*ICANN draft dated 31 May 2018*

*For discussion purposes*

**PRIVACY AND PROXY SERVICE PROVIDER**
**DATA ESCROW REQUIREMENT SPECIFICATION**

The Privacy and Proxy Provider ("***Provider***") will engage an independent entity to act as data escrow agent ("***Escrow Agent***") for the provision of data escrow services related to the Privacy and Proxy Service Provider Accreditation Agreement ("***Provider Agreement***"). The following Technical Specifications set forth in Part A, and Legal Requirements set forth in Part B, will be included in any data escrow agreement between Provider and the Escrow Agent, under which ICANN must be named a third-party beneficiary. In addition to the following requirements, the data escrow agreement may contain other provisions that are not contradictory or intended to subvert the required terms provided below.

## Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Fields defined as OPTIONAL MAY be empty only if no information exists in the Provider database.

## PART A – TECHNICAL SPECIFICATIONS

1. **Deposits**. There will be two types of Deposits: Full and Differential.

   1.1. "**Full Deposit**" will consist of data that reflects the state of the Provider records as of 00:00:00 UTC (Coordinated Universal Time) on the day that such Full Deposit is submitted to Escrow Agent.

   1.2. "**Differential Deposit**" means data that reflects all transactions that were not reflected in the last previous Full or Differential Deposit, as the case may be. Each Differential Deposit will contain all database additions or modifications since the previous Deposit was completed as of 00:00:00 UTC of each day, but Sunday. Differential Deposits MUST include complete Escrow Records as specified below that were not included or changed since the most recent full or Differential Deposit (i.e., all additions and modifications of data).

   This document defines as "Differential" deposit what in the Registrar Data Escrow Specification (see Part A, Section 9, reference (6)6 of this Specification) is referred to as "Incremental" deposit.

2. **Schedule for Deposits**. Provider will submit an escrow deposit on a daily basis as follows:

2.1. Each Sunday, a Full Deposit MUST be submitted to the Escrow Agent by 23:59 UTC.

2.2. The other six (6) days of the week, a Full Deposit or the corresponding Differential Deposit MUST be submitted to Escrow Agent by 23:59 UTC.

3. **Escrow Format Specification**.

3.1. **Deposit's Format**.

3.1.1. Escrow records shall be compiled into a single (uncompressed) CSV text file or multiple (uncompressed) CSV text files, in compliance with RFC 4180 <http://tools.ietf.org/html/rfc4180>. The encoding shall be UTF-8.

3.1.2. Numerous fields indicate "date" and "time", such as the expiry dates for domain names. These fields SHALL contain timestamps indicating the date and time in UTC as specified in RFC 3339, with no offset from the zero meridian.

3.1.3. The first line of the CSV files defined in this document is:

<version>,<creation_datetime>,<timeline_watermark>,<number_of_lines>,<id>

Where:

- <version>, version of the file, this field MUST be 1.
- <creation_datetime>, date and time that the file was created.
- <timeline_watermark>, date and time of on which to base the collecting of database objects for a Deposit. Deposits are expected to be consistent to that point in time.
- <number_of_lines>, number of escrow records in the CSV file. Note: this total MUST exclude the two required header lines.
- <id>, that unequivocally identifies the escrow deposit that must the same in all the CSV files of a deposit as defined in draft-arias-noguchi-registry-data-escrow (see Part A, Section 9, reference 5 of this Specification). The Provider is responsible for maintaining its own escrow deposits identifier space to ensure uniqueness.

3.1.4. Providers MUST use "handles" or other unique identifiers to represent identical contact information and provide two separate CSV files: one that is populated with the handles for each domain name's contacts, and a second that provides detailed contact information relative to each handle.

3.1.4.1. The domain file is contained in a CSV formatted file named "pp_domains.csv" that has the following structure:

*first line:*

As defined in 3.1.3.

*second line: a header line as specified in [RFC4180]*

With the header names as follows:

roid,domainName,ianaID,registrantHandle,adminHandle,technicalHandle,billingHandle

*Followed by a line for each domain name using the Provider's services*

Where:

- <roid>, domain name Repository Object IDentifier (DNROID) in the registry database.
- <domainName>, fully qualified domain name. For Internationalized Domain Names, the A-label form is used.
- <ianaID>, IANA Registrar ID of the sponsoring registrar.
- <registrantHandle>, OPTIONAL contact handle of the Customer's registrant contact
- <adminHandle>, OPTIONAL contact handle of the Customer's administrative contact
- <techHandle>, OPTIONAL contact handle of the Customer's technical contact
- <billingHandle>, OPTIONAL contact handle of the Customer's billing contact

3.1.4.2. The contact file is contained in a CSV formatted file named "pp_contact_handles.csv" that has the following structure:

*first line:*

As defined in 3.1.3.

*second line: a header line as specified in [RFC4180]*

With the header names as follows:

contactHandle,name,org,street1,street2,street3,city,sp,cc,pc,email,voice,voiceExt,fax,faxExt

*Followed by a line for each contact handle referenced in the Provider's domain file*

Where:

- <contactHandle>, unique identifier for the contact within the deposit.
- <name>, name of the individual or role represented by the contact.
- <org>, OPTIONAL, name of the organization with which the contact is affiliated.
- <street1>, contact's street address.
- <street2>, OPTIONAL, contact's street address.
- <street3>, OPTIONAL, contact's street address.
- <city>, contact's city.

- <sp>, OPTIONAL, contact's state or province.
- <cc>, contact's two-letter country code.
- <pc>, OPTIONAL, contact's postal code.
- <email>, contact's email address.
- <voice>, contact's voice telephone number.
- <voiceExt>, OPTIONAL, contact's voice telephone number extension.
- <fax>, OPTIONAL, contact's facsimile telephone number.
- <faxExt>, OPTIONAL, contact's facsimile telephone number extension.

3.1.5. Differential deposits must include complete Escrow Records for each Customer data that was not included or modified in the most recent full or differential deposit (i.e., newly added or modified). Differential deposits shall incorporate the cross-reference and handle conventions described above since the last deposit.

4. **Processing of Deposit files**. The use of compression is recommended in order to reduce electronic data transfer times, and storage capacity requirements. Data encryption will be used to ensure the privacy of Provider escrow data. Files processed for compression and encryption will be in the binary OpenPGP format as per OpenPGP Message Format - RFC 4880, see Part A, Section 9, reference 1 of this Specification. 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, see Part A, Section 9, reference 2 of this Specification, that are also royalty-free. The process to follow for the data file in original text format is:

(1) The CSV file(s) of the deposit are aggregated in a tarball file named as described in Section 5 but with extension tar.

(2) A compressed and encrypted OpenPGP Message is created using the tarball file as sole input. The suggested algorithm for compression is ZIP as per RFC 4880. The compressed data will be encrypted using the escrow agent's public key. The suggested algorithms for Public-key encryption are Elgamal and RSA with a key size of at least 2048 bits as per RFC 4880. The suggested algorithms for Symmetric-key encryption are AES192 and AES256 as per RFC 4880.

(3) The file may be split as necessary if, once compressed and encrypted, it is larger than the file size limit agreed with the escrow agent. Every part of a split file, or the whole file if not split, will be called a processed file in this section.

(4) A digital signature file will be generated for every processed file using the Provider's private key. The digital signature file will be in binary OpenPGP format as per RFC 4880, and will not be compressed or encrypted. The suggested algorithms for Digital signatures are DSA and RSA as per RFC 4880. The suggested algorithm for Hashes in Digital signatures is SHA256.

(5) The processed files and digital signature files will then be transferred to the Escrow Agent through secure electronic mechanisms, such as, SFTP, SCP,

HTTPS file upload, etc. as agreed between the Escrow Agent and the Provider.

(6) The Escrow Agent will then validate every (processed) transferred data file using the procedure described in Part A, Section 8 of this Specification.

5. **File Naming Conventions**. The tarball file will be named according to the following convention: {Provider ICANN ID}_{YYYY-MM-DD}_{type}_S{#}_R{rev}.{ext} where:

5.1. {Provider ICANN ID} is replaced with the Provider's unique ID assigned by ICANN, in the format PP####;

5.2. {YYYY-MM-DD} is replaced by the date corresponding to the time used as a timeline watermark for the transactions; i.e. for the Full Deposit corresponding to 2009-08-02T00:00Z, the string to be used would be "2009-08-02";

5.3. {type} is replaced by:

5.3.1. "full", if the data represents a Full Deposit;

5.3.2. "diff", if the data represents a Differential Deposit;

5.4. {#} is replaced by the position of the file in a series of files, beginning with "1"; in case of a lone file, this must be replaced by "1".

5.5. {rev} is replaced by the number of revision (or resend) of the file beginning with "0". Note: this value is incremented each time the escrow deposit failed the verification procedure at the receiving party and a new escrow deposit needs to be generated by the Provider for that specific date.

5.6. {ext}, extension, is replaced by "sig" if it is a digital signature file of the quasi-homonymous file. Otherwise it is replaced by "ppde".

6. **Distribution of Public Keys**. Each of Provider and Escrow Agent will distribute its public key to the other party (Provider or Escrow Agent, as the case may be) via email to an email address to be specified. 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, like in person meeting, telephone, etc. In this way, public key transmission is authenticated to a user able to send and receive mail via a mail server operated by the distributing party. Escrow Agent, Provider and ICANN will exchange public keys by the same procedure.

7. **Notification of Deposits**. Along with the delivery of each Deposit, Provider will deliver to Escrow Agent and to ICANN (using the API described in draft-icann-ppsp-interfaces, see Part A, Section 9, reference 3 of this Specification (the "Interface Specification")) a statement from Provider that includes a copy of the report generated upon creation of

the Deposit and states that the Deposit has been inspected by Provider and is complete and accurate. The preparation and submission of this statement must be performed by the Provider or its designee, provided that such designee may not be the Escrow Agent or any of Escrow Agent's Affiliates. Provider will include the Deposit's <id> in its statement.

8. **Verification Procedure**.

(1) The signature file of each processed file is validated.

(2) If processed files are pieces of a bigger file, the latter is put together.

(3) Each file obtained in the previous step is then decrypted and uncompressed.

(4) Each data file contained in the previous step is then validated against the format defined in section 3.

(5) The Internet-Draft draft-icann-ppsp-interfaces, see Part A, Section 9, reference 3, defines error codes that the Escrow Agent shall use to report verification problems when validating a deposit. If a verification problem is detected the Escrow Agent shall reject the deposit.

If any discrepancy is found in any of the steps, the Deposit will be considered incomplete.

9. **References**.

(1) OpenPGP Message Format, http://www.rfc-editor.org/rfc/rfc4880.txt

(2) OpenPGP parameters, http://www.iana.org/assignments/pgp-parameters/pgp-parameters.xhtml

(3) ICANN interfaces for privacy and proxy providers and their data escrow agents, http://tools.ietf.org/html/draft-icann-ppsp-interfaces

(4) ICANN interfaces for registrars and their data escrow agents, http://tools.ietf.org/html/draft-icann-registrar-interfaces

(5) Registry Data Escrow Specification, https://tools.ietf.org/html/draft-arias-noguchi-registry-data-escrow

(6) Registrar Data Escrow Specification, https://www.icann.org/en/system/files/files/rde-specs-09nov07-en.pdf

**PART B – LEGAL REQUIREMENTS**

1. **Escrow Agent**. Prior to entering into an escrow agreement, the Provider must provide notice to ICANN as to the identity of the Escrow Agent, and provide ICANN with contact information and a copy of the relevant escrow agreement, and all amendments thereto. In addition, prior to entering into an escrow agreement, Provider must obtain the consent of ICANN to (a) use the specified Escrow Agent, and (b) enter into the form of escrow agreement provided by ICANN. ICANN must be expressly designated as a third-party beneficiary of the escrow agreement. ICANN reserves the right to withhold its consent to any Escrow Agent, escrow agreement, or any amendment thereto, all in its sole discretion.

2. **Fees**. Provider must pay, or have paid on its behalf, fees to the Escrow Agent directly. If Provider fails to pay any fee by the due date(s), the Escrow Agent will give ICANN written notice of such non-payment and ICANN may pay the past-due fee(s) within fifteen (15) calendar days after receipt of the written notice from Escrow Agent. Upon payment of the past-due fees by ICANN, ICANN shall have a claim for such amount against Provider, which Provider shall be required to submit to ICANN together with the next fee payment due under the Provider Agreement.

3. **Ownership**. Ownership of the Deposits during the effective term of the Provider Agreement shall remain with Provider at all times. Thereafter, Provider shall assign any such ownership rights (including intellectual property rights, as the case may be) in such Deposits to ICANN. In the event that during the term of the Provider Agreement any Deposit is released from escrow to ICANN, any intellectual property rights held by Provider in the Deposits will automatically be licensed to ICANN or to a party designated in writing by ICANN on a non-exclusive, perpetual, irrevocable, royalty-free, paid-up basis, for any use related to the TLD.

4. **Integrity and Confidentiality**. Escrow Agent will be required to (i) hold and maintain the Deposits in a secure, locked, and environmentally safe facility, which is accessible only to authorized representatives of Escrow Agent, (ii) protect the integrity and confidentiality of the Deposits using commercially reasonable measures and (iii) keep and safeguard each Deposit for one (1) year. ICANN and Provider will be provided the right to inspect Escrow Agent's applicable records upon reasonable prior notice and during normal business hours. Provider and ICANN will be provided with the right to designate a third-party auditor to audit Escrow Agent's compliance with the technical specifications and maintenance requirements of this Specification from time to time.

   If Escrow Agent receives a subpoena or any other order from a court or other judicial tribunal pertaining to the disclosure or release of the Deposits, Escrow Agent will promptly notify the Provider and ICANN unless prohibited by law. After notifying the Provider and ICANN, Escrow Agent shall allow

sufficient time for Provider or ICANN to challenge any such order, which shall be the responsibility of Provider or ICANN; provided, however, that Escrow Agent does not waive its rights to present its position with respect to any such order. Escrow Agent will cooperate with the Provider or ICANN to support efforts to quash or limit any subpoena, at such party's expense. Any party requesting additional assistance shall pay Escrow Agent's standard charges or as quoted upon submission of a detailed request.

5. **Copies**. Escrow Agent may be permitted to duplicate any Deposit, in order to comply with the terms and provisions of the escrow agreement.

6. **Release of Deposits**. Escrow Agent will make available for electronic download (unless otherwise requested) to ICANN or its designee, within twenty-four (24) hours, at the Provider's expense, all Deposits in Escrow Agent's possession in the event that the Escrow Agent receives a request from Provider to effect such delivery to ICANN, or receives one of the following written notices by ICANN stating that:

   6.1. The Provider Agreement has expired without renewal, or been terminated; or

   6.2. ICANN has not received a notification as described in Part B, Sections 7.1 and 7.2 of this Specification from Escrow Agent within five (5) calendar days after the Deposit's scheduled delivery date; (a) ICANN gave notice to Escrow Agent and Provider of that failure; and (b) ICANN has not, within seven (7) calendar days after such notice, received the notification from Escrow Agent; or

   6.3. ICANN has received notification as described in Part B, Sections 7.1 and 7.2 of this Specification from Escrow Agent of failed verification of the latest escrow deposit for a specific date or a notification of a missing deposit, and the notification is for a deposit that should have been made on Sunday (i.e., a Full Deposit); (a) ICANN gave notice to Provider of that receipt; and (b) ICANN has not, within seven (7) calendar days after such notice, received notification as described in Part B, Sections 7.1 and 7.2 of this Specification from Escrow Agent of verification of a remediated version of such Full Deposit; or

   6.4. ICANN has received five notifications from Escrow Agent within the last thirty (30) calendar days notifying ICANN of either missing or failed escrow deposits that should have been made Monday through Saturday (i.e., a Differential Deposit), and (x) ICANN provided notice to Provider of the receipt of such notifications; and (y) ICANN has not, within seven (7) calendar days after delivery of such notice to Provider, received notification from Escrow Agent of verification of a remediated version of such Differential Deposit; or

6.5. Provider has: (i) ceased to conduct its business in the ordinary course; or (ii) filed for bankruptcy, become insolvent or anything analogous to any of the foregoing under the laws of any jurisdiction anywhere in the world; or

6.6. a competent court, arbitral, legislative, or government agency mandates the release of the Deposits to ICANN; or

6.7. pursuant to Contractual and Operational Compliance Audits as specified under the Provider Agreement.

Unless Escrow Agent has previously released the Provider's Deposits to ICANN or its designee, Escrow Agent will deliver all Deposits to ICANN upon expiration or termination of the Provider Agreement or the Escrow Agreement.

7. **Verification of Deposits**.

7.1. Within twenty-four (24) hours after receiving each Deposit or corrected Deposit, Escrow Agent must verify the format and completeness of each Deposit and deliver to ICANN a notification generated for each Deposit. Reports will be delivered electronically using the API described in draft-icann-ppsp-interfaces (see Part A, Section 9, reference 3 of this Specification).

7.2. If Escrow Agent discovers that any Deposit fails the verification procedures or if Escrow Agent does not receive any scheduled Deposit, Escrow Agent must notify Provider either by email, fax or phone and ICANN (using the API described in draft-icann-ppsp-interfaces, see Part A, Section 9, reference 3 of this Specification) of such nonconformity or non-receipt within twenty-four (24) hours after receiving the non-conformant Deposit or the deadline for such Deposit, as applicable. Upon notification of such verification or delivery failure, Provider must begin developing modifications, updates, corrections, and other fixes of the Deposit necessary for the Deposit to be delivered and pass the verification procedures and deliver such fixes to Escrow Agent as promptly as possible.

8. **Amendments**. Escrow Agent and Provider shall amend the terms of the Escrow Agreement to conform to this Specification within ten (10) calendar days of any amendment or modification to this Specification. In the event of a conflict between this Specification and the Escrow Agreement, this Specification shall control.

9. **Indemnity**. Escrow Agent shall indemnify and hold harmless Provider and ICANN, and each of their respective directors, officers, agents, employees, members, and stockholders ("Indemnitees") absolutely and forever from and against any and all claims, actions, damages, suits, liabilities, obligations, costs, fees, charges, and any other expenses whatsoever, including reasonable attorneys' fees and costs, that may be asserted by a third party against any Indemnitee in connection with the misrepresentation, negligence or misconduct of Escrow Agent, its directors, officers, agents, employees and contractors.