load-balancers, etc.

Log entries include the following elements:

- Date and time of the entry based on NTP
- Identity of the entity making the journal entry
- Serial or sequence number of entry, for automatic journal entries
- Entry type and log level

4.4.2 Frequency of Processing Log Information

Logs are continuously analyzed through automatic and manual controls.

4.4.3 Retention Period for Audit Log Information

Electronic logs are retained on-line for one year. All log information collected is archived for at least three years.

4.4.4 Protection of Audit Log

All audit log information is stored securely to protect against unauthorized viewing and manipulation.

4.4.5 Audit log backup procedures

All audit log information is stored securely at multiple physically separate locations

4.4.6 Audit Collection System

Automated audit data is generated and recorded at the application, network, and operating system level.
Manually generated audit data is recorded by GMO personnel and stored using current methods for physical and fire protection.

4.4.7 Vulnerability Assessments

All anomalies in the collected log information are investigated to analyze potential vulnerabilities.

4.5 Compromise and Disaster Recovery

4.5.1 Incident and Compromise Handling Procedures

All actual and suspected events relating to security that have caused or could have caused an outage,
damage to computer systems, disruptions and defects due to incorrect information or security breaches are defined as incidents. All incidents are handled according to GMO's standard procedures.

4.5.2 Corrupted Computing Resources, Software and/or Data

Any defect which results in the generation of inaccurate data will be addressed by the deployment of
multiple, independent signing implementations. All such defects will trigger incident management procedures.

4.5.3 Entity Private Key Compromise Procedures

A suspected or actual ZSK compromise will be addressed by immediately by removing the compromised ZSK from service, replacing it with a newly-generated or pre-generated replacement key. A suspected or actual KSK compromise will be addressed by immediately executing a controlled key
rollover.

4.5.4 Business Continuity and IT Disaster Recovery Capabilities

GMO's organisation-wide business continuity and IT disaster recovery plans include measures to ensure continuity of operation for registry and zone distribution systems including all DNSSEC signing components.

4.6 Entity Termination

If GMO needs to discontinue DNSSEC for the TLD zone for any reason and return to an unsigned zone, the removal of DNSSEC will take place in an orderly manner with public notification.
If operation of the TLD registry is transferred to another party, GMO will participate in the transition so as to make it as smooth as possible according to the same rules and conditions as defined for registrant transfer and cooperation of DNSSEC operations.

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 is managed by trained and specifically authorized personnel in trusted roles. The cryptographic modules are used for the Storage
Master Key (SMK), KSK, and ZSK meet the requirements for FIPS-140-2 Level 4.

The SMK, KSK, and ZSK are generated in a key generation ceremony based on proven ceremony implementations as published by IANA and used for the root zone[9]. The activities of this key generation ceremony are recorded, dated, and signed by the individuals involved. These records are kept for audit and tracking purposes.

5.1.2 Public Key Delivery

One SA, one SO, and one WI must be present throughout the Public Key Delivery process. The public part of each generated KSK pair is exported from the key generation system and verified by the SA and the SO. The SO is responsible for publishing the public part of each generated KSK pair. The SA is responsible for ensuring that the keys that are published are the same as those that were generated. The WI ensures that all processes are followed and any anomalies are documented.

5.1.3 Public Key Parameters Generation and Quality Checking

Key parameters, including the key length and the algorithm type, are verified by the SA, SO and the WI.

5.1.4 Key Usage Purposes

Keys generated for DNSSEC are never used for any other purpose or outside the signing systems.

5.2 Private Key Protection and Cryptographic Module Engineering Controls

All cryptographic operations are performed within FIPS-140 certified HSM's and no private keys are ever available in unprotected form outside an HSM.

5.2.1 Cryptographic Module Standards and Controls

For KSK and ZSK key pair generation and signing, GMO uses hardware modules that are certified to FIPS 140-2 level 4.

5.2.2 Private Key (M of N) Multi-Person Control

GMO has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive cryptographic operations. The threshold number of trusted individuals needed is three.

5.2.3 Private Key Escrow

Private components of zone KSK and ZSK are not escrowed.

5.2.4 Private Key Backup

The key archive is encrypted with a Storage Master Key (SMK). The encrypted key archive and SMK are stored on Smart Card in a TL-30 rated bank vault, only accessible by an SO and Witness.

5.2.5 Private Key Storage on Cryptographic Module

Private keys do not leave the cryptographic module without first being encrypted with the SMK. The private keys are stored in encrypted form on smart cards.

5.2.6 Private Key Archival

GMO KSK and ZSK key pairs do not expire, but are retired when superseded.

5.2.7 Private Key Transfer into or from a Cryptographic Module

During the installation of each signing system a shared SMK is transferred via portable media to each
HSM. Keys are transferred between HSM's in encrypted key archives stored on portable media.

5.2.8 Method of Activating Private Key

Private keys are activated by putting an HSM on-line. Access to the HSM is provided by an SA; credentials for putting an HSM on-line are held by a SO. Ensuring no process violations occur is provided by the WI.

5.2.9 Method of Deactivating Private Key

Private keys are deactivated by taking an HSM off-line, either by manipulation of the device by an SO or due to a power failure or tamper attempt.

5.2.10 Method of Destroying Private Key

Private keys are not destroyed. After their useful life, keys are removed from the signing system.
Tampering with an HSM destroys its contents. If there is any operational issue with an HSM, a controlled temper will be performed before returning the HSM to the vendor, ensuring

destruction of
private keys.

5.3 Other Aspects of Key Pair Management

Public keys are backed up and archived as part of GMO's routine backup procedures.
The operational period of each KSK and ZSK ends upon its supersession. The superseded zone KSK and ZSK will be never be reused to sign a resource record.

5.4 Activation Data

The activation data are the credentials held by the SO to activate the HSM.

5.4.1 Activation Data Generation and Installation

Each SO is responsible for specifying a PIN which is used in conjunction with a physical token. The PIN is known only to the SO that specified it. Physical tokens are stored with the HSM they are intended to be used with.

5.4.2 Activation Data Protection

Each SO is responsible for protecting their PIN in a secure fashion. If there is suspicion that a PIN has
been compromised, the SO concerned must immediately change it. The SO will sign an agreement
acknowledging their responsibilities.

5.4.3 Other aspects of activation data

Not applicable.

5.5 Computer Security Controls

All production computer systems are housed in secure facilities. Physical access to computer systems is limited to authorized personnel. Remote (network) access to signing systems is only possible via an authenticated VPN connection by an SA. All attempts to access computer systems, successful and unsuccessful, are logged.

5.6 Network Security Controls

GMO's DNSSEC signing infrastructure is logically separated from other components. This separation prevents network access except through defined application processes. GMO uses firewalls to protect the DNSEC signing network from both internal and external intrusion and to limit the nature and source of network activities that may access DNSSEC signing systems. The network that connects signing systems to HSMs is wholly contained within a locked cabinet that
houses the signing systems and HSMs.

All data transfers between a signing systems and distribution and validation systems are initiated by signing system. It is not possible to transfer data to or from a signing system using atransaction initiated from a remote host with the exception of an SA initiated VPN connection. All firewall components generate logs which are collected, analyzed and retained.

5.7 Timestamping

All DNSSEC components are time-synchronised to diverse, reputable time servers using authenticated
NTP.

5.8 Life Cycle Technical Controls

Applications are developed and implemented by GMO in accordance with GMO systems development and change management processes. All software deployed on production systems can be traced to change management tickets. GMO has technologies and/or policies in place to control and monitor the configurations of its systems.

The signer system is designed to require a minimum of maintenance. Updates critical to the security and operations of the signer system from the vendors will be applied after formal testing and approval.

The origin of all software and firmware will be securely authenticated by available means. Critical hardware components of the signer system (HSM) will be procured directly from the manufacturer and transported in tamper-evidence bags to their destination in the secure facility. All hardware will be decommissioned well before the specified lifetime expectancy.

6 Zone Signing

6.1 Key Lengths and Algorithms

KSK Algorithm	RSASHA256 (DNSKEY Type Code 8)
KSK Length	2048 bits
ZSK Algorithm	RSASHA256 (DNSKEY Type Code 8)
ZSK Length	1024 bits

6.2 Authenticated Denial of Existence

Authenticated denial of existence will be provided through the use of NSEC3 records as specified in RFC 5155[14] without OPT-OUT.

6.3 Signature Format

Zone KSK and ZSK signatures are generated using RSA over SHA256 (RSASHA256, as specified in RFC 5702[10]).

6.4 Key Roll-over

ZSK rollovers are carried out at least every 90 days

Key Activity	Length	Description
Active	90 days	The maximum number of days a key is used to sign a zone before rolling over to a new key
Pre-publish	7 days	Before signing a zone with a key, that key will be pre-published in the zone for this period
Post-publish	7 days	After the old key is rolled over, it is still published (however nothing is signed with it) in the zone for this period
Emergency	2 days	If a ZSK is believed to be compromised, an emergency rollover rollover post- of the ZSK will result in the old key still being published in the publish zone for 2 days; ensuring resolvers do not malfunction but the zone is not signed with it.

KSK rollover is carried out every year or as revised based on events.

Key Activity	Length	Description
Active	365 days	The maxium number of days a key is used to sign a zone before rolling over to a new key
Pre-publish	30 days	Before signing a zone with a key, the key is pre-published in the zone for this period
Post-publish	30 days	After the old key is rolled over, it is still published (however nothing is signed with it) in the zone for this period
Emergency	7 days	If a ZSK is believed to be compromised, an emergency rollover rollover post- of the ZSK will result in the old key still being published in the publish zone for 7 days; ensuring resolvers do not malfunction but the zone is not signed with it.

6.5 Signature Lifetime and Re-Signing Frequency

Resource Record sets (RRSets) are signed with ZSKs with a validity period between six and

eight days, using jittered signature lifetime periods.

Re-signing takes place every time a new TLD zone is generated, though signature re-use limits the
amount of re-signing that has to take place.

6.6 Verification of Resource Records

Each signed zone is subject to a number of tests, all of which must pass before the signed zone is
distributed to name servers. These tests include verification of the chain of trust from the root zone to
signatures over the apex DNSKEY RRSet.

Cryptographic software from at least two independent implementations are used to sign copies of the zone and compared for consistenc. All resource records are verified prior to distribution. The integrity of the unsigned zone contents is also validated prior to distribution. Cryptographic software from independent vendors is used for validation.

Orphaned glue records will be signed by GMO when these appear in the zone file as a result of a domain deletion.

6.7 Resource Records Time-to-Live

The following time-to-live parameters will be used

SOA	86400 seconds (24 hours)
DNSKEY	43200 seconds (12 hours)
NS, A, AAAA	86400 seconds (24 hours)
RRSIG	inherited from signed RRSet
DS	86400 seconds (24 hours)
NSEC3	3600 seconds (1 hour)

7 Compliance audit

Audits are conducted using stored audit information to ensure system integrity and procedural compliance of all procedures related to the DNSSEC signing system.

7.1 Frequency of entity compliance audit

GMO conducts audits at least annually and will conduct more frequent audits in the event of system changes, outages, anomalies or significant staff changes.

7.2 Identity and qualifications of auditor

GMO compliance audits are performed by firms that have a well known proficiency in security and DNSSEC.

7.3 Auditor's relationship to audited party

GMO will appoint an external auditor who is responsible for the audit's implementation.

7.4 Topics covered by audit

Each audit will include a review of events which occurred during a specified audit period. The auditor will ensure that GMO is informed and prepared prior to the audit, including details of the particular topic of the audit.

7.5 Actions taken as a result of deficiency

GMO will take immediately action to resolve deficiencies found by an audit, and consult with well respected firms in the IETF and DNSSEC communities to resolve such found deficiencies.

7.6 Communication of results

Results of each audit will be provided to GMO in a written report no later than 14 days following the completion of the audit.

8 Legal matters

No fees are charged for any function related to DNSSEC. GMO accepts no financial responsibility for security incidents or outages based on its DNSSEC deployments.

Disputes among DNSSEC participants shall be resolved pursuant to provisions in the applicable
agreements among the parties. Parties are not obliged to hand over private key material, but must cooperate by removing or adding DS records as requested by the registrant, regardless of standing of the registrant. DS record management may not be used to enforce financial or other agreements between registrant and registrar.

This DPS shall be governed by the laws of Japan.

Appendix A

1. https://tools.ietf.org/html/draft-ietf-dnsop-dnssec-dps-framework-07
2. https://www.iis.se/docs/se-dnssec-dps-eng.pdf
3. http://cira.ca/knowledge-centre/technology//practice-statement/
4. https://tools.ietf.org/html/rfc1034
5. https://tools.ietf.org/html/rfc1035
6. https://tools.ietf.org/html/rfc4033
7. https://tools.ietf.org/html/rfc4034
8. https://tools.ietf.org/html/rfc4035
9. https://tools.ietf.org/html/rfc5155
10. https://tools.ietf.org/html/rfc5702
11. https://data.iana.org/root-anchors/
12. https://www.iana.org/procedures/root-dnssec-records.html
13. https://tools.ietf.org/html/rfc5910

14. https://data.iana.org/ksk-ceremony/
15. http://tools.ietf.org/html/draft-ietf-dnsop-rfc4641bis