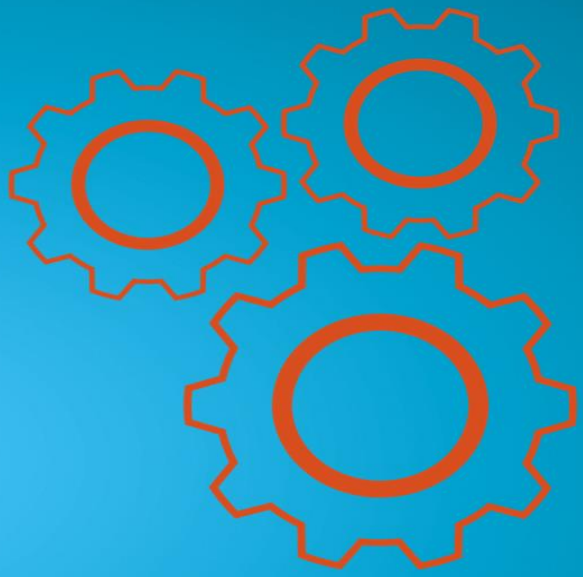
TECHNICAL ONBOARDING FOR RDE V3.2.1



https://denic-services.de

November 2023

Back to Content →

Overview

This manual describes the onboarding process to our system through our **Control Center (CC)**. This is the second part, technical onboarding.

During the onboarding process, you will always have the menu on the left side with the next steps. A completed step has a checkmark. All steps must be completed.

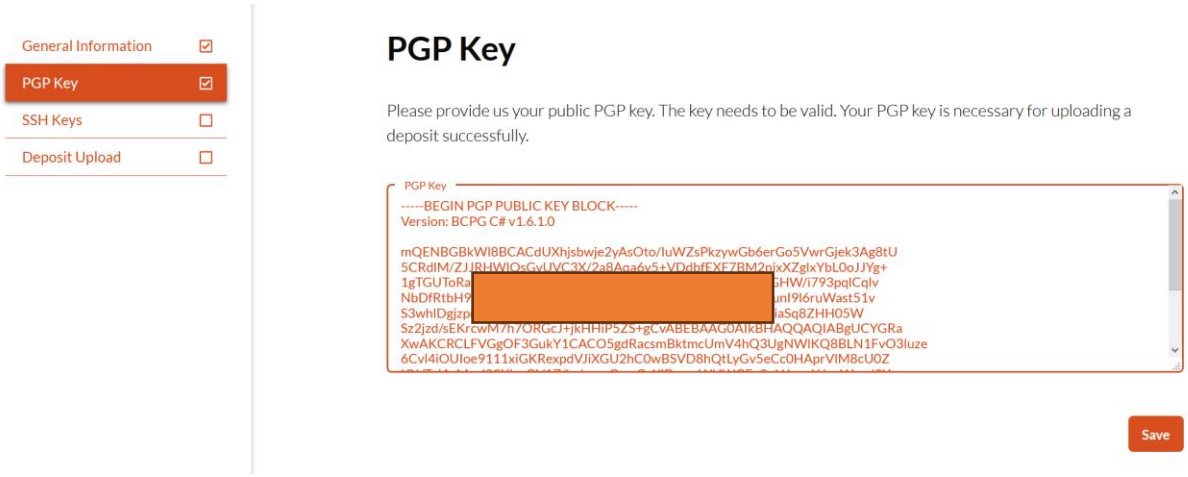
1. Continue Email

After DocuSign is finished, the CC Admin will receive a Continue Email with a link to our CC. After login, the Technical Onboarding starts.

If you have a Back-end Provider/Operator you may ask him for assistance.

2. PGP Key

Here you may provide us your public PGP key. The key needs to be valid. Your PGP key is necessary for uploading a deposit successfully.



For creating a PGP Key we recommend to use GnuPG:

- https://gnupg.org (Linux)
- https://www.gpg4win.org (Windows)

Validation period of at least five (5) years and length 2048 Bit.

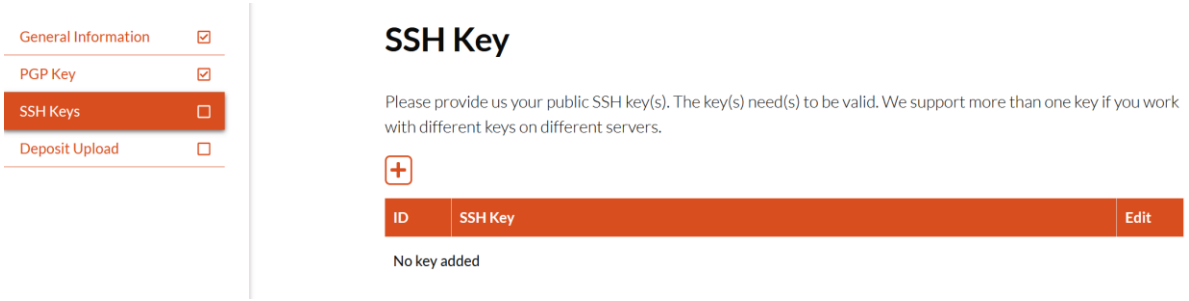
Accepted Algorithms

RIPEMD160withRSA	SHA256withECDSA	SHA512withECDSA
RIPEMD160withECDSA	SHA384withDSA	SHA256withRSA
RIPEMD256withRSA	SHA384withECDSA	SHA384withRSA
SHA256withDSA	SHA512withDSA	SHA512withRSA

Back to Content →

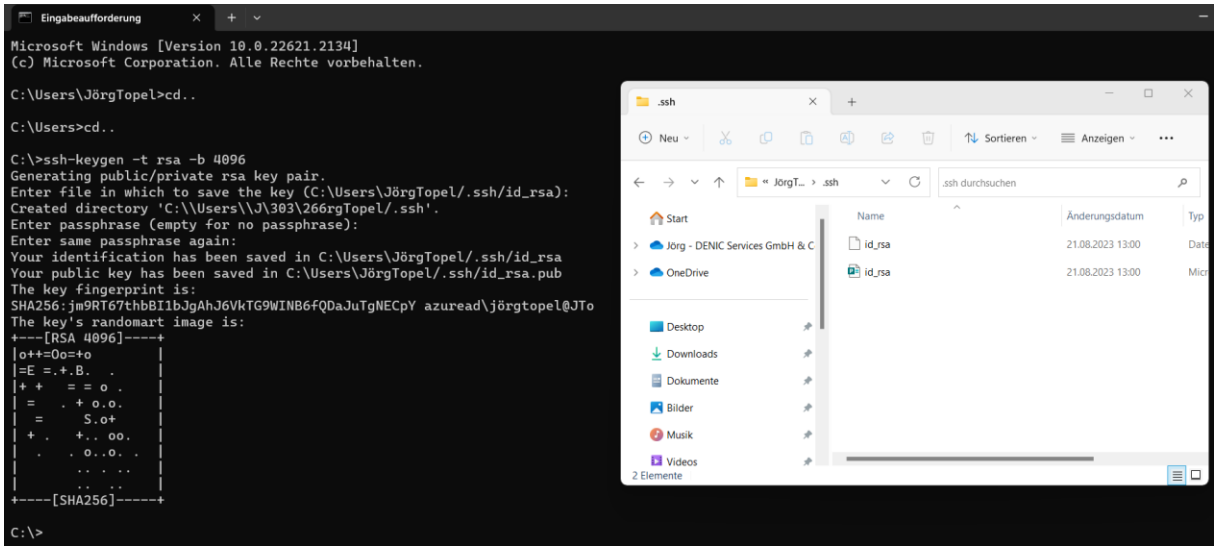
3. SSH Keys

Here you can add your public SSH key for logging in to our SFTP server. You may provide more than one key.



You can use ssh-keygen at the command line for creating the SSH Key.

As an example: ssh-keygen -t rsa -b 4096



Server Upgrade or Changes

Requirements

If you experience trouble using the SSH Key after you have updated SFTP Servers, you can try to use some of this:

1. Generate a new key with the secure algorithm ed25519 and exchange the stored public key in the CSP. (Recommended)
2. If you want to continue using the old RSA key, you can change the ~/.ssh/config to hard-activate the RSA algorithm again, see the Potentially-incompatible changes section in the release note on https://www.openssh.com/txt/release-8.8
3. Expand the SFTP command with the argument -oPubkeyAcceptedAlgorithms=+ssh-rsa, this will allow RSA support directly for this connection and the FTP connect should work again.

4. Deposit Upload

For Uploading you may use any SFTP application via terminal or client such as escrow-rde-client or FileZilla.

Back to Content →

4.1. escrow-rde-client

config-rde-client-example-v1.0.0.yaml

```yaml
# Your IANA id.
ianaID: 9999

# depositBaseDir - the directory where the depositfiles can be found
depositBaseDir: examples/deposits/rde

# runDir - the directory where the processed files will be located
runDir: deposit-run-rde

# compressAndEncrypt - if set to true, a hashfile of the depositfiles
# will be created and the files will be compressed and encrypted.
# set this to false if you just want to do validation of your files.
compressAndEncrypt: true

# uploadFiles - if set to true, the processed files will
# be uploaded to the escrow agent
uploadFiles: false

# multi - if set to true, all deposit files (except hash) are assumed
# to be part of a sequence of files. You need to add a sequence number
# at the end of the filename like "foobar_full_1.csv", "foobar_full_2.csv", ...
# Deposit files without a sequence number will not be processed when multi
# is active. Only the first file of the sequence should contain the header defin
multi: false
```

The client takes care of the following tasks:

- Validates the RDE deposits
- Creates hashfile over the content of delivery
- Compresses, encrypt and sign the deposit files
- Uploads the files to the Data Escrow Agent

Important things to remember

- Using the correct credentials and SFTP server
- Using the correct PGP keys
  - Using our public PGP key for encryption
  - Using your private PGP key for signing
- Using the correct SSH key (or password) for login

Click here for the manual: escrow-rde-client. The Client can be downloaded there as well.

4.1.1. Data Escrow RDE Client Manual

Prerequisites

- Your Data Escrow Agent (DEA) must have set up your public PGP-Key- and your public SSH-key parts along with your account

The escrow-rde-client will need access to the following files:

- Your private (encrypted) PGP key to sign the deposit files

Back to Content →

- Your private SSH key for authentication at the SFTP service
- The public PGP key of the Data Escrow Agent to encrypt the deposit files.

Download the client.

Download the client package for your platform (linux/windows) using the links above and extract it to a desired folder.

Prepare the configuration file

- Generate a configuration file with ./escrow-rde-client -i
- rename the generated configuration file to config.yaml (optional)
- edit the parameters in the configuration file

Prepare your deposit files

- to upload a deposit for the **current day** the source filenames (.csv) can have any filename as long as the name includes full, inc and hdl (denoting full-deposit, incremental deposit and handle file)
- to upload a deposit for any past day, the filenames must follow this convention:

```
<IANAID>_RDE_<YYYY>-<MM>-<DD>_full.csv (or) <IANAID>_RDE_<YYYY>-<MM>-
<DD>_inc.csv
<IANAID>_RDE_<YYYY>-<MM>-<DD>_hdl.csv
```

Replace your IANA ID, and year/month/day.

Splitted deposit files

Source files with more than 1 million rows or 1 gigabyte of size need to be splitted into a sequence of files. The consecutive sequence numbers start with 1 and are contained in the filename by the following convention:

```
<IANAID>_RDE_<YYYY>-<MM>-<DD>_full_#.csv (or) <IANAID>_RDE_<YYYY>-<MM>-
<DD>_inc_#.csv
<IANAID>_RDE_<YYYY>-<MM>-<DD>_hdl_#.csv
```

The symbol # is replaced by the corresponding sequence numbers. Only the first file should contain row headers, all other files just start with the successive content lines. To enable splitted deposits you need to update your configuration file:

```
multi: true
```

Run the client

```
./escrow-rde-client -c config.yaml
```

You can additionally use the -s flag to only print the last validation error message. To print validation output directly to a file, add the following configuration line to your yaml config file:

Back to Content →

```
logFile: /path/to/your/log/file
```

Troubleshooting

This section discusses some known problems and possible solutions.

Crashes due to out-of-memory errors

Out-of-memory errors can cause the application to crash without further error messages. If you run low on memory during computation, consider activating the file system cache in the configuration file:

```
useFileSystemCache: true
```

This will drastically reduce the amount of memory required but also increases computation time.

You can report problems with this tool via e-mail to escrow@denic-services.de

Example data

Single-file full deposit, with handle references, *full.csv*. These examples may be splitted according the conventions of multi-file deposits (see above).

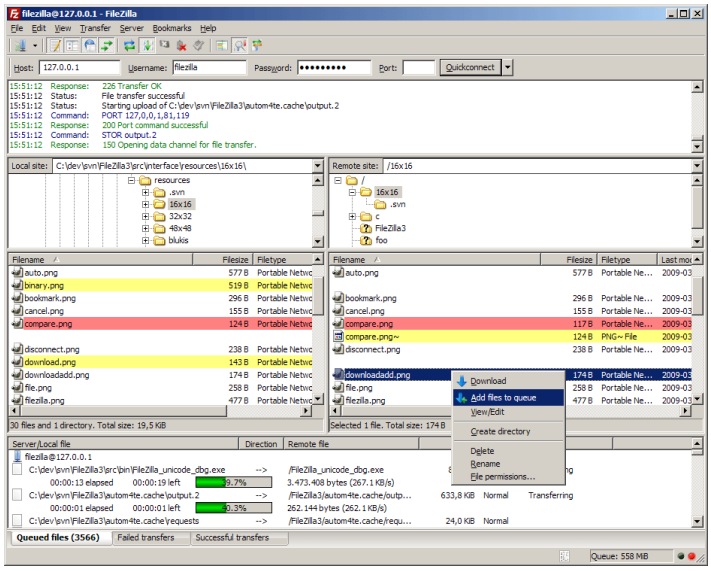
```
"domain","ns1","ns2","ns3","ns4","expiration_date","rt-handle","tc-handle","ac-handle","bc-handle","prt-handle","ptc-handle","pac-handle","pbc-handle"
"foobar0.test","ns1.dns.test","ns2.dns.test","ns3.dns.test","ns4.dns.test","2018-05-30 12:30:45","foo-123","foo-123","foo-123","foo-123","foo-123","foo-123","foo-123","foo-123"
"foobar1.test","ns1.dns.test","ns2.dns.test","ns3.dns.test","ns4.dns.test","2018-08-30T12:30:45Z","foo-123","foo-123","foo-123","foo-123","foo-123","foo-1235","foo-123","foo-123"
"foobar2.test","ns1.dns.test","ns2.dns.test","ns3.dns.test","ns4.dns.test","2018-05-30T12:30:45Z","foo-123","foo-123","foo-123","foo-123 foo-1234","foo-123","foo-1235","foo-123","foo-123"
"foobar3.test","ns1.dns.test","ns2.dns.test","ns3.dns.test","ns4.dns.test","2018-05-30 12:30:45","foo-123","foo-1234","foo-123","foo-123 foo-1235",,,,
"foobar4.test","ns1.dns.test","ns2.dns.test","ns3.dns.test","ns4.dns.test","2018-05-30 12:30:45","foo-123","foo-1234","foo-123","foo-123",,,,
```

Handles used in the example data above, *hdl.csv*:

```
"handle","name","address","state","zip","city","country","email","phone","fax"
"foo-123","Foo Bar","At Home 123","Foostate",12345,"Foocity","Fooland","foo@bar.test","+555.123-345-123",0
"foo-1234","Alice Bob","742 Evergreen Terrace","Foostate","12345","Foocity","Fooland","alice@bar.test","+555.123-345-678","0"
"foo-1235","Bob Alice","Escaped ""Quote"" Street 42","Barstate","54321","Barcity","Barland","bob@bar.test","+555.123-345-345","0"
```

Back to Content →

4.2. FileZilla



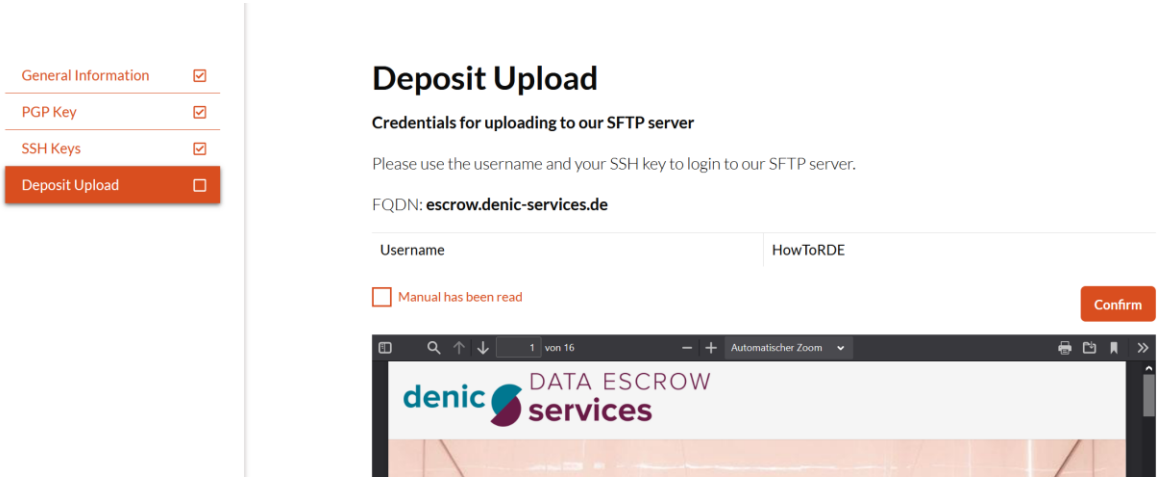
https://filezilla-project.org

The number of simultaneous connections must be set to 1. How to set it in FileZilla:

> “Transfer Settings” → “Limit number of simultaneous connections” and set to 1.

5. SFTP Credentials

On this page you will find your SFTP credentials as well as information about deposits, preparation and upload. Please do not forget to check the checkbox, that you have read this manual.

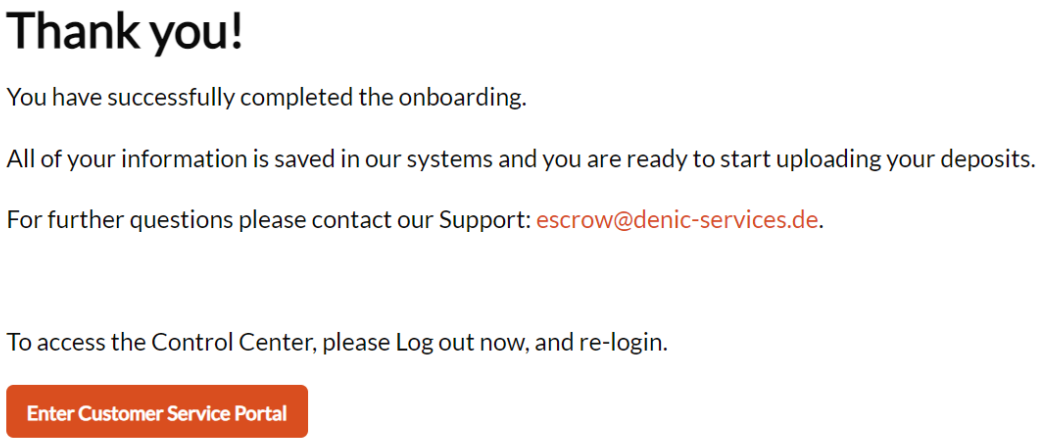


Back to Content →

5.1. Technical Onboarding completion

As soon as you flag the box and click on “Confirm” you completed the Technical Onboarding. Please go ahead and enter the Control Center in daily business. This step is necessary to view your success for the next steps.

Note: We offer a third manual for the CC in daily business.



5.2. Deposit preparation

Please prepare your deposit files according to the official ICANN specifications:

ICANN RDE Specifications.

!We **highly recommend** using full deposit, including the handle references.

Single-file full deposit, with handle references, *full.csv*. These examples may be splitted according the conventions of multi-file deposits (see above).

```
"domain","ns1","ns2","ns3","ns4","expiration_date","rt-handle","tc-handle","ac-handle","bc-handle","prt-handle","ptc-handle","pac-handle","pbc-handle"
"foobar0.test","ns1.dns.test","ns2.dns.test","ns3.dns.test","ns4.dns.test","2018-05-30 12:30:45","foo-123","foo-123","foo-123","foo-123","foo-123","foo-123","foo-123","foo-123"
"foobar1.test","ns1.dns.test","ns2.dns.test","ns3.dns.test","ns4.dns.test","2018-08-30T12:30:45Z","foo-123","foo-123","foo-123","foo-123","foo-123","foo-1235","foo-123","foo-123"
"foobar2.test","ns1.dns.test","ns2.dns.test","ns3.dns.test","ns4.dns.test","2018-05-30T12:30:45Z","foo-123","foo-123","foo-123","foo-123 foo-1234","foo-123","foo-1235","foo-123","foo-123"
"foobar3.test","ns1.dns.test","ns2.dns.test","ns3.dns.test","ns4.dns.test","2018-05-30 12:30:45","foo-123","foo-1234","foo-123","foo-123 foo-1235",,,,
"foobar4.test","ns1.dns.test","ns2.dns.test","ns3.dns.test","ns4.dns.test","2018-05-30 12:30:45","foo-123","foo-1234","foo-123","foo-123",,,,
```

Back to Content →

5.2.1. Further Instructions on deposit preparation

1. Please see section 4.1.18. Your deposit must be accompanied by a hash file. The hash file must contain the hash sum of the domain files before the files have been compressed and signed/encrypted. As stated in the specifications:

"Each line shall consist of the hash value for one file, followed by whitespace, followed by the name of the file."

Please note, DENIC Services requires SHA-256 hash sums. Example of hash.txt data format:

```
c58fcf{...hashcontent....}3d2e5c4ba74 $account_iana_id_c_RDE_$account_date_modified_full_1.csv

c58fcf5{..hashcontent...}2e5c4ba74 $account_iana_id_c_RDE_$account_date_modified_hdl_1.csv
```

2. All file names must appear in the format specified in section 4.1.21: [IANA ID]_RDE_[YYYY-MM-DD]_[full/inc/hdl/hash]_[#] According to the specifications, your files must be named as follows:

```
$account_iana_id_c_RDE_$account_date_modified_full_1.csv
$account_iana_id_c_RDE_$account_date_modified_hdl_1.csv
$account_iana_id_c_RDE_$account_date_modified_hash.txt
```

The "full_1" file must contain the number of the domain records. To comply with the format specified for the use of handles, the header row must appear as follows:

```
"domain_name","nameservers","expiration_date","rt_handle","tc_handle","ac_handle","bc_handle"
```

The "hdl_1" file must contain the complete contact information for each handle ID used for the domains in the "full_1" file. The header row must appear as follows:

```
"handle","name","address","state","zip","city","country","email","phone","fax"
```

In the examples above, a proper abbreviation has been used as stated in Section 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'); field names referring to the administrative contact shall be prefixed with the string 'ac-' (as in 'ac-name'); field names referring to the technical contact shall be prefixed with the string 'tc-' (as in 'tc-country'), and field names referring to a billing contact shall be prefixed with 'bc-' (as in 'bc-phone')"

In case you have more than one handle contact in the same role (rt, ac, tc or bc), two different syntaxes are supported:

- Include all handles concatenated with spaces under the regular field name, e.g.:

Back to Content →

tc-handle
HANDLE1 HANDLE2

- Use separate field names for each handle contact with the syntax roleprefix-N-fieldname, e.g.: tc-1-handle, tc-2-handle

To comply with section 4.1.13, the decimal character has been replaced with the underscore character:

"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', upper case 'A' through upper case '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."

To comply with section 4.1.6, the field for "contact.tld" has been removed.

To comply with section 4.1.5 and to support delivery of beneficial user information in case of privacy or proxy services, we suggest usage of the following additional fields

```
"prt_handle","ptc_handle","pac_handle","pbc_handle"
```

which can be added at the end of the mandatory escrow records. The referenced handles must obviously appear in the handle file.

We strongly recommend using the aforementioned header field names. Otherwise, you are obliged to comply with section 4.1.15. Usage of undocumented header field names may lead to unexpected results in case of an ICANN audit.

3. After you have created your files, the full and hdl files must be compressed first with gzip compression:

```
Output= $account_iana_id_c_RDE_$account_date_modified_full_1.csv.gz
Output=$account_iana_id_c_RDE_$account_date_modified_hdl_1.csv.gz
```

4. After the files have been compressed, you must sign and encrypt the compressed files. Please sign first with your private key and then encrypt with DENIC's public key. Signature and encryption should be done in the same pass.

```
Output= $account_iana_id_c_RDE_$account_date_modified_full_1.csv.gz.gpg
Output= $account_iana_id_c_RDE_$account_date_modified_hdl_1.csv.gz.gpg
```

Back to Content →

5. You must upload all files to your SFTP account with DENIC Data Escrow Services. Please note that the session-close-event is used as a trigger to determine the completeness of the deposit, so make sure to upload all files through the same sftp connection/session.

$account_iana_id_c_RDE_$account_date_modified_full_1.csv.gz.gpg $account_iana_id_c_RDE_$account_date_modified_hdl_1.csv.gz.gpg $account_iana_id_c_RDE_$account_date_modified_hash.txt

You must use our public production key to encrypt the deposit:

DENIC Services RDE public PGP Key.

5.3. Deposit upload to DENIC Services SFTP server

Please use the provided credentials for uploading to our SFTP server.

Protocol: SFTP FQDN/Host: Please use escrow.denic-services.de for storage in EU FQDN/Host: Please use escrow.denic-services.com for storage in USA Username: RDE-{your IANA ID}, e.g., RDE-9999 Passwort: Your SSH key (or password) Please note: These are only example credentials. You can find your credentials later in the CC as soon as you completed the Technical Onboarding part.

6. Successful First Deposit

When the Technical Onboarding has been completed you can upload your first full deposit to our SFTP server.

As soon as you uploaded it successfully, we will be starting the obligated first RDAP Audit for the delivered deposit. Please take care on section 6.1, RDAP Audit. After the successful audit our reporting to ICANN will start.

6.1 RDAP Audit

Please bear in mind that your first deposit always must be audited by Denic Services. This audit may only be done using RDAP Service with the RDAP Server which you have listed on the IANA Website. Please assure that we can audit 20 randomly selected domains per IANA ID in a row, and the RDAP Server is responding and answering with the data which are used in the deposit. RDAP query limitations may result in a failed audit.

6.2 ICANN reporting

Remember that you must keep uploading deposits to your current Data Escrow Agent until the Final Transition Notice from ICANN arrives (see below).

Back to Content →

7. Final Transition Notice

After ICANN validates your successful upload to our servers, they will send a Final Transition Notice. From that point on the DEA change is completed and we are your Data Escow Agent.

You can stop delivering deposits to your old Data Escrow Agent now.

Congratulations!

I - Contact and Support

	DENIC Services GmbH & Co. KG Heinrich-Hertz-Str. 6 64295 Darmstadt Germany	
	Phone	+49-6151-62 92 710
	Fax	+49-6151-62 92 711
	E-Mail	escrow@denic-services.de
	Internet	https://www.denic-services.de/en

Back to Content →