DNSSEC Policy and Practice Statement (DPS)
for .SMART V1
Smart Communications Incorporated
19 February 2015

1
1.1 Introduction Overview

The purpose of this DNSSEC Policy and Practice Statement (DPS) is to document the policies and procedures for the operation of DNSSEC in .SMART TLD. This document conforms to the IETF Internet draft for a DNSSEC Practice Statement, or DPS (see: draft-ietf-dnsop-dnssec-dps-framework-07)

1.2 Document name and identification

Title: DNSSEC Policy and Practice Statement (DPS) for .SMART
Version: 1.0
Date: 19 February 2015

1.3 Community and applicability

Smart Communications, Inc, is the registry for .SMART which it operates for its own exclusive use. The registration of any domain in the registry is restricted to the company and is based on the company's operational needs. The owner and operator of any zone in .SMART is the company. Therefore, there is no intermediary between the child zones and the .SMART parent zone.

1.3.1 Registry

As the registry and sole registrar for the .SMART domain, the company is responsible for all the data related to domain names under .SMART. As such, the company is responsible for signing all such zones and making the public keys available to the general public.

1.3.2 Dependent entities

Users of the .SMART DNSSEC data are responsible for maintaining the appropriate DNSSEC trust anchors and for the configuration of their resolvers and other applications.

1.4 Specification administration

This DPS will be periodically reviewed and updated, as appropriate.

1.4.1 Specification administration organization

SMART Communications, Incorporated

1.4.2

Contact information

ATTN: Domain Manager
Network Services Division
SMART Tower 1
Ayala Avenue, Makati City
PHILIPPINES
1.4.3

Specification change procedures

Modifications to this document must be signed off by the Chief Information Officer. The current version of the DPS will be published at the company website.

2 PUBLICATION AND REPOSITORIES

2.1 Repositories

All DNSSEC-related information will be published at the company TLSsecured website.

2.2 Publication of public keys

The deployed KSKs will be published in the form of DS Resource Record directly to the root zone.

3 OPERATIONAL REQUIREMENTS

3.1 Meaning of domain names

There is no overall policy in the meaning of domain names. However, before registration, each domain name must be vetted by the following departments:

1. the requesting department or business unit
2. the Legal Division
3. the Marketing Division
4. the Network Services Division
5. the office of the Chief Information Officer

3.2 Identification and authentication of child zone manager

The registration of child zones is done by DNS Administrator of the Network Services Division under the supervision of the head of the division. There will be no child zone managers.

3.3 Registration of delegation signer (DS) resource records

The registration of child zones is done by the DNS Administrator of the Network Services Division. The DNS Administrator is responsible for the creation of the DS resource records for the created child zone.

3.4 Method to prove possession of private key

The registration of child zones is done by the DNS Administrator of the Network Services Division. There are no child zone managers except for the DNS Administrator.

3.5
3.5.1 Removal of DS resource records

Who can request removal
-
The head of the department or business unit which requested for a child zone may request for the removal for the DS resource records for that child zone.

3.5.2 Procedure for removal request

The head of the department or business unit which requested for a child zone fills up the necessary request form and submits it to the Network Services Division office for proper action. The Network Services Division verifies the request through e-mail, fax, or a phone to confirm the request and understand the reason for the request.

3.5.3 Emergency removal request

There are no special procedures for emergency removal requests.

4 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS
4.1
4.1.1 Physical controls

Site location and construction

The network facilities of the registry are located in the VITRO Data Center, the first purposely built, industrial strength Internet Data Center (IDC) in the Philippines. It is owned and operated by ePLDT, a subsidiary of the Philippine Long Distance Telephone (PLDT) company, the parent company of SMART Communications, Inc.
In addition to being accredited by the Philippine Economic Zone Authority (PEZA), VITRO has the following international certifications:
1. ISO 9001:2008 Quality Management System
2. ISO 14001:2004 Environmental Management System
3. ISO 27001:2005 Information Security Management System
VITRO is located in Pasig City in the National Capital Region of the Philippines.

4.1.2 Physical access

Physical security mechanisms include security guards, closed circuit TV surveillance video cameras, and intrusion detection systems. The network operations center monitors access to all locations on a 24 x 7 x 365 basis. All employees must present badges to gain entrance, and must them at all times while in the facility. All visitors must register to gain entrance to the data center. Visitors must display visitor badges at all times while they are in the facility, and must be escorted by a Data Center employee. Visitor registration records are maintained for a period of one year.

4.1.3 Power and air conditioning

Server power is drawn from UPS units at 230-volts and have 800-amp and 500-amps distributed through 6 and 4 power panels on average.

5 Backup power supply is from 2 x 800 kva ,3 x 300 kva and 3 x 800 kva secondary UPSes. 5 x 1,500 kva generators are available to supply emergency power with a diesel supply contract and site fuel storage tank capacity. These systems provide the necessary uninterruptible power for the operation of the ventilation and air conditioning systems which control the temperature and relative humidity of the facility.

4.1.4 Water exposures

Systems inside VITRO are protected from water exposure.

4.1.5 Fire prevention and protection

VITRO's fire prevention and protection systems exceed all the local fire safety regulations. VITRO has taken the reasonable precautions to prevent and extinguish fires and protect the systems from damage due to fire or smoke.

4.1.6 Media storage

Media containing sensitive information are stored in a fireproof safe, accessible only to authorized personnel.

4.1.7 Waste disposal

All sensitive documents are shredded before disposal. Media used to store sensitive information are zeroed or rendered physically unreadable before disposal.

4.1.8 Off-site backup

.SMART performs routine backups of its critical systems and data. Aside from the on-site backup, media are also stored off-site in VITRO's disaster recovery facility in Cebu City, Philippines.

4.2
4.2.1 Procedural controls

Trusted roles

The trusted persons in the company are the employees who have access to or control the cryptographic operations which affect the .SMART TLD. These trusted persons include, but are not limited to:

1. DNS Administrators
2. System Administrators
3. Information Security Officers
4. The executives tasked to manage the above persons
5. The Controller, Internal Audit (IA) Head, and Internal Resource Management (IRM) Head

4.2.2 Number of persons required per task

Any task related to the cryptographic operations of the .SMART requires the presence of at least two trusted persons in addition to the Controller, IA Head, or the IRM Head.

4.2.3 Identification and authentication for each role

Physical accesses to the devices are described in Section 4. At the very minimum, company identification cards and written approval from the head of the Technical Services are necessary before physical access to any of the devices is granted.

4.2.4 Tasks requiring separation of duties

The generation, publication, implementation, or destruction of the .SMART DNSSEC keys require the separation of duties.

4.3
4.3.1 Personnel controls Qualifications, experience, and clearance requirements

Candidates to Trusted Persons are required to present proof of the required background, experience, and qualifications for the job. In addition, candidates undergo a thorough screening through behavioral and functional tests and interviews and assessments based on the prescribed qualifications of the role.

4.3.2 Background check procedures

The applicant is required to submit the following documents:
• Medical exam
• National Bureau of Investigation (NBI) clearance
• Clearance from previous employer/ certificate of employment
• Dependents birth certificate
• Marriage certificate (if married)
• Transcript of Records

• Government forms/documents (i.e. Bureau of Internal Revenue, Social Security System,Philippine Health Insurance) These documents are all verified and confirmed with the issuer. The applicant is then subject to a background investigation, using leads from the above documents.

4.3.3 Training requirements

The primary reason for training is to build skills that will help the individual perform his role effectively. Defining the training and learning activities of an employee is one of the primary responsibilities of a line manager/supervisor. The main reference point for nominating and approving a training request is a defined need or skill gap.

Base Training is immediately needed on the job and employee has an identified skill gap. Knowledge and skills to be acquired from the program are useful and directly applicable to the job. Build Employee is given new responsibilities or has transferred functions. Needs to develop certain skills to properly dispense the job Enhance Employee possesses skills needed on the job, performance level is appropriate. Learning is needed on the job for enhancement purposes

4.3.4 Retraining frequency and requirements

SMART provides refresher training for its employees to ensure that each and every employee maintains the basic knowledge and skill to perform the job requirements. The frequency and coverage is determined by the line manager or supervisor.

4.3.5 Job rotation frequency and sequence

The company transfers employees to provide opportunities for career development and support operational exigencies. The transfer of an employee should satisfy the following conditions:

- Manpower vacancy - There is an existing vacancy in a particular team, department, or subsidiary.
- Regular employment status - Only regular employees can request for transfer. Probationary employees cannot apply for transfer except when company initiates the transfer due to operational requirements.
- Duration of residency in current team - For employee-initiated transfer, employee must have at least stayed with the current team for one year prior to request for transfer.
- Transfer to a SMART subsidiary - Employees shall carry over tenure and regular status.
- Eligibility and suitability to the job - The employee satisfies the eligibility and suitability requirements of the job where he shall be transferred.
- Performance appraisal - The employee should have a satisfactory rating and meets expectations from the previous performance appraisal review.
- Pending recommendation for Upgrade and Promotion - Upgrade / promotion recommendation from originating department shall not be automatically carried over to the new assignment. Recommendation shall be reviewed based on new role.

- Disciplinary action - The employee does not have any record of disciplinary action for the last 12 months nor has any pending administrative case with the company.

4.3.6 Sanctions for unauthorized actions

Sanctions may vary and depend on the classification and nature of actions committed.

1. Classification of Offenses
Level 1 Offense is a minor offense characterized by the presence of all of the following circumstances:
(a) There is no malicious, fraudulent or criminal intent;
(b) There is no breach of trust and confidence or serious incompetence;
(c) The act or omission constituting the offense does not result in financial loss or damage to the Company; and
(d) The act or omission contributes to disorderliness in the workplace, results in minor interruption in the business process and/or slightly affects professionalism and the image of the Company.
Level 2 Offense is a violation characterized by the presence of all of the following circumstances:
(a) There is no malicious, fraudulent or criminal intent:
(b) There is no breach of trust and confidence or serious incompetence;
(c) The act or omission involves a failure to exercise due diligence resulting in delay in operations, financial loss and/or unrealized revenues to a degree that is not considered serious; and
(d) The offense contributes to disorderliness in the workplace, results in minor interruption in the business process, affects the image of the Company, compromises health, safety and security of employees and/or creates an occasion for injury.

Even in the absence of the above-described circumstances, repeated commission of a Level One Offense, as herein defined, for more than three (3) times within a continuous period of twelve (12) months shall elevate the offense to a Level 2 Offense for purposes of imposing the penalty.
Level 3 When the act or omission constituting the offense is characterized by any one of the following:
(a) Violation that results in serious financial loss, unrealized revenues, lost opportunities or any other damage or prejudice to the Company;
(b) Malice, fraud or criminal intent;
(c) Willful breach of trust and confidence;
(d) Gross or habitual disregard for established policy or procedure, or serious neglect of assigned responsibilities;
(e) Serious misconduct; Dishonesty in relation to the discharge of ones functions and responsibilities or in dealings with company officers, fellow employees, customers, contractors and vendors;
(f) Serious misrepresentation with respect to ones qualification for employment and/or other required disclosures;
(g) Willful disobedience by the employee of the lawful orders of his superior or the Company in connection with his functions or designated responsibilities; and
(h) Other circumstances similar or analogous to the foregoing.

2. Types of Penalties

- Verbal Reprimand - This is an oral advice given by the Immediate Superior to the employee for the purpose of calling attention to the violation and guiding the employee to better behavior in the future with a reminder that a repetition would merit a more serious penalty in the future.
- Written Reprimand - A Written Reprimand is an admonition in writing addressed to the employee, summarizing the events that led to the imposition of the penalty, stating the basis therefore and reminding the employee that a repetition of the offense shall warrant a stiffer penalty.
- Suspension - Suspension is a forced withdrawal from work and withholding of pay for a designated period, during which time the employee is barred from entering the premises of his team, department or group without the approval of his Immediate Superior.

  The employee shall be served an NOD indicating the exact dates to be covered by the suspension, the offenses for which he is being suspended and the grounds for the imposition of the penalty.

  While the suspension imposed as a penalty is distinct from preventive suspension, as defined in Section 2 (e), the period served in the latter shall be credited to the former. In the event the period of preventive suspension served is in excess of the period of suspension imposed as a penalty, the employee shall be entitled to his/her pay corresponding to the difference in the number of days already served and the period of suspension imposed as a penalty.
- Dismissal - This refers to involuntary termination of employment and the forfeiture of all benefits which the employee would normally be entitled to upon retirement, voluntary resignation or other separation for reasons other than just or authorized causes of termination.
- Restoration/Restitution - Restoration or restitution may be required of the employee independently or together with any other penalty in cases involving financial loss; actual destruction of or damage to company property; theft or fraud from which the employee obtained personal gain; or any other loss resulting from the employees negligence, neglect of duty or deviation from established policies and procedures.

4.3.7 Contracting personnel requirements

Contractors are sourced from the company’s accredited agencies. The accreditation of agencies is via the Vendor Management process. Clauses with agencies include the provision to pre-terminate contractors who are not performing or not in compliance with the policies of the company.

4.3.8 Documentation supplied to personnel

All pertinent information and documents related to employee records, career lattice, role success profile and the like are made available to employees.

4.4
4.4.1 Audit logging procedures
Types of events recorded

The following events are logged, manually or automatically:
1. physical access to the devices
2. remote access to the devices
3. any DNSSEC operation, including but not limited to key generation, rollover, storage, recovery, archiving, and destruction

4.4.2 Frequency of processing log

All logs are examined daily for significant events. Examination of the logs includes the verification of the integrity of the logs. Actions undertaken as a result of a review are documented.

4.4.3 Retention period for audit log information

All audit logs are kept in the system for at least thirty (30) days and then archived off-site for at least three (3) months.

4.4.4 Protection of audit log

All audit logs are digitally signed. Only an authorized trusted person may obtain direct access to a log file.

4.4.5 Audit log backup procedures

Daily incremental back ups are performed for all logs. Full backups are performed weekly.

4.4.6 Audit collection system

The different systems (routers, servers, applications) automatically generate and record audit data. These data are backed up and archived as described in the preceding sections.

4.4.7 Notification to Event-causing Subject

An event may be triggered by a device, an application, or a person. No notice is required to be given to the event-triggering subject.

4.4.8 Vulnerability assessments

All unusual events are analyzed as indicators of potential system vulnerabilities.

4.5
4.5.1 Compromise and disaster recovery
Incident and compromise handling procedures

In the event of a system compromise, the Information Asset and Protection Assurance (IAPA) unit is notified. IAPA will assess the extent and scope of the intrusion on the system level and determine the damage and degree of data corruption using backups of audit data and database records kept in an off-site facility. Restoration of data from backups will be performed. The .SMART Policy board will be informed immediately and an incident report will be forwarded to it.

4.5.2 Corrupted computing resources, software, and/or data

In the event of corruption of computing resources, software, and/or data, the Information Asset and Protection Assurance (IAPA) unit is notified. IAPA will follow its pre-defined recovery procedures for replacing computing resources (in case of hardware failure) or rebuilding/recovering data. If necessary, SMART's disaster recovery procedures will be implemented. This includes a thorough system test to ensure that the rebuilt systems are functioning normally and valid responses are being generated.

4.5.3 Entity private key compromise procedures

In the event of a suspected or known compromise of either the Zone Signing Key (ZSK) or Key Signing Key (KSK), the Information Asset and Protection Assurance (IAPA) unit is notified. IAPA will assess the situation and develop an action plan. The .SMART Policy board will be informed immediately and an incident report will be forwarded to it. IAPA will implement the action plan with the approval of the board. An emergency key roll-over will be performed if necessary.

4.5.4 Business continuity and IT disaster recovery capabilities

In the event of a disaster, SMART will recover all of its services from its Disaster Recovery site backup data center.

4.6 Entity termination

In the event that it becomes necessary to terminate DNSSEC services, SMART will implement its pre-defined procedures which includes dissemination of information to the general public. In the event that it is necessary to transition operations to other parties, SMART will coordinate and cooperate with all concerned parties to effect a secure and seamless transition.

5
5.1 TECHNICAL SECURITY CONTROLS

Key pair generation and installation

DNSSEC is a set of security extensions intended to address security risks within DNS. BlueCat Address Manager supports DNSSEC with the following functions:

- DNSSEC Signing Policies: you can define policies that contain the parameters for creating and managing Zone Signing Keys (ZSKs) and Key Signing Keys (KSKs).
- DNSSEC Key Generation and Rollover Functions: BlueCat Address Manager manages ZSK and KSK generation and rollover automatically, but you can also manually override these functions.
- DNSSEC Deployment Options: where you can enable and configure DNSSEC on managed DDS servers using DNSSEC deployment options. Three deployment options are available to enable DNSSEC, to enable DNSSEC validation, and to create DNSSEC trust anchors.
- DNSSEC Signing Summary report: you can generate a report that lists all signed and unsigned zones in a configuration.*

5.1.1 DNSSEC Signing Policies

Key Generation Ceremonies take place as necessary, pre-scheduled for a key rollover or for unscheduled emergencies. There must be at least 2 Trusted Persons in addition to either the Controller, IA Head, or the IRM Head. For the entire ceremony, there must at least be three trusted persons present. The entire ceremony is logged and signed by all the present individuals.

DNSSEC Signing Policies simplify administration by allowing you to configure DNSSEC settings in one place, and then apply the policy to forward and reverse zones. A DNSSEC Signing Policy contains all of the parameters needed to define the Key Signing Key (KSK) and Zone Signing Key (ZSK) for a zone, including the settings for automatic key rollover.

Administrators can create and managed DNSSEC signing polices from the DNSSEC Policy Management link on the Administration tab. You can create multiple signing policies to create KSKs and ZSKs to meet the unique requirements for each zone, but a zone can only be linked to a single signing policy at any given time.

5.1.2 DNSSEC Key Generation and Rollover Functions

Both the DNS Administrator and System Administrator verify the synchronization of the keys within the entire .SMART DNSSEC system

BlueCat Address Manager normally handles the generation and roll over of DNSSEC keys automatically. BlueCat Address Manager creates Zone Signing Keys (ZSKs) and Key Signing Keys (KSKs) for a zone automatically when you sign the zone. ZSKs and KSKs roll over automatically according to the key parameters in the DNSSEC signing policy.

Both the DNS Administrator and System Administrator verify the synchronization of the keys within the entire .SMART DNSSEC system

5.1.3 Key pair generation

Key Generation Ceremonies take place as necessary, pre-scheduled for a key rollover or for unscheduled emergencies. There must be at least 2 Trusted Persons in addition to either the Controller, IA Head, or the IRM Head. For the entire ceremony, there must at least be three trusted persons present. The entire ceremony is logged and signed by all the present individuals.

5.1.2 Public key delivery

During the signing ceremony, the public pair of the KSKs are verified by the System Administrator and DNS Administrator. The DNS Administrator publishes the DS record to the root zone. Both the DNS Administrator and System Administrator verify the synchronization of the keys within the entire .SMART DNSSEC system.

5.1.3 Public key parameters generation and quality checking

The key parameters, including the lengths, are verified to conform to the Zone Signing Policy (see Section 6).

5.1.4 Key usage purposes

Keys generated for DNSSEC must not be used for any other purposes. Each zone must have its own unique key with no key being reused.

5.2 Private Key protection and cryptographic module engineering controls

All cryptographic-related operations are performed on the BlueCat Address Manager. The private keys are exported from the system in encrypted form for key backups.

5.2.1 Private key (m-of-n) multi-person control

A minimum of three out of five persons are required to be present when the computer is activated.

5.2.2 Private key escrow

Private keys are not escrowed.

5.2.3 Private key backup

Private keys are stored in at least 2 RHCS BlueCat DDS Servers. The procedure for copying the private keys to the backup systems is in accordance with this DPS.

5.2.4 Private key archival

Superseded private keys are not specifically archived although they may be found in the normal backup copies before they were superseded.

5.2.5 Method of activating private key

Private keys are activated by a team consisting of three out five trusted persons.

5.2.6 Method of deactivating private key

The private keys are deactivated when the system is shutdown.

5.2.7 Method of destroying private key

Private keys are not destroyed. When no longer used, they are removed from the DNSSEC system.

5.3
5.3.1 Other aspects of key pair management

Public key archival

All public keys are included in the routine backup and archival process.

5.3.2 Key usage periods

All KSK and ZSK are used until superseded. When superseded, the keys are never reused. KSKs are rolled over when necessary. ZSKs are rolled over every 90 days or as necessary.

5.4
5.4.1 Activation data

Activation data generation and installation

Each trusted person is responsible for generating his own activation data.

5.4.2 Activation data protection

Each trusted person is responsible for the protection of his activation data.

5.5 Computer security controls

Access to the key components of the registry is restricted to the trusted persons. Access is logged.

All passwords must meet the minimum length and form (e.g. alphanumeric, with special characters, etc). They must also be periodically changed.

5.6 Network security controls

The system is compartmentalized into different security zones with access to each zone only through a defined process. The different zones are protected by firewalls. The communication of sensitive information is encrypted.

5.7 Timestamping

The company operates two Strata-1 Time Servers as the company's trusted time sources. All components of the system are synchronized with either one of the two servers. All asserted times are derived from these two servers.

5.8
5.8.1 Life cycle technical controls

System Development Controls

Application development falls under the company's coding and software development standards. The use and modification of open source products falls under the same standards.

5.8.2 System Management Controls

The configuration of each system, installed software, versions, and the like are recorded and monitored through a software management system.

6
6.1 ZONE SIGNING

Key lengths, key types and algorithms

The .SMART KSK key pair(s) is an RSA key pair, with a modulus size of 2048 bits. The .SMART ZSK key pair(s) is an RSA key pair, with a modulus size of 1024 bits.

6.2 Authenticated denial of existence

NSEC3 as defined in RFC 5155 is used to provide the authenticated denial of existence response.

6.3 Signature format

The .SMART zone file is signed using the RSA/SHA-2 digital signature algorithm as defined in RFC 5702.

6.4 Zone Signing Key roll-over

The ZSK lifetime is ninety (90) days.

6.5 Key Signing Key roll-over

Currently, there are no scheduled KSK roll-overs but these will be performed as needed.

6.6 Signature life-time and re-signing frequency

The KSK signatures of the TLD zone DNSKEY RRset will have a validity period of 15 days. The ZSK signatures of the TLD zone authoritative data will have a validity period between 12 and 14 days.

6.7 Verification of zone signing key set

The trusted person will verify the authenticity of the signature data by validating the public key data contained in the KSR.

6.8 Verification of resource records

All record signatures are verified before distribution. The resource records are verified to be conformant to all current standards before publication.

6.9 Resource records time-to-live

The following are the RR and their respective TTLs:
RR
TTL
DS
24 hours
DNSKEY 24 hours
NSEC3
24 hours
RRSIG
inherited from RRset

7COMPLIANCE AUDIT

SMART is required to comply with U.S. Sarbanes-Oxley Act.

7.1 Frequency of entity compliance audit

Audit is done yearly, at the minimum, or as the need arises.

7.2 Identity/qualifications of auditor

The audit is performed by a public accounting firm which is accredited by the American Institute of Certified Public Accountants (AICPA) and demonstrates proficiency in information technology security techniques, tools and practices.

7.3 Auditor's relationship to audited party

The public accounting firm is independent of SMART.

7.4 Topics covered by audit

As part of Sarbanes-Oxley Act, the assessment by the external party is to ensure User Access Management (UAM) is strictly followed by the company. UAM in SMART is being reviewed based on the following:

- Type of access (i.e. physical and logical access)
- Type of account (e.g. administrator, regular user, system account)
- Access privilege to ensure practice of least privilege and segregation of duties
- Frequency of review (e.g. monthly, quarterly)
- Employee movement (e.g. transfer, resignation)

Also included are processes related to the DNSSEC operations including but not limited digital key management and security, infrastructure, and management controls.

7.5 Actions taken as a result of deficiency

Actions taken are based on the severity of the reported deficiencies. The determination of severity is done by the SMART management team in consultation with the auditor. It is also the management team's responsibility to formulate and implement any corrective or remedial actions.

7.6 Communication of results

SMART will communicate the results of the audit and the corrective actions taken (if any) in its corporate website.

8 LEGAL MATTERS

The Registry operates in the Republic of the Philippines and is governed by the laws of the Republic.