

Pre-Delegation Testing

Data Escrow Test Plan

Version F

File name: PDT_DataEscrow_TP.docx

Last saved: 2013-07-01

Copyright (c) 2013 Internet Corporation For Assigned Names and Numbers. All rights reserved.

Document control

Document information and security

| Made by | Responsible for fact | Responsible for document |
|------------------|----------------------|--------------------------|
| Rickard Bellgrim | Rickard Bellgrim | Rickard Bellgrim |

| Security class | File name |
|----------------|------------------------|
| External | PDT_DataEscrow_TP.docx |

Revisions

| Date | Version | Name | Description |
|------------|---------|---------------------|---|
| 2013-01-05 | PA1 | Rickard Bellgrim | Initial document |
| 2013-01-07 | PA2 | Andreas Fredriksson | Add requirements |
| 2013-01-17 | PA3 | Rickard Bellgrim | Continue with test cases |
| 2013-01-20 | PA4 | Rickard Bellgrim | Updates after external review |
| 2013-01-22 | PA5 | Rickard Bellgrim | Updates after external review |
| 2013-01-24 | PA6 | Rickard Bellgrim | Add picture and text updates |
| 2013-02-06 | PA7 | Rickard Bellgrim | Add Document Hierarchy and final chapters |
| 2013-02-07 | PA8 | Rickard Bellgrim | Updated requirements |
| 2013-03-22 | PB1 | Rickard Bellgrim | Added Note 2 in 2.1.1 Added Note 1 in 2.1.3 Moved and updated test case Data Escrow Profile |
| 2013-04-08 | B | Staffan Hagnell | Delivery D2 for production |
| 2013-04-17 | PC1 | Rickard Bellgrim | Changed Note 1 in 2.1.3. Now all deposits are using tar archive. Removed extension ryde-csv.tar. Added Note 3 in 2.1.3. Case insensitive. |
| 2013-04-19 | C | Mats Dufberg | Release. |
| 2013-04-29 | PD1 | Rickard Bellgrim | Changes from ICANN: <ul style="list-style-type: none">• Updated external references• Updated specification 2• Removed Note 1 in 2.1.3 |
| 2013-05-03 | D | Amar Andersson | Released |
| 2013-05-08 | PE1 | Rickard Bellgrim | Changes from ICANN: <ul style="list-style-type: none">• Updated Note 1 in 2.1.1• Updated REG2.1 |
| 2013-06-04 | E | Mats Dufberg | Released |
| 2013-06-24 | PF1 | Rickard Bellgrim | Handle the data escrow profile differently |
| 2013-07-01 | F | Mats Dufberg | Released. |

LIST OF CONTENTS

| | |
|---|-----------|
| 1. INTRODUCTION..... | 4 |
| 1.1 SCOPE..... | 4 |
| 1.2 REFERENCES | 4 |
| 1.2.1 <i>External</i> | 4 |
| 1.2.2 <i>Internal</i> | 4 |
| 1.2.3 <i>Document Hierarchy</i> | 4 |
| 1.3 LEVEL IN THE OVERALL SEQUENCE..... | 4 |
| 1.4 TEST CLASSES AND OVERALL TEST CONDITIONS | 4 |
| 2. DETAILS FOR THIS LEVEL OF TEST PLAN..... | 5 |
| 2.1 TEST ITEMS AND THEIR IDENTIFIERS..... | 5 |
| 2.1.1 <i>Statement of Work</i> | 5 |
| 2.1.2 <i>Applicant Guidebook</i> | 5 |
| 2.1.3 <i>Specification 2</i> | 6 |
| 2.1.4 <i>Algorithms</i> | 7 |
| 2.2 TEST TRACEABILITY MATRIX | 8 |
| 2.3 FEATURES TO BE TESTED..... | 8 |
| 2.4 FEATURES NOT TO BE TESTED..... | 8 |
| 2.5 APPROACH..... | 8 |
| 2.6 ITEM PASS/FAIL CRITERIA | 9 |
| 2.7 SUSPENSION CRITERIA AND RESUMPTION REQUIREMENTS | 9 |
| 2.8 TEST DELIVERABLES | 9 |
| 3. TEST MANAGEMENT | 10 |
| 4. GENERAL | 11 |
| 4.1 GLOSSARY..... | 11 |
| 4.2 DOCUMENT CHANGE PROCEDURES..... | 11 |

1. Introduction

This Level Test Plan focuses on the Data Escrow functionality of the new gTLDs.

1.1 Scope

The Pre-Delegation Testing Provider will validate the format of the data escrow deposit as provided by the applicant.

1.2 References

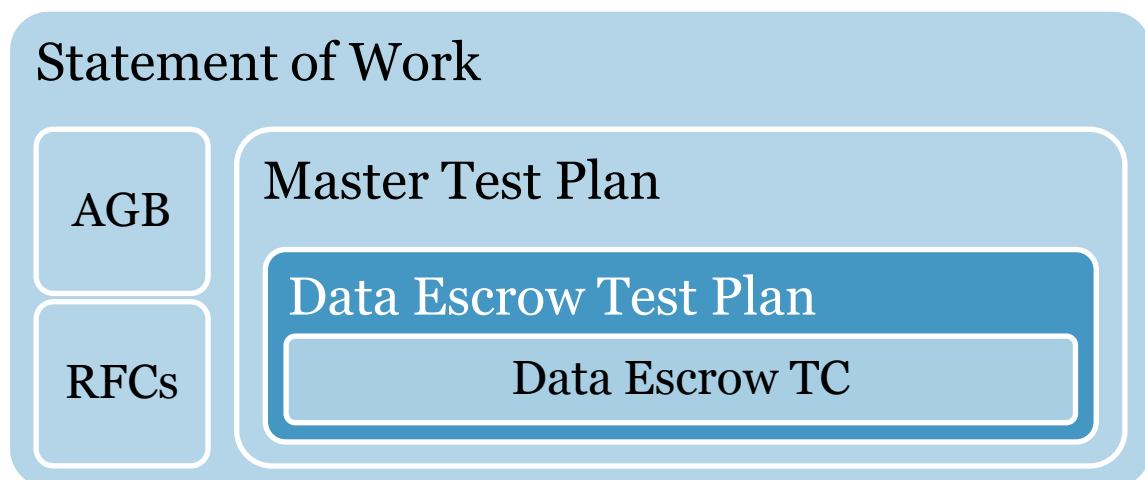
1.2.1 External

- IEEE 829-2008
- ICANN gTLD Applicant Guidebook, Version 2012-06-04
- <http://tools.ietf.org/html/draft-arias-noguchi-registry-data-escrow>
- <http://tools.ietf.org/html/draft-arias-noguchi-dnrd-objects-mapping>
- <http://tools.ietf.org/html/draft-gould-thippeswamy-dnrd-csv-mapping>

1.2.2 Internal

- Pre-Delegation Testing, Statement of Work
- Pre-Delegation Testing, Master Test Plan
- Pre-Delegation Testing, Documentation Test Plan
- Pre-Delegation Testing, Data Escrow Test Cases

1.2.3 Document Hierarchy



1.3 Level in the overall sequence

This Test Plan and the associated Test Cases can be run in parallel with the other Level Test Plans.

1.4 Test classes and overall test conditions

Both full and incremental deposits of sample data will be tested with positive test cases.

2. Details for this level of test plan

2.1 Test items and their identifiers

2.1.1 Statement of Work

The main requirements for testing data escrow are found in the Statement of Work:

- [R21]** Validate the format of one full and one incremental data escrow deposit as provided by the applicant for compliance with the New gTLD Registry Agreement Specification 2 – *Data Escrow Requirements* set forth in Module 5 of the AGB.
- [R22]** Verify that the applicant's data escrow profile is in compliance with section 3 of the New gTLD Registry Agreement Specification 2 – *Data Escrow Requirements* set forth in Module 5 of the AGB.

Requirements [R23] and [R24] in the Statement of Work are also about Data Escrow, but they are only about document reviewing and are handled by the Documentation Test Plan. They are thus not included in this test plan.

Note 1: In contrary with the requirements, ICANN are now allowing applicants to only deliver full data escrow deposits each time. Incremental files will thus be tested only if the applicant delivers such files to the PDT Provider.

Note 2: The PDT Provider shall validate the deposit against an archive of ICANN approved data escrow schemas. Requirement [R22] is thus more about checking that the applicant is using XML schemas which have been agreed upon with ICANN.

2.1.2 Applicant Guidebook

Section 5.2 of the AGB states the following requirements:

Escrow deposit -- The applicant-provided samples of data deposit that include both a full and an incremental deposit showing correct type and formatting of content will be reviewed. Special attention will be given to the agreement with the escrow provider to ensure that escrowed data can be released within 24 hours should it be necessary. ICANN may, at its option, ask an independent third party to demonstrate the reconstitutability of the registry from escrowed data. ICANN may elect to test the data release process with the escrow agent.

The following requirements have been identified from the text above. Note that the requirements on the data escrow agreement are handled by the Documentation Test Plan, as mentioned in 2.1.1.

- {AGB1}** One full deposit of sample data **MUST** be tested
- {AGB2}** One differential deposit of sample data deposit **MUST** be tested

Note 1: The word “differential” is used in the requirement above and not “incremental”. This is because specification 2 uses this term.

2.1.3 Specification 2

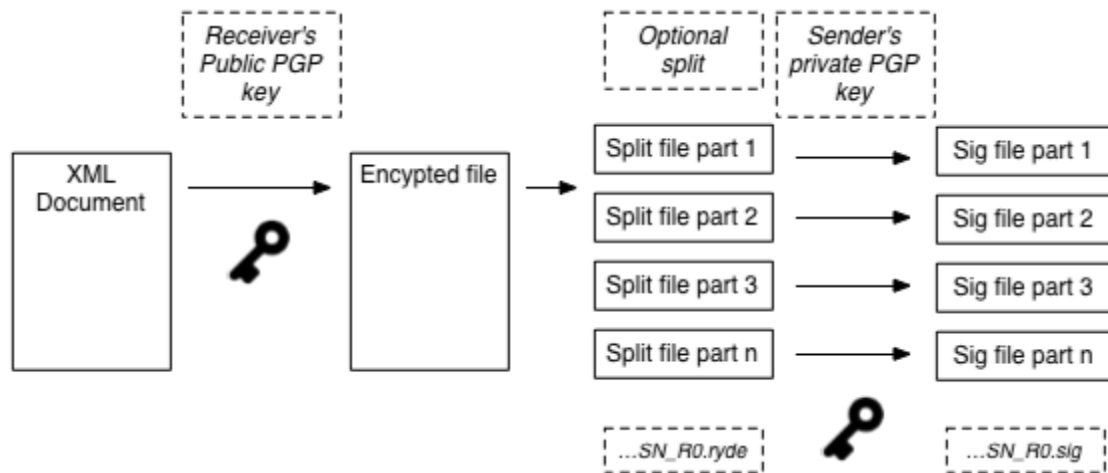
Specification 2 of the registry agreement will not be fully cited here, but a number of requirements have been identified.

- [REG1] Acceptable algorithms for Public-key cryptography, Symmetric-key cryptography, Hash and Compression are those enumerated in RFC 4880, not marked as deprecated in OpenPGP IANA Registry, that are also royalty-free.
- [REG2] Escrow format:
 - [REG2.1] Registry objects, such as domains, contacts, name servers, registrars, etc. **MUST** be compiled into a file constructed as described in draft-arias-noguchi-dnrd-objects-mapping and draft-gould-thippeswamy-dnrd-csv-mapping (if using CSV, once the merged XML and CSV draft is published, draft-arias-noguchi-dnrd-objects-mapping will be the only reference).
 - [REG2.2] Registry Operator **MUST** use the draft versions available at the time of signing the Agreement, if not already an RFC. Once the specification is published as an RFC, Registry Operator **MUST** implement that specification, no later than 180 days after.
 - [REG2.3] UTF-8 character encoding **MUST** be used.
 - [REG2.4] If a Registry Operator offers additional Registry Services that require submission of additional data, not included above, additional “extension schemas” **MUST** be defined in a case by case base to represent that data. These “extension schemas” **MUST** be specified as described in the drafts.
- [REG3] Processing of files:
 - [REG3.1] The XML **MUST** be named as the containing file but with the extension xml.
 - [REG3.2] The data file(s) **MUST** be aggregated in a tarball file named as the deposit but with the extension tar.
 - [REG3.3] The tarball file **SHOULD** be compressed using ZIP as per RFC 4880.
 - [REG3.4] The (compressed) file **MUST** be encrypted using the escrow agent’s public key, using the suggested algorithms in Specification 2.
 - [REG3.5] The encrypted file **MAY** be split into smaller files.
 - [REG3.6] The file(s) **MUST** be signed using the Registry’s private key, using the suggested algorithms in Specification 2.
 - [REG3.7] The digital signature file(s) **MUST** be in binary OpenPGP format as per RFC 4880.
 - [REG3.8] The processed files and digital signature files **MUST** be transferred to the Escrow Agent through secure electronic mechanisms.
 - [REG3.9] The Escrow Agent **MUST** validate every transferred data file according to [REG6].
- [REG4] Files **MUST** be named according to the following convention:
{gTLD}_{YYYY-MM-DD}_{type}_S{#}_R{rev}.{ext}
- [REG5] Distribution of public keys:
 - [REG5.1] Each of Registry Operator and Escrow Agent **MUST** distribute its public key to the other party via email to an email address to be specified.
 - [REG5.2] Each party will confirm receipt of the other party's public key with a reply email, and the distributing party will subsequently reconfirm the authenticity of the key transmitted via offline methods.
- [REG6] Verification procedure:
 - [REG6.1] The signature file of each processed file **MUST** be validated.
 - [REG6.2] If processed files are pieces of a bigger file, the latter **MUST** be put together.
 - [REG6.3] Each file obtained in the previous step **MUST** be decrypted and uncompressed.
 - [REG6.4] Each data file contained in the previous step **MUST** be validated against the format defined in the drafts.

Note 1: [REG5] will not be tested, see section .

Note 2: [REG4] is case insensitive.

Processing of files can be illustrated by this picture. The verification procedure is the reverse of this process.



2.1.4 Algorithms

RFC 4880 enumerates a number of algorithms used for Public-key cryptography, Symmetric-key cryptography, Hash and Compression. The algorithm must not be marked as deprecated in OpenPGP IANA Registry and must also be royalty-free.

- {ALGO1} Public-key cryptography
- {ALGO1.1} RSA used both for signing and encryption. RFC 4880 says that RSA Encrypt-Only and RSA Sign-Only are deprecated.
- {ALGO1.2} DSA for signatures and Elgamal for encryption.
- {ALGO1.3} ECDSA for signatures and ECDH for encryption. RFC 4880 has reserved code points for this. The full specification is in RFC 6637.
- {ALGO2} Symmetric-key cryptography: IDEA, TripleDES, CAST5, Blowfish, AES128, AES192, AES256, or Twofish.
- {ALGO3} Hash: SHA1, RIPEMD160, SHA224, SHA256, SHA384, or SHA512.
- {ALGO3.1} MD5 is marked as deprecated in the IANA Registry and MUST not be used.
- {ALGO4} Compression: ZIP, ZLIB, or BZip2.

Note 1: IDEA was patented in some countries, but they have now expired.

2.2 Test Traceability Matrix

| Test ID | Description | Requirement Point |
|--------------------------|--|--|
| Data Escrow File Name 01 | Receive one full deposit of sample data. Verify file names. | [R21], [AGB1], [REG4] |
| Data Escrow File Name 02 | Receive one differential deposit of sample data. Verify file names. | [R21], [AGB2], [REG4] |
| Data Escrow Verify 01 | Verify signature of files for full deposit. Put split files together. Decrypt and uncompress file. | [R21], [AGB1], [REG3], [REG6.1], [REG6.2], [REG6.3], [ALGO] |
| Data Escrow Verify 02 | Verify signature of files for differential deposit. Put split files together. Decrypt and uncompress file. | [R21], [AGB2], [REG3], [REG6.1], [REG6.2], [REG6.3], [ALGO] |
| Data Escrow Content 01 | Validate the full deposit against the profile provided by ICANN. | [R21], [R22], [AGB1], [REG2], [REG6.4] |
| Data Escrow Content 02 | Validate the differential deposit against the profile provided by ICANN. | [R21], [R22], [AGB2], [REG2], [REG6.4] |

2.3 Features to be tested

- File names
- Processing of files
- Escrow profile
- Escrow format

2.4 Features not to be tested

It has been decided not to do a proper public key distribution with offline verification methods, as described in [REG5]. The tests are performed on dummy data and are thus not considered sensitive. Also, this will simplify the testing process. The applicant can get the public key from a public website.

The reconstitutability of the registry from escrowed data will not be tested.

2.5 Approach

The applicant must at least deliver full deposits of sample data including signature files and the public PGP key of the applicant. Encryption must be done using the public key provided by the Pre-Delegation Testing System. The applicant must deliver the differential files, if they are supporting this functionality.

The Test Officer will verify the files and their contents using manual inspection together with support tools and scripts.

The data escrow draft is still under development, which will impact this test plan and test cases. The test plan and test cases will be updated to match the current draft. However, multiple versions are needed to be supported.

ICANN will provide the XML schemas for any approved extensions made by the applicant. This is what the deposit is validated against.

ICANN may also elect to test the release process with the escrow agent. This is however described in a separate document because it is an extra service outside the normal pre-delegation testing.

2.6 Item pass/fail criteria

The test will fail if the test item does not follow the requirement for each step in the procedure.

2.7 Suspension criteria and resumption requirements

The test cases need to run in the correct order, because the outcome from one test is used in the following test. If a test fails then no other cases will be run.

2.8 Test deliverables

The Data Escrow test level will produce:

- Level Test Logs (LTL)
- Anomaly Report (AR) in case of error
- Level Test Report (LTR)

3. Test management

The goal of these documents is to describe the test cases and how the new gTLDs are tested. This is just a part of a larger project and defining test management is not part of this subproject. However, some information can be found in the Master Test Plan.

4. General

4.1 Glossary

The glossary is available in the Master Test Plan.

4.2 Document change procedures

Document change procedures are documented in the Master Test Plan.