

Registrar Data Escrow Specifications 2024

1 Introduction

- 1.1 Section 3.6 of the [2013 Registrar Accreditation Agreement \(RAA\)](#) obligates all ICANN-accredited registrars to submit a data escrow deposit according to the schedule, terms, and format specified by ICANN.
- 1.2 In regards to their data escrow deposits, registrars (1) must include the data elements specified in Section 8.1 of the [Registration Data Policy](#) and Section 3.4.1.3 of the RAA; (2) if applicable, must include the data elements specified in Section 8.2 of the Registration Data Policy and Sections 3.4.1.4 through 3.4.1.5 of the RAA; and (3) may include the data elements included in Section 8.3 of the Registration Data Policy.
- 1.3 The collective contents of escrowed data elements for a domain name registration is referred to as an Escrow Record. The collection of Escrow Records that are required to be submitted to the Data Escrow Agent (DEA) is referred to in this document as a data escrow deposit.
- 1.4 This document specifies the schedule, terms, and format registrars must use to escrow data pursuant to Section 3.6 of the RAA.

2 Schedule

2.1 Deposit Schedule

- 2.1.1 The data deposit schedule for each registrar will vary depending on the registrar's quarterly gTLD transaction volume as determined by ICANN. Registrars whose transaction volume meets or exceeds 100,000 registration-years per ICANN fiscal quarter will be required to submit differential¹ deposits daily and full deposits weekly. Registrars with fewer than 100,000 registration-years per quarter will be required to deposit data into escrow once per week, but submission of daily differential deposits for such registrars will be optional.
- 2.1.2 ICANN will notify registrars of their required deposit schedules which will be determined based on the registrar's quarterly gTLD transaction volume. Registrars will also be provided notifications in the event their required deposit schedule changes due to a change in quarterly transaction volume.
- 2.1.3 The following table sets out the deposit schedule applicable to each registrar by quarterly transaction volume. The number on the far left represents transaction-years billed by ICANN.

¹ Note: in the previous version of this specification, "Differential" deposits (see RFC8909) were referred to as "Incremental" deposits.

Quarterly Transaction Volume	Frequency of "Full" Deposits	Frequency of Differential Deposits
1 - 99,999	once every week	n/a
100,000 +	once every week	once every day, except those days when a "Full Deposit" is being delivered

3 Terms

3.1 Generally Applicable Terms

3.1.1 Registrars may deposit their Escrow Records with an ICANN-Designated Registrar DEA at no charge or they may choose to use an ICANN-Approved Registrar DEA at the registrar's expense. In either case, the provisions of this document will apply to all escrow arrangements and are hereby incorporated into the agreement(s) between ICANN, the registrar, and the DEA and the agreement(s) between ICANN and the ICANN-Designated Registrar DEA (each, an "Agreement"). In the event of a conflict between this document and any Agreement, this document shall control.

3.1.1.1 Within thirty (30) days of notice by ICANN that a registrar's data escrow provision is being invoked, the registrar must choose whether it will escrow data with an ICANN-Designated Registrar DEA or with an ICANN-Approved Registrar DEA.

3.1.1.2 Within sixty (60) days of notice by ICANN that a registrar's data escrow provision is being invoked, the registrar must begin escrowing data. ICANN may, within its discretion, extend this deadline upon a showing of good cause by the registrar.

3.1.1.3 Registrars may change their DEA by providing a written notice to ICANN at least seven (7) days in advance. In order to assist ICANN in monitoring the effectiveness of the Registrar Data Escrow (RDE) program, registrars are encouraged to include in their notice a brief explanation of the basis for the change of DEA.

3.1.1.4 In the event deposits are not made according to the required schedule, the DEA shall promptly notify ICANN and the registrar if a deposit is not received on the scheduled deposit date. The DEA shall provide notice to ICANN within twenty-four (24) hours of any missing, valid or failed deposit using the ICANN's Registration Reporting Interface (RRI) as defined in ICANN Registrar Interfaces (RRI Specification), available at <https://tools.ietf.org/html/draft-icann-registrar-interfaces>. The

- DEA must use the mapping in Appendix A when generating the notification. In case of missing and failed deposits, the DEA shall directly work with the registrar to resolve any issues.
- 3.1.1.5 The DEA shall verify the integrity of the deposit through checksum validation as set forth below. A deposit that does not pass integrity verification is considered a failed deposit and shall not be accepted by the DEA.
 - 3.1.1.6 The DEA shall verify each Escrow Record to ensure conformance with the requirements in this document and only accept deposits without errors. A deposit with one (1) or more Escrow Records with errors is considered a failed deposit.
 - 3.1.1.7 The DEA shall perform manual reviews of deposits necessary to assist registrars in remedying failed data validation tests and as reasonably requested by ICANN.
 - 3.1.1.8 The DEA shall release Escrow Records to ICANN within twenty-four (24) hours of written notice by ICANN via email electronically signed using ICANN's OpenPGP private key; provided, however, if applicable law requires additional notice, the DEA must immediately inform ICANN of any such additional requirements. In the event the data is released to ICANN, ICANN or its assignee shall have a non-exclusive, irrevocable, royalty-free license to exercise (only for transitional purposes) or have exercised all rights necessary to provide registrar services. When releasing data to ICANN, the data shall be first decrypted by the DEA and then encrypted using ICANN's OpenPGP public key.
 - 3.1.1.9 Notwithstanding the terms of the RAA, upon mutual agreement of ICANN and the registrar, the DEA shall release Escrow Records at any time to ICANN, the registrar, or another designated party. When releasing data to ICANN, the data shall be first decrypted by the DEA and then encrypted using ICANN's OpenPGP public key.
 - 3.1.1.10 All parties shall employ commercially reasonable means to ensure security of data, including use of encryption during file storage and transmission.
 - 3.1.1.11 ICANN shall have the right, either directly or through use of an independent auditor or other agent, to perform an inspection and audit of the records and systems of all DEAs
 - 3.1.1.12 The terms, format, and schedule outlined in this document may be changed by ICANN upon 60 days' notice to registrars and DEAs in accordance with each Agreement.
 - 3.1.2 Registrars who deposit Escrow Records with a DEA shall enter into a standardized agreement with ICANN and the DEA which outlines the obligations and liabilities of all parties to the agreement.

3.2 Terms Applicable to Registrars that Deposit Escrow Data with an ICANN-Designated Registrar DEA

- 3.2.1 The following terms apply only to those registrars who choose to deposit data with an ICANN-Designated Registrar DEA.
 - 3.2.1.1 [RESERVED]

- 3.2.1.2 ICANN or an ICANN-Designated Registrar DEA may impose limitations on the format of data and method of transmission of data that are more restrictive than the specifications contained in this document. (e.g., the DEA might accept deposits electronically only or may require exclusive use of a particular data compression method. These are examples, not an exhaustive list of possible limitations.)
- 3.2.1.3 ICANN-Designated Registrar DEAs, as applicable or upon request by ICANN, may review data deposited to verify its completeness, consistency, and formatting at any time, without notice to the registrar. The cost of such reviews will be borne by ICANN or such ICANN-Designated Registrar DEA.

3.3 Terms Applicable to Registrars Utilizing ICANN-Approved Registrar DEA

- 3.3.1 Registrars may choose to escrow data with an ICANN-Approved Registrar DEA of escrow services in lieu of depositing with an ICANN-Designated Registrar DEA. The following terms apply to registrars who choose to deposit with ICANN-Approved Registrar DEA:
 - 3.3.1.1 ICANN-Approved Registrar DEA approval criteria and application instructions are available [here](#), as may be updated from time to time.
 - 3.3.1.2 Each ICANN-Approved Registrar DEA and ICANN will exchange public keys via email. 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.
 - 3.3.1.3 Once a DEA becomes an ICANN-Approved Registrar DEA, any registrar may utilize its services without need for an additional ICANN-Approved Registrar DEA application, except that no registrar shall be permitted to escrow data with an ICANN-Approved Registrar DEA with whom it has any relationship or affiliation, including, without limitation, common ownership, management, or staff. (This does not obligate ICANN-Approved Registrar DEA to accept any willing registrar as a client; ICANN-Approved Registrar DEAs may contract with whomever they choose.) Any newly approved ICANN-Approved Registrar DEAs will be published on ICANN's website.
 - 3.3.1.4 In the event ICANN withdraws its approval of an ICANN-Approved Registrar DEA, affected registrars will be notified and provided at least sixty (60) days to choose an ICANN-Designated Registrar DEA or another ICANN-Approved Registrar DEA as their new DEA. Affected registrars may be required to begin escrowing data with the newly chosen DEA upon the effective date of the withdrawal by ICANN of such ICANN-Approved Registrar DEA's approval.
 - 3.3.1.5 ICANN-Approved Registrar DEAs may impose limitations on the format of data and method of transmission of data that are more restrictive than the specifications contained in this

- document.
- 3.3.1.6 ICANN-Approved Registrar DEAs shall retain and archive two copies of all Escrow Records for at least one year from the date of deposit. The archived data may be stored on its original medium (in addition to one copy) or two copies may be retained in another reliable form (e.g., copied to a redundant array of independent hard drives or optical storage) provided that checksum validation is successfully performed following any copying or transfer of data and the files are not otherwise modified from the form in which they were deposited by the registrar. To the extent data is copied to hard drives, the ICANN-Approved Registrar DEAs shall not store any two sequential, "full" deposits by the same registrar on the same drive or array of drives.
 - 3.3.1.7 ICANN-Approved Registrar DEAs shall erase or destroy all deposited data older than one year (including copies and derivative versions), unless a longer period is agreed to by the registrar and the ICANN-Approved Registrar DEA.

4 Format

- 4.1 The following format requirements are applicable to all registrars, regardless of whether the registrar deposits data with an ICANN-Designated Registrar DEA or an ICANN-Approved Registrar DEA.
 - 4.1.1 Escrow records shall be compiled into a single (uncompressed) CSV text file or multiple (uncompressed) text files approximately 1 gigabyte or one million rows in size, or a greater limit per mutual agreement of the registrar and DEA. The CSV file(s) shall comply with RFC4180. The character encoding for the CSV file(s) must be UTF-8, unless specified otherwise by ICANN.
 - 4.1.2 Registrars may include fields to hold sub-elements where it is logical to do so (e.g., one field may contain the registrant's name and another may hold the registrant's telephone number).
 - 4.1.3 In the case of internationalized domain names, the A-label (ASCII compatible form of the IDN string) shall be referenced in the domain name field (e.g., "xn--11b5bs1di.tld"), not the U-label.
 - 4.1.4 [RESERVED]
 - 4.1.5 In order to comply with Section 3.4.1.5 of the RAA, registrars must include additional fields in the text file to escrow the names, postal addresses, e-mail addresses, and voice telephone numbers provided by the customers of any privacy service or licensee of any proxy registration service, in each case, offered or made available by Registrar or its Affiliates (as defined in the RAA) in connection with each registration.
 - 4.1.6 No additional data, other than what is described in this document, should be included in a data escrow deposit.
 - 4.1.7 Registrars shall deposit Escrow Records for every gTLD name under their management as registrar, except that registrars may optionally exclude from the deposit any name in an add-grace period on the date

- of the data file's compilation.
- 4.1.8 The deposited data shall be temporally current, relative to the last deposit date (i.e., no more than six (6) days old for registrars who only make weekly deposits and no more than twenty-three (23) hours old for registrars who make daily deposits).
 - 4.1.9 Registrars who use "handles" or other unique identifiers to represent identical contact information may provide two separate data files: one that is populated with the handles for each domain name's contacts, and a second text file in the same general format that provides detailed contact information relative to each handle.
 - 4.1.10 Registrars who do not use handles may populate otherwise redundant fields in an Escrow Record with reference to a completely populated field in the same record. (For example the registrant-c field in one record might contain complete data, but if the tech-c is identical, the tech-c field could be populated with "rc" or a similarly unambiguous abbreviation as a cross-reference, instead of redundant data.)
 - 4.1.11 Differential deposits, where required, must include complete Escrow Records for each domain name under the registrar's sponsorship that was not included in the most recent full or differential deposit (i.e., newly added or transferred-in names). Differential deposits may incorporate the cross-reference and handle conventions described above and do not need to include Escrow Records for names for which there was merely a change to registration data since the last deposit.
 - 4.1.12 The CSV file(s) shall include the respective header in the first row of the (first) file (in the series). If the data is spread across a sequence of multiple files with identical format, only the first file in the sequence should contain the header row.
 - 4.1.13 The header shall clearly designate the data contained within the corresponding fields. Field names in the header row shall be composed of the following characters: lower case 'a' through lower case 'z', uppercase 'A' through uppercase 'Z', decimal digits '0' through '9', the ASCII underscore character ('_'), and the ASCII hyphen ('-'). Field names must begin with a letter. No other characters are allowed; in particular, embedded spaces, punctuation characters, or other special characters are not allowed.
 - 4.1.14 The first field in the header row shall be the domain name (or handle in the handle definition file). Unambiguous abbreviations may be used. Field names referring to the registrant shall be prefixed with the string 'rt-' (e.g., 'rt-fax') and field names referring to the technical contact shall be prefixed with the string 'tc-' (as in 'tc- country').
 - 4.1.15 Registrars shall provide ICANN and their DEA with a copy of their header row and a table with the following:
 - 4.1.15.1 the mapping of the field's name in the header row and the name of the data elements described in Sections 8.1 through 8.3 of the Registration Data Policy when the field contains the value of data elements described in Sections 8.1 through 8.3 of the Registration Data Policy;
 - 4.1.15.2 an explanation of any abbreviations used per Section 4.1.10;
 - 4.1.15.3 for additional fields included per Section 3.4.1.3, 3.4.1.4 and 3.4.1.5 of the RAA, an explanation for every additional field.
 - 4.1.16 Each record or row following the header shall contain registration details for only one domain name or handle.

- 4.1.17 If the size of a single file exceeds one gigabyte, the file shall be split by the registrar into files approximately one gigabyte or one million rows in size, or a greater limit per mutual agreement of the registrar and DEA. File splits shall occur only at the end of record boundaries.
- 4.1.18 The registrar shall generate a SHA-256 hash for each file (after file splitting, if applicable). The hash string(s) shall be submitted in a single, uncompressed text file along with the respective file name(s). The text file with checksums shall be composed of ASCII lines of text. Each line shall consist of the hash value for one file, followed by white space, followed by the name of the file. (This is the format produced by the widely available "sha256sum" utility.) An alternative or replacement hash function or verification method may be specified by ICANN in the future as the technology evolves.
- 4.1.19 The registrar shall compress each file (excluding the hash file) using any one of the following methods:
 - 4.1.19.1 UNIX compress
 - 4.1.19.2 gzip
 - 4.1.19.3 bzip2
 - 4.1.19.4 PKZIP (or compatible .zip)
 - 4.1.19.5 RAR (version 2.0 or older, only)
 - 4.1.19.6 An alternative compression method specified in the future by ICANN as the technology evolves.
- 4.1.20 Compressed files shall be encrypted using the DEA's public OpenPGP key and signed using the registrar's OpenPGP private key. Acceptable algorithms for Public-key cryptography, Symmetric-key cryptography, Hash and Compression are those enumerated in RFC4880, not marked as deprecated in OpenPGP IANA Registry, that are also royalty-free.
- 4.1.21 Files shall be named according to the following convention:
[IANA ID]_RDE_[YYYY-MM-DD]_[full/diff/hdl/hash]_[#], where
 - 4.1.21.1 [IANA ID] is replaced with the registrar's IANA ID number;
 - 4.1.21.2 [YYYY-MM-DD] is replaced by the file creation date;
 - 4.1.21.3 [full/diff/hdl/hash] is replaced by "full" if the data represents a full dump, "diff" if the escrowed data represents a differential deposit, "hdl" if the data includes underlying contact data for each handle, or "hash" in the case of the text file containing the hash string(s);
 - 4.1.21.4 [#] is replaced by the position of the file in the series of files (but not used for the hash file); and
 - 4.1.21.5 a file extension, appropriate to the compression method, is appended.
- 4.1.22 The compressed files and the text file containing the hash string(s) shall be transferred to the escrow agent through secure electronic mechanisms, such as, SFTP, SCP, HTTPS file upload, etc. as agreed between the DEA and the registrar. Non-electronic delivery through a physical medium such as CD-ROMs, DVD-ROMs, or USB storage devices may be used if authorized by ICANN.
- 4.1.23 ICANN may, in its sole discretion, reject as non-compliant any particular implementation of these specifications it reasonably determines to be inconsistent with the purposes of these standardized requirements (i.e., where the data could not be readily or practically used as permitted by the RAA).

Appendix A.

Verification Requirements and Error Code Mapping for RRI

Verification requirement	Error Code	Message
Registrars must provide a single text file with the deposit hash string(s) following the naming convention in Section 4.1.21.	2001	No corresponding hash file found for deposit file.
Provided hash string(s) must match for each deposit file.	2002	Hash does not match corresponding deposit file.
Provided hash string(s) must follow the format specified in Section 4.1.18.	2003	Invalid hash file format.
- The encrypted and compressed data escrow file(s) must be digitally signed using OpenPGP. - File signature(s) must successfully validate the data escrow deposit file(s) using the registrar's public OpenPGP key.	2004	Data escrow deposit OpenPGP signature verification error.
- Each one of the compressed files must follow the naming convention defined in Section 4.1.21. - All the compressed files provided by the registrar must be able to be decrypted into the CSV format using any of the compression methods listed in Section 4.1.19.	2005	Archive includes unrecognized files.
CSV file must not have an encoding other than UTF-8 unless specified otherwise by ICANN.	2006	Invalid encoding for data escrow deposit file.
Uncompressed individual data escrow deposit files must not exceed 1 GB in size as required in Section 4.1.1 or the greater limit as agreed between the registrar and the DEA.	2007	Data escrow deposit file size exceeds maximum allowed size.
Individual data escrow deposit files must not exceed 1,000,000 rows as required in Sections 4.1.1 and 4.1.17 or the greater limit as agreed between the registrar and DEA.	2008	Data escrow deposit file exceeds maximum allowed number of lines.

• CSV header row must match the header that was provided and agreed initially between the registrar, ICANN and the DEA. • The first field in the header should be the domain name or contact handle as applicable. • CSV header field names must begin with a letter, and consist of a-z, A-Z, 0-9, “-“, “_” characters only.	2101	Unrecognized data escrow deposit file CSV header.
• Data Escrow file contents must be compliant with RFC4180. • If the data escrow deposit is split in multiple files, the file splits must occur only at the end of record boundaries.	2102	Escrow Record structure does not conform with CSV header definition.
• Data for the elements referenced in Section 1.2 must be present for every Escrow Record in the deposit.	2103	Escrow Record found missing data in required field(s).
• Value for the domain name must be composed of NR- LDH labels or valid IDNA2008 A-Labels as defined in the standards track RFCs 5890, 5891, 5892 and 5893 or any RFC that replaces or updates the listed RFCs. • Grandfathered domain names compliant with IDNA2003 are also allowed in the deposit.	2104	Invalid domain name syntax in Escrow Record.
• When present, contact email address syntax must comply with RFC5322 or its successors.	2105	Invalid email syntax in Escrow Record.
• None. This error code is not applicable and shall not be used.	2106	Invalid hostname syntax in Escrow Record.
• None. This error code is not applicable and shall not be used.	2107	Invalid date syntax in Escrow Record.

When present, contact telephone and fax number syntax must comply with Section 2.5 of RFC5733.	2108	Invalid phone syntax in Escrow Record.
- Each domain name must appear only once across the data escrow file. - If used, each contact handle must appear only once in the handle file(s).	2109	Duplicate domain or handle Escrow Record found in deposit.
When handles are used, all referenced contact handles must be present in the data escrow deposit files.	2110	Handle reference by Escrow Record not found.
- Frequency of "Full" deposits must comply with the schedule defined in Section 2.1.3, in accordance with the registrar deposit schedule as notified by ICANN. - A "Full" deposit may be received in place of a "Differential" deposit.	2201	"Full" data escrow deposit expected but received "Differential" instead.
The data escrow deposit date, as indicated in the file naming convention defined in Section 4.1.21, must not be a future date.	2202	Data Escrow deposit date is in the future.
Once a data escrow deposit has been received and passed the verification process, no additional versions of such deposit may be accepted for the same deposit date and registrar.	2203	A data escrow deposit has been already successfully verified for that date.