

Pre-Delegation Testing

Escrow Release Test Plan

Version G

File name: PDT_EscrowRelease_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_EscrowRelease_TP.docx

Revisions

Date	Version	Name	Description
2013-03-05	PA1	Rickard Bellgrim	Initial document
2013-03-08	PA2	Rickard Bellgrim	Clarify the approach
2013-03-11	PA3	Staffan Hagnell	Review text
2013-04-03	PA4	Rickard Bellgrim	Added Note 1 and Note 2 in 2.1.3 Added Note 1 in 2.1.5 Remove test cases for profile validation Renamed test cases
2013-04-08	B	Staffan Hagnell	Delivery D2 for production
2013-04-15	PC1	Rickard Bellgrim	Removed Note 2 in 2.1.3, the deposit will be validated against the schemas. Added Note 2 in 2.1.3, ICANN will do the key exchange. I2 – ICANN will do the key exchange. I3 – The tests will be performed on request by ICANN. I9 – ICANN will decrypt the deposit. I10- Files are exchanged via a shared drive. Added test case for profile validation. Adjusted the approach.
2013-04-17	PC2	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.
2013-04-18	PC3	Rickard Bellgrim	Added Note 2 in 2.1.4.
2013-04-19	C	Mats Dufberg	Released.
2013-04-24	PD1	Rickard Bellgrim	Adjust Release Request to UTC
2013-04-24	D	Mats Dufberg	Released.
2013-04-29	PE1	Rickard Bellgrim	Changes from ICANN: <ul style="list-style-type: none">• Updated external references• Updated specification 2• Removed Note 1 in 2.1.3• Updated Note 2 in 2.1.4
2013-05-03	E	Amar Andersson	Released
2013-05-08	PF1	Rickard Bellgrim	Changes from ICANN: <ul style="list-style-type: none">• Updated REG2.1
2013-06-04	F	Mats Dufberg	Released
2013-06-24	PG1	Rickard Bellgrim	Handle the data escrow profile differently

Date	Version	Name	Description
2013-07-01	G	Mats Dufberg	Released.

LIST OF CONTENTS

1. INTRODUCTION.....	5
1.1 SCOPE.....	5
1.2 REFERENCES	5
1.2.1 <i>External</i>	5
1.2.2 <i>Internal</i>	5
1.2.3 <i>Document Hierarchy</i>	5
1.3 LEVEL IN THE OVERALL SEQUENCE.....	5
1.4 TEST CLASSES AND OVERALL TEST CONDITIONS	5
2. DETAILS FOR THIS LEVEL OF TEST PLAN.....	6
2.1 TEST ITEMS AND THEIR IDENTIFIERS.....	6
2.1.1 <i>Statement of Work</i>	6
2.1.2 <i>Applicant Guidebook</i>	6
2.1.3 <i>Specification 2</i>	7
2.1.4 <i>Algorithms</i>	8
2.1.5 <i>ICANN</i>	9
2.2 TEST TRACEABILITY MATRIX	10
2.3 FEATURES TO BE TESTED.....	10
2.4 FEATURES NOT TO BE TESTED.....	10
2.5 APPROACH.....	11
2.6 ITEM PASS/FAIL CRITERIA	11
2.7 SUSPENSION CRITERIA AND RESUMPTION REQUIREMENTS	11
2.8 TEST DELIVERABLES	11
3. TEST MANAGEMENT	12
4. GENERAL	13
4.1 GLOSSARY.....	13
4.2 DOCUMENT CHANGE PROCEDURES.....	13

1. Introduction

This Test Plan focuses on the data release process with the escrow agent.

1.1 Scope

The Pre-Delegation Testing Provider will validate if the escrow agent, upon a request, can release data within 24 hours. The received data will be validated against the requirements given by ICANN in the Applicant Guidebook.

1.2 References

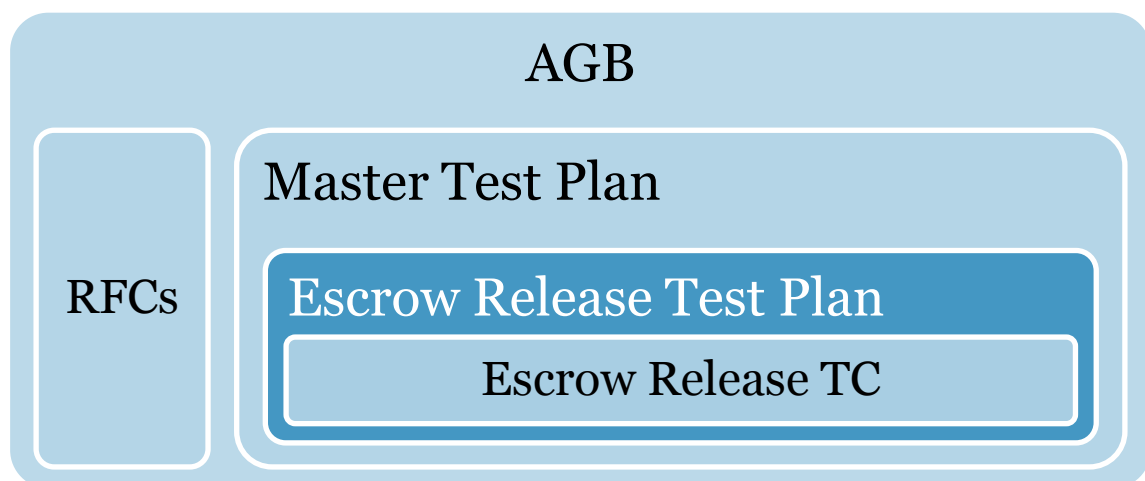
1.2.1 External

- 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 are only executed if requested by ICANN. It must however be executed after the EPP tests in order to validate if data from the registry is pushed to the escrow agent.

1.4 Test classes and overall test conditions

One full deposit and any differential deposits of 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 requirement for testing the escrow agent is found in the Statement of Work:

“ICANN may also elect to have the Pre-Delegation Testing Provider verify the data escrow release process.”

It is not part of the overall test requirements on a gTLD, but is an extra option for ICANN to request this during the pre-delegation testing.

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.

[AGB1] Escrowed data **MUST** be released within 24 hours, if requested by ICANN.

Note 1: The requirements on the sample data are handled by the Data Escrow Test Plan. Also, the test for reconstitutability is out of scope.

2.1.3 Specification 2

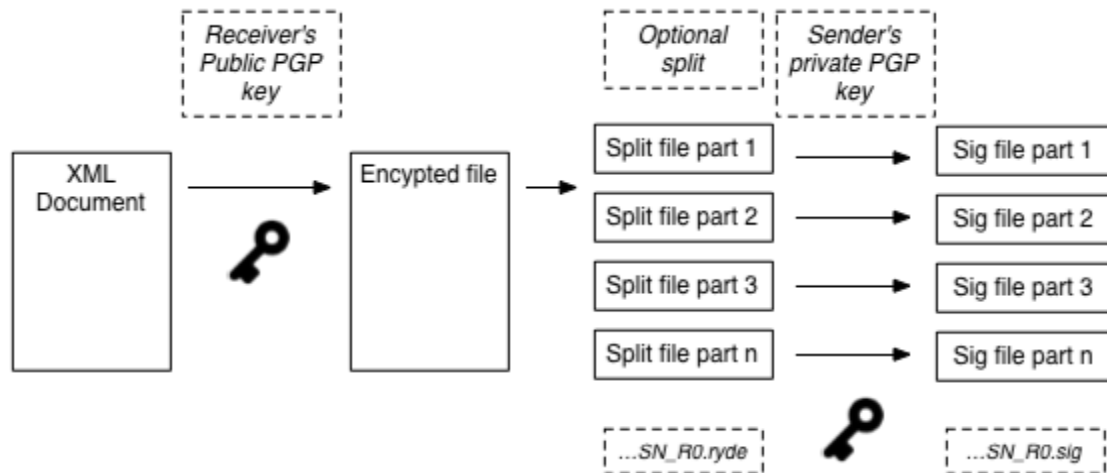
Specification 2 of the registry agreement will not be fully cited here, but a number of requirements have been identified.

- [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: As required in 2.1.5, ICANN will do the key exchange and not the PDT Provider. [REG5] is thus not part of the tests.

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.

Note 2: The PDT Provider cannot check directly what symmetric algorithm is used in the deposit. That is because this particular OpenPGP information is encrypted using ICANN's public key. ICANN must make a note on what symmetric algorithm was used by the data escrow agent.

2.1.5 ICANN

ICANN has some additional requirements on the test and release process.

- [I1] Once a data escrow agent is approved, ICANN will provide the PDT Provider: numeric authentication code, name of the data escrow agent, time zone of the data escrow agent and phone number.
- [I2] ICANN will exchange keys with the data escrow agent following the procedures given in specification 2 of the registry agreement.
- [I3] ICANN MAY elect to test a data escrow agent in combination with an applicant. This will be signaled in the test schedule delivered by ICANN.
- [I4] The data escrow agent MUST be able to receive data release requests regardless of time or day.
- [I5] The objective is to test that the data escrow agent can release a deposit during the weekend (worst case scenario). The PDT Provider will know the time zone of the escrow agent to decide the best time frame (Sunday between 10.00 and 16.00 UTC) to run the test).
- [I6] The PDT Provider MUST authenticate themselves using the numeric authentication code, and inform the data escrow agent of the email address they shall send a notification to when the deposit is available for download.
- [I7] The data escrow deposit MUST be validated against the requirements given in specification 2 of the registry agreement.
- [I8] The data escrow deposit MUST contain information from the EPP tests performed previously during the testing week.
- [I9] The deposit MUST be sent from the PDT Provider to ICANN for decryption, since they are the intended recipient.
- [I10] ICANN and the PDT Provider MUST exchange files via a shared drive.

Note 1: Since the test is initiated on a Sunday, it may be the case that the Escrow Agent has not received the latest full deposit and thus have to release e.g. one full deposit and six differential deposits.

2.2 Test Traceability Matrix

Test ID	Description	Requirement Point
Escrow Release Request	Request the release of a data escrow deposit.	[AGB1], [I1], [I3], [I4], [I5], [I6]
Escrow Release File Name	Verify file names of the deposit.	[I7], [REG4]
Escrow Release Verify	PDT Provider: <ul style="list-style-type: none">• Check for valid algorithms• Check that all files are present ICANN: <ul style="list-style-type: none">• Verify the signatures of the deposit.• Put split files together.• Decrypt and uncompress file.	[I7], [I9], [I10], [REG1], [REG3], [REG6.1], [REG6.2], [REG6.3], [ALGO]
Escrow Release Content	Validate the deposit against the profile provided by ICANN. Check that the deposit contains information created by the EPP tests.	[I8], [REG2], [REG6.4]

2.3 Features to be tested

- Release process
- File names
- Processing of files
- Escrow profile
- Escrow format
- Escrow data sent from registry operator to escrow agent

2.4 Features not to be tested

- Public key exchange will be performed by ICANN.
- The reconstitutability of the registry from escrowed data will not be tested.

2.5 Approach

ICANN will handle the public key exchange with the Escrow Agent. Signature verification and decryption must thus be handled via ICANN as a proxy.

The Escrow Agent must, upon request, make a full deposit of data, including signature, available for download (e.g. HTTPS or SFTP) within 24 hours. Encryption must be done using the public key provided by ICANN. It may be the case that the Escrow Agent releases one full deposit and multiple differential deposits.

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 of the draft 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.

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.