

Pre-Delegation Testing

Data Escrow Test Cases

Version PA6

DRAFT

File name: PDT_DataEscrow_TC.docx

Last saved: 2013-02-07

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_TC.docx

Revisions

Date	Version	Name	Description
2013-01-17	PA1	Rickard Bellgrim	Initial document
2013-01-20	PA2	Rickard Bellgrim	Update after external review
2013-01-22	PA3	Rickard Bellgrim	Update after external review
2013-01-24	PA4	Rickard Bellgrim	Update text
2013-02-06	PA5	Rickard Bellgrim	Add Document Hierarchy and final chapter
2013-02-07	PA6	Rickard Bellgrim	Updated requirements

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	CONTEXT	5
1.4	NOTATION FOR DESCRIPTION	5
2.	DATA ESCROW PROFILE	6
2.1	TEST CASE IDENTIFIER	6
2.2	OBJECTIVE.....	6
2.3	INPUTS	6
2.4	OUTCOME(S)	6
2.5	ENVIRONMENTAL NEEDS	6
2.6	SPECIAL PROCEDURAL REQUIREMENTS	6
2.7	INTERCASE DEPENDENCIES	6
2.8	ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE	6
3.	DATA ESCROW FILE NAME o1	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.	DATA ESCROW FILE NAME o2.....	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.	DATA ESCROW VERIFY o1	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	12
6.	DATA ESCROW VERIFY o2.....	13
6.1	TEST CASE IDENTIFIER	13
6.2	OBJECTIVE.....	13
6.3	INPUTS	13
6.4	OUTCOME(S)	13
6.5	ENVIRONMENTAL NEEDS	13
6.6	SPECIAL PROCEDURAL REQUIREMENTS	13
6.7	INTERCASE DEPENDENCIES	13

6.8	ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE	14
7.	DATA ESCROW CONTENT o1.....	15
7.1	TEST CASE IDENTIFIER	15
7.2	OBJECTIVE.....	15
7.3	INPUTS	15
7.4	OUTCOME(S)	15
7.5	ENVIRONMENTAL NEEDS	15
7.6	SPECIAL PROCEDURAL REQUIREMENTS	15
7.7	INTERCASE DEPENDENCIES	15
7.8	ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE	15
8.	DATA ESCROW CONTENT o2	16
8.1	TEST CASE IDENTIFIER	16
8.2	OBJECTIVE.....	16
8.3	INPUTS	16
8.4	OUTCOME(S)	16
8.5	ENVIRONMENTAL NEEDS	16
8.6	SPECIAL PROCEDURAL REQUIREMENTS	16
8.7	INTERCASE DEPENDENCIES	16
8.8	ORDERED DESCRIPTION OF STEPS TO BE TAKEN TO EXECUTE THE TEST CASE	16
9.	GLOBAL.....	17
9.1	GLOSSARY.....	17
9.2	DOCUMENT CHANGE PROCEDURES	17

1. Introduction

1.1 Scope

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

1.2 References

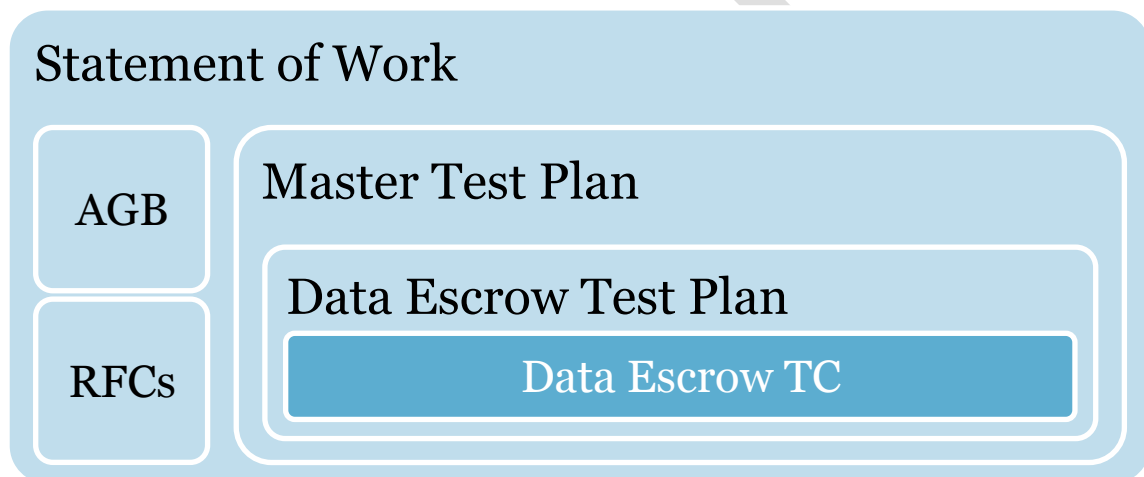
1.2.1 External

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

1.2.2 Internal

- Pre-Delegation Testing, Statement of Work
- Pre-Delegation Testing, Master Test Plan
- Pre-Delegation Testing, Data Escrow 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 data escrow is described in their own chapter. The test procedures are described directly in the test case.

2. Data Escrow Profile

2.1 Test case identifier

DataEscrowProfile

2.2 Objective

The test will verify that the profile is in accordance with the escrow format and the data escrow draft.

Requirements from the test plan: [R22], [REG2]

2.3 Inputs

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

Id	Description	Type
DataProfile	The data escrow profile described using W3C XML Schema	XML file

2.4 Outcome(s)

The data escrow profile MUST be compliant with the W3C XML schema format, data escrow draft, and the data escrow format.

2.5 Environmental needs

This test has no environmental needs.

2.6 Special procedural requirements

This test has no special procedural requirements.

2.7 Intercase dependencies

This test has no intercase dependencies.

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

1. Check that it is a valid W3C XML Schema.
2. Check that it uses the basic elements as described in the data escrow draft.
3. Check that it describes registry objects, such as domains, contacts, name servers, and registrars.
4. Check that any extension schemas are described in accordance with the data escrow draft.

3. Data Escrow File Name 01

3.1 Test case identifier

DataEscrowFileName01

3.2 Objective

The test will receive one full deposit of sample data. The objective is to verify file names.

Requirements from the test plan: [R21], [AGB1], [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
DataFileFull-[1..n]	The files containing the full deposit	Files
DataSigFull-[1..n]	The files containing the signature	Files

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

This test has no intercase dependencies.

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

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

For each **<DataFileFull>**, 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. The file MUST be maximum one month old.
3. {type} is equal to "full".
4. {#} is a number greater than or equal to 1.
5. {rev} is a number greater than or equal to 0.
6. {ext} is equal to "ryde".

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

For each **<DataSigFull>**, 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. The file MUST be maximum one month old.
3. {type} is equal to "full".
4. {#} is a number greater than or equal to 1.
5. {rev} is a number greater than or equal to 0.
6. {ext} is equal to "sig".

4. Data Escrow File Name 02

4.1 Test case identifier

DataEscrowFileName02

4.2 Objective

This test is optional and will only be performed if the applicant has supplied a differential deposit.

The test will receive one differential deposit of sample data. The objective is to verify file names.

Requirements from the test plan: [R21], [AGB2], [REG4]

4.3 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
DataFileDiff-[1..n]	The files containing the differential deposit	Files
DataSigDiff-[1..n]	The files containing the signature	Files

4.4 Outcome(s)

Files MUST be named according to the following convention:

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

4.5 Environmental needs

This test has no environmental needs.

4.6 Special procedural requirements

This test has no special procedural requirements.

4.7 Intercase dependencies

This test has no intercase dependencies.

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

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

For each **<DataFileDiff>**, 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. The file MUST be maximum one month old.
3. {type} is equal to "diff".
4. {#} is a number greater than or equal to 1.
5. {rev} is a number greater than or equal to 0.
6. {ext} is equal to "ryde".

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

For each **<DataSigDiff>**, 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. The file MUST be maximum one month old.
3. {type} is equal to "diff".
4. {#} is a number greater than or equal to 1.
5. {rev} is a number greater than or equal to 0.
6. {ext} is equal to "sig".

5. Data Escrow Verify 01

5.1 Test case identifier

DataEscrowVerify01

5.2 Objective

The test will verify the signatures of the received files. If it is a multi-part transmission, then the files are put together. Decrypt and uncompress the result.

Requirements from the test plan: [R21], [AGB1], [REG3], [REG6.1], [REG6.2], [REG6.3], [ALGO]

5.3 Inputs

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

Id	Description	Type
DataFileFull-[1..n]	The files containing the full deposit	Files
DataSigFull-[1..n]	The files containing the signature	Files
DataRegPubKey	The public key used for verification	File

5.4 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.

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

DataEscrowFileName01 must first have been executed successfully.

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

All operations are done in accordance with RFC 4880.

For each **<DataSigFull>**:

1. Check that the signature is valid for **<DataFileFull>** using **<DataRegPubKey>**.
2. Check that the signature was made with digest algorithm SHA1, RIPEMD160, SHA224, SHA256, SHA384, or SHA512. MD5 is deprecated and MUST NOT be used.
3. Check that the signature was made with the public key algorithm RSA, DSA or ECDSA.

If there is more than one **<DataFileFull>**:

1. Check that all file parts are present. See {#} in the file name and that they form a sequence of numbers starting with 1.
2. Concatenate the files in order.

Decrypt and uncompress the (concatenated) file:

1. Decrypt the file using the private test key.
2. Uncompress the file.
3. Check that the encrypted file was made with symmetric algorithm IDEA, TripleDES, CAST5, Blowfish, AES128, AES192, AES256, or Twofish.
4. Check that the encrypted file was made with public key algorithm RSA, Elgamal or ECDH.

6. Data Escrow Verify 02

6.1 Test case identifier

DataEscrowVerify02

6.2 Objective

This test is optional and will only be performed if the applicant has supplied a differential deposit.

The test will verify the signature of the received files. If it is a multi-part transmission, then the files are put together. Decrypt and uncompress the result.

Requirements from the test plan: [R21], [AGB2], [REG3], [REG6.1], [REG6.2], [REG6.3], [ALGO]

6.3 Inputs

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

Id	Description	Type
DataFileDiff-[1..n]	The files containing the differential deposit	Files
DataSigDiff-[1..n]	The files containing the signature	Files
DataRegPubKey	The public key used for verification	File

6.4 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.

6.5 Environmental needs

This test has no environmental needs.

6.6 Special procedural requirements

This test has no special procedural requirements.

6.7 Intercase dependencies

DataEscrowFileName02 must first have been executed successfully.

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

All operations are done in accordance with RFC 4880.

For each **<DataSigDiff>**:

1. Check that the signature is valid for **<DataFileDiff>** using **<DataRegPubKey>**.
2. Check that the signature was made with digest algorithm SHA1, RIPEMD160, SHA224, SHA256, SHA384, or SHA512. MD5 is deprecated and MUST NOT be used.
3. Check that the signature was made with the public key algorithm RSA, DSA or ECDSA.

If there is more than one **<DataFileDiff>**:

1. Check that all file parts are present. See {#} in the file name and that they form a sequence of numbers starting with 1.
2. Concatenate the files in order.

Decrypt and uncompress the (concatenated) file:

1. Decrypt the file using the private test key.
2. Uncompress the file.
3. Check that the encrypted file was made with symmetric algorithm IDEA, TripleDES, CAST5, Blowfish, AES128, AES192, AES256, or Twofish.
4. Check that the encrypted file was made with public key algorithm RSA, Elgamal or ECDH.

7. Data Escrow Content 01

7.1 Test case identifier

DataEscrowContent01

7.2 Objective

This test will validate the full deposit against the profile.

Requirements from the test plan: [R21], [AGB1], [REG2], [REG6.4]

7.3 Inputs

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

Id	Description	Type
DataFileFull	The unencrypted file containing the full deposit	File
DataProfile	The data escrow profile described using W3C XML Schema	XML file

7.4 Outcome(s)

The full deposit MUST have valid XML and contain required and valid attributes.

7.5 Environmental needs

This test has no environmental needs.

7.6 Special procedural requirements

This test has no special procedural requirements.

7.7 Intercase dependencies

DataEscrowProfile and DataEscrowVerify01 must first have been executed successfully.

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

1. Validate the **<DataFileFull>** XML file against the **<DataProfile>** XML schema.
2. Check that the type is "FULL".
3. Check that the date part of the watermark matches the date in the file name.
4. Check that there is no deletes element in the file.

8. Data Escrow Content 02

8.1 Test case identifier

DataEscrowContent02

8.2 Objective

This test is optional and will only be performed if the applicant has supplied a differential deposit.

This test will validate the differential deposit against the profile.

Requirements from the test plan: [R21], [AGB2], [REG2], [REG6.4]

8.3 Inputs

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

Id	Description	Type
DataFileDiff	The unencrypted file containing the differential deposit	File
DataProfile	The data escrow profile described using W3C XML Schema	XML file

8.4 Outcome(s)

The differential deposit MUST have valid XML and contain required and valid attributes.

8.5 Environmental needs

This test has no environmental needs.

8.6 Special procedural requirements

This test has no special procedural requirements.

8.7 Intercase dependencies

DataEscrowProfile and DataEscrowVerify02 must first have been executed successfully.

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

1. Validate the **<DataFileDiff>** XML file against the **<DataProfile>** XML schema.
2. Check that the type is "DIFF".
3. Check that the prevId attribute is present.
4. Check that the date part of the watermark matches the date in the file name.

9. Global

9.1 Glossary

The glossary is available in the Master Test Plan.

9.2 Document change procedures

Document change procedures are documented in the Master Test Plan.

DRAFT