

Pre-Delegation Testing

Escrow Release Test Cases

Version F

File name: PDT_EscrowRelease_TC.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_TC.docx

Revisions

Date	Version	Name	Description
2013-03-08	PA1	Rickard Bellgrim	Initial document
2013-03-08	PA2	Rickard Bellgrim	Notify that the deposit has been downloaded
2013-03-11	PA3	Rickard Bellgrim	Add email address
2013-03-11	PA4	Staffan Hagnell	Review text
2013-04-03	PA5	Rickard Bellgrim	Updated text after comments from ICANN
2013-04-03	PA6	Rickard Bellgrim	Removed test case for data escrow profile. Differential deposits may now also be supplied to the tests.
2013-04-08	B	Staffan Hagnell	Delivery D2 for production
2013-04-15	PC1	Rickard Bellgrim	Deleted test case EscrowReleaseKeyExchange Adjusted test case EscrowReleaseVerify Added test case EscrowReleaseProfile Adjusted test case EscrowReleaseContent
2013-04-17	PC2	Rickard Bellgrim	File names are case insensitive. Removed .ryde-csv.tar as an extension. All deposits are now a tar archive.
2013-04-18	PC3	Rickard Bellgrim	Cannot check the symmetric algorithm. That OpenPGP information is encrypted and ICANN is the one with the private key.
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 Check file names on tarball and XML
2013-05-03	E	Mats Dufberg	Released
2013-06-12	PF1	Rickard Bellgrim	Clarified the test description for each test case.
2013-06-24	PF2	Rickard Bellgrim	Clarified pass/fail criteria. Removed test case EscrowReleaseProfile. Now part of EscrowReleaseContent01.
2013-07-01	F	Mats Dufberg	Released.

LIST OF CONTENTS

1. INTRODUCTION	4
1.1 SCOPE.....	4
1.2 REFERENCES	4
1.2.1 External	4
1.2.2 Internal	4
1.2.3 Document Hierarchy	4
1.3 CONTEXT	4
1.4 NOTATION FOR DESCRIPTION	4
2. ESCROW RELEASE REQUEST.....	5
2.1 TEST CASE IDENTIFIER	5
2.2 OBJECTIVE.....	5
2.3 INPUTS	5
2.4 OUTCOME(S)	5
2.5 ENVIRONMENTAL NEEDS	5
2.6 SPECIAL PROCEDURAL REQUIREMENTS	5
2.7 INTERCASE DEPENDENCIES	5
2.8 ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE	6
3. ESCROW RELEASE FILE NAME	7
3.1 TEST CASE IDENTIFIER	7
3.2 OBJECTIVE.....	7
3.3 INPUTS	7
3.4 OUTCOME(S)	7
3.5 ENVIRONMENTAL NEEDS	7
3.6 SPECIAL PROCEDURAL REQUIREMENTS	7
3.7 INTERCASE DEPENDENCIES	7
3.8 ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE	8
4. ESCROW RELEASE VERIFY	9
4.1 TEST CASE IDENTIFIER	9
4.2 OBJECTIVE.....	9
4.3 INPUTS	9
4.4 OUTCOME(S)	9
4.5 ENVIRONMENTAL NEEDS	9
4.6 SPECIAL PROCEDURAL REQUIREMENTS	9
4.7 INTERCASE DEPENDENCIES	9
4.8 ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE	10
5. ESCROW RELEASE CONTENT	11
5.1 TEST CASE IDENTIFIER	11
5.2 OBJECTIVE.....	11
5.3 INPUTS	11
5.4 OUTCOME(S)	11
5.5 ENVIRONMENTAL NEEDS	11
5.6 SPECIAL PROCEDURAL REQUIREMENTS	11
5.7 INTERCASE DEPENDENCIES	11
5.8 ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE	11
6. GLOBAL.....	12
6.1 GLOSSARY.....	12
6.2 DOCUMENT CHANGE PROCEDURES.....	12

1. Introduction

1.1 Scope

All of the test cases for the escrow release can be found in this document. The 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.

1.2 References

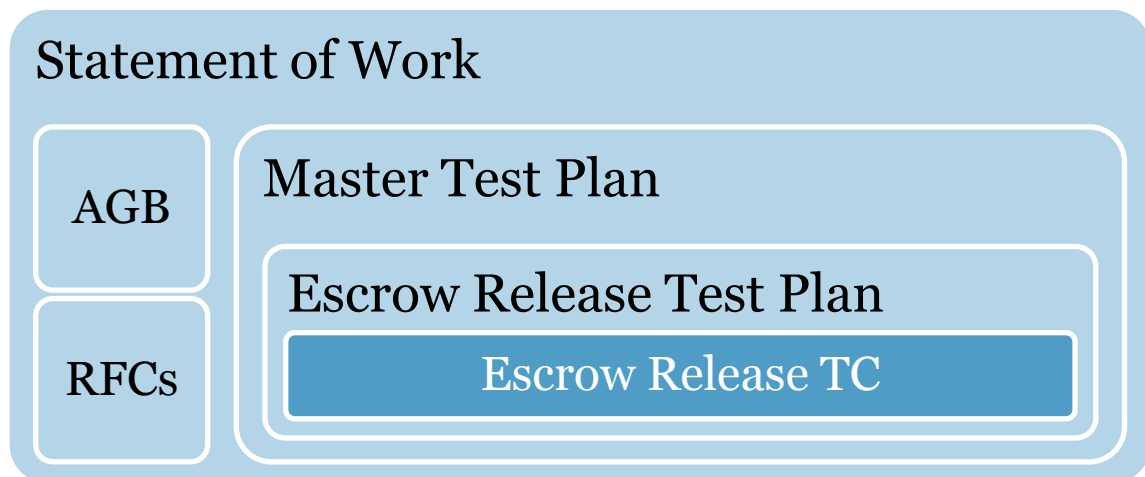
1.2.1 External

- 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, Escrow Release Test Plan

1.2.3 Document Hierarchy



1.3 Context

All tests are performed locally in the test environment.

1.4 Notation for description

Each test case for the escrow release is described in their own chapter. The test procedures are described directly in the test case.

2. Escrow Release Request

2.1 Test case identifier

EscrowReleaseRequest

2.2 Objective

The test will request the release of a data escrow deposit.

Requirements from the test plan: [AGB1], [I3], [I4], [I5], [I6]

2.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
TLD	The ASCII compatible name of the TLD	String
EscrowName	Name of the data escrow agent	String
EscrowPhone	Phone number to the data escrow agent	String
EscrowTimeZone	Time zone of the data escrow agent	String
EscrowCode	Numeric authentication code	String

Once a data escrow agent is approved, ICANN will provide this input data.

2.4 Outcome(s)

The requested data was available for download within 24 hours. The files are used as input for the following test cases.

2.5 Environmental needs

This test has no environmental needs.

2.6 Special procedural requirements

The purpose is to test that the 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.

2.7 Intercase dependencies

ICANN must have distributed their public key to the escrow agent.

2.8 Ordered description of steps to be taken to execute the test case

1. Decide when the release request shall be made.
2. At the given time, call the Escrow Agent using the telephone number <EscrowPhone>.
 - a. Authenticate as the Pre-Delegation Testing Provider using the <EscrowCode>.
 - b. Request the release of a data escrow for the given TLD.
 - c. Inform the Escrow Agent of the email address where they shall send a notification when the data escrow deposit is ready for download (HTTPS or SFTP), pdt@iis.se
3. The notification **MUST** be received within 24 hours.
4. Download and verify that deposit is complete. The following files **MUST** be present:
 - a. One or more encrypted deposit files
 - b. One or more signature files
5. Reply to the Escrow Agent that the deposit has been downloaded.

3. Escrow Release File Name

3.1 Test case identifier

EscrowReleaseFileName

3.2 Objective

The test will receive one full deposit of data and optionally one or more differential deposits. The objective is to verify the file names.

Requirements from the test plan: [I7], [REG4]

3.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
TLD	The ASCII compatible name of the TLD	String
EscrowFileFull-[1..n]	The files containing the full deposit	Files
EscrowSigFull-[1..n]	The files containing the signature	Files
EscrowFileDiff[0..n]-[1..n]	Optional files containing differential deposits	Files
EscrowSigDiff[0..n]-[1..n]	Optional files containing the signature	Files

Input data comes from the test EscrowReleaseRequest.

3.4 Outcome(s)

Files **MUST** be named according to the following convention:

{gTLD}_{YYYY-MM-DD}_{type}_S{#}_R{rev}.{ext}

3.5 Environmental needs

This test has no environmental needs.

3.6 Special procedural requirements

This test has no special procedural requirements.

3.7 Intercase dependencies

EscrowReleaseRequest must first have been executed successfully.

3.8 Ordered description of steps to be taken to execute the test case

All of the checks are case insensitive.

The files **MUST** follow this format {gTLD}_{YYYY-MM-DD}_{type}_S{#}_R{rev}.{ext}

For each <EscrowFileFull>, check that:

1. {gTLD} is equal to <TLD>. If it is an IDN-TLD, then this **MUST** be the A-label.
2. {YYYY-MM-DD} is equal to year, month, and day.
3. {type} is equal to "full".
4. {#} is a number greater than or equal to 1. Leading zeroes are not allowed.
5. {rev} is a number greater than or equal to 0. Leading zeroes are not allowed.
6. {ext} is equal to "ryde".

For each <EscrowFileDiff>, check that:

1. {gTLD} is equal to <TLD>. If it is an IDN-TLD, then this **MUST** be the A-label.
2. {YYYY-MM-DD} is equal to year, month, and day.
3. {type} is equal to "diff".
4. {#} is a number greater than or equal to 1. Leading zeroes are not allowed.
5. {rev} is a number greater than or equal to 0. Leading zeroes are not allowed.
6. {ext} is equal to "ryde".

For each <EscrowSigFull>, check that:

1. {gTLD} is equal to <TLD>. If it is an IDN-TLD, then this **MUST** be the A-label.
2. {YYYY-MM-DD} is equal to year, month, and day.
3. {type} is equal to "full".
4. {#} is a number greater than or equal to 1. Leading zeroes are not allowed.
5. {rev} is a number greater than or equal to 0. Leading zeroes are not allowed.
6. {ext} is equal to "sig".

For each <EscrowSigDiff>, check that:

1. {gTLD} is equal to <TLD>. If it is an IDN-TLD, then this **MUST** be the A-label.
2. {YYYY-MM-DD} is equal to year, month, and day.
3. {type} is equal to "diff".
4. {#} is a number greater than or equal to 1. Leading zeroes are not allowed.
5. {rev} is a number greater than or equal to 0. Leading zeroes are not allowed.
6. {ext} is equal to "sig".

4. Escrow Release Verify

4.1 Test case identifier

EscrowReleaseVerify

4.2 Objective

The test will check that valid algorithms are used and that all files are present. ICANN will perform signature verification and decryption.

Requirements from the test plan: [I7], [I9], [I10], [REG1], [REG3], [REG6.1], [REG6.2], [REG6.3], [ALGO]

4.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
EscrowFileFull-[1..n]	The files containing the full deposit	Files
EscrowSigFull-[1..n]	The files containing the signature	Files
EscrowFileDiff[0..n]-[1..n]	Optional files containing differential deposits	Files
EscrowSigDiff[0..n]-[1..n]	Optional files containing the signature	Files

Input data comes from the EscrowReleaseRequest.

4.4 Outcome(s)

- The signature, encryption, and compression are done in accordance with RFC 4880.
- The files **MUST** be signed using RSA, DSA, or ECDSA with SHA1, RIPEMD160, SHA224, SHA256, SHA384, or SHA512.
- If multi-part files, then all files **MUST** be present.
- The files **MUST** be encrypted using RSA, Elgamal, or ECDH with IDEA, TripleDES, CAST5, Blowfish, AES128, AES192, AES256, or Twofish.
- The decrypted and uncompressed file will be used in upcoming test.

4.5 Environmental needs

- RFC 4880 capable software

4.6 Special procedural requirements

This test has no special procedural requirements.

4.7 Intercase dependencies

EscrowReleaseFileName must first have been executed successfully.

4.8 Ordered description of steps to be taken to execute the test case

All operations are done in accordance with RFC 4880.

Check the properties of each **<EscrowSigFull>** and **<EscrowSigDiff{n}>**:

1. Digest algorithm SHA1, RIPEMD160, SHA224, SHA256, SHA384, or SHA512 **MUST** be used. MD5 is deprecated and **MUST NOT** be used.
2. Public key algorithm RSA, DSA or ECDSA **MUST** be used.

If there is more than one **<EscrowFileFull>** or **<EscrowFileDiff{n}>**:

1. All file parts **MUST** be present. See {#} in the file name and that they form a sequence of numbers starting with 1.

Check the properties of each **<EscrowFileFull>** and **<EscrowFileDiff{n}>**:

1. Public key algorithm RSA, Elgamal or ECDH **MUST** be used.
2. (Cannot check the symmetric algorithm. That OpenPGP information is encrypted and ICANN is the one with the private key. This step is performed below with information given by ICANN.)

Deliver the files to ICANN for decryption:

1. Upload the files to the shared drive.
2. Send a notification of delivery to the ICANN Registry Technical Liaisons.
3. ICANN will send a notification to *pdt@iis.se* when the files have been verified and decrypted.

Receive files from ICANN:

1. Download the files from the shared drive.
2. ICANN will make a note on what symmetric algorithm was used. Symmetric algorithm IDEA, TripleDES, CAST5, Blowfish, AES128, AES192, AES256, or Twofish **MUST** be used.
3. Check the file name of the unencrypted deposits. They **MUST** be named the same as the encrypted deposits but with extension tar.
4. Untar the decrypted archive and check that there is an XML file. It **MUST** be named as the deposit but with the extension xml. The XML file **MUST NOT** be placed in any subdirectory within the archive.

5. Escrow Release Content

5.1 Test case identifier

EscrowReleaseContent

5.2 Objective

This test will check that the deposit is valid and contains information created by the EPP tests.

Requirements from the test plan: [I8], [REG2], [REG6.4]

5.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
EscrowFull	The unencrypted file containing the full deposit	File
EscrowDiff[0..n]	Optional unencrypted files containing the differential deposits	File
EscrowProfile	The data escrow profile described using W3C XML Schema. Provided by ICANN.	XML file
EPPInput	EPP input data given by the applicant	XML file

Input data comes from the test EscrowReleaseVerify.

5.4 Outcome(s)

The deposits **MUST** have data created by the EPP tests.

5.5 Environmental needs

This test has no environmental needs.

5.6 Special procedural requirements

This test has no special procedural requirements.

5.7 Intercase dependencies

EscrowReleaseVerify must first have been executed successfully.

5.8 Ordered description of steps to be taken to execute the test case

For each <EscrowFileFull> and <EscrowFileDiff[n]>:

1. Check if it is an XML or CSV deposit.
 - a. If CSV deposit, then use the corresponding XML in the tests below.
2. Validate the XML file against the <EscrowProfile> XML schema provided by ICANN. The applicant **MUST** use extensions which have been agreed upon with ICANN.

Manually inspect the files. They **MUST** contain data created by the EPP tests.

6. Global

6.1 Glossary

The glossary is available in the Master Test Plan.

6.2 Document change procedures

Document change procedures are documented in the Master Test Plan.