Escrow for (cc)TLDs

by David Kipling

Agenda

- **Why Escrow your data?**
- **Latest ICANN requirements**
- **Data Security**
- **Data Integrity**
- **Keeping you informed**
- **Q&A**

Why Escrow your data?

Data Security

- Enhance DR Processes
- Verify Impartially and Externally

Secure Business & Increase Revenue

- Customer protection
- Builds trust and reputation

Keeping up with the new gTLDs

- Essential stakeholder protection
- A competitive advantage

Why Escrow your data?

- Confidence your data is Secured, Accessible and Usable

- Gives customers Confidence in your services

- Independent verification of you most Valuable asset
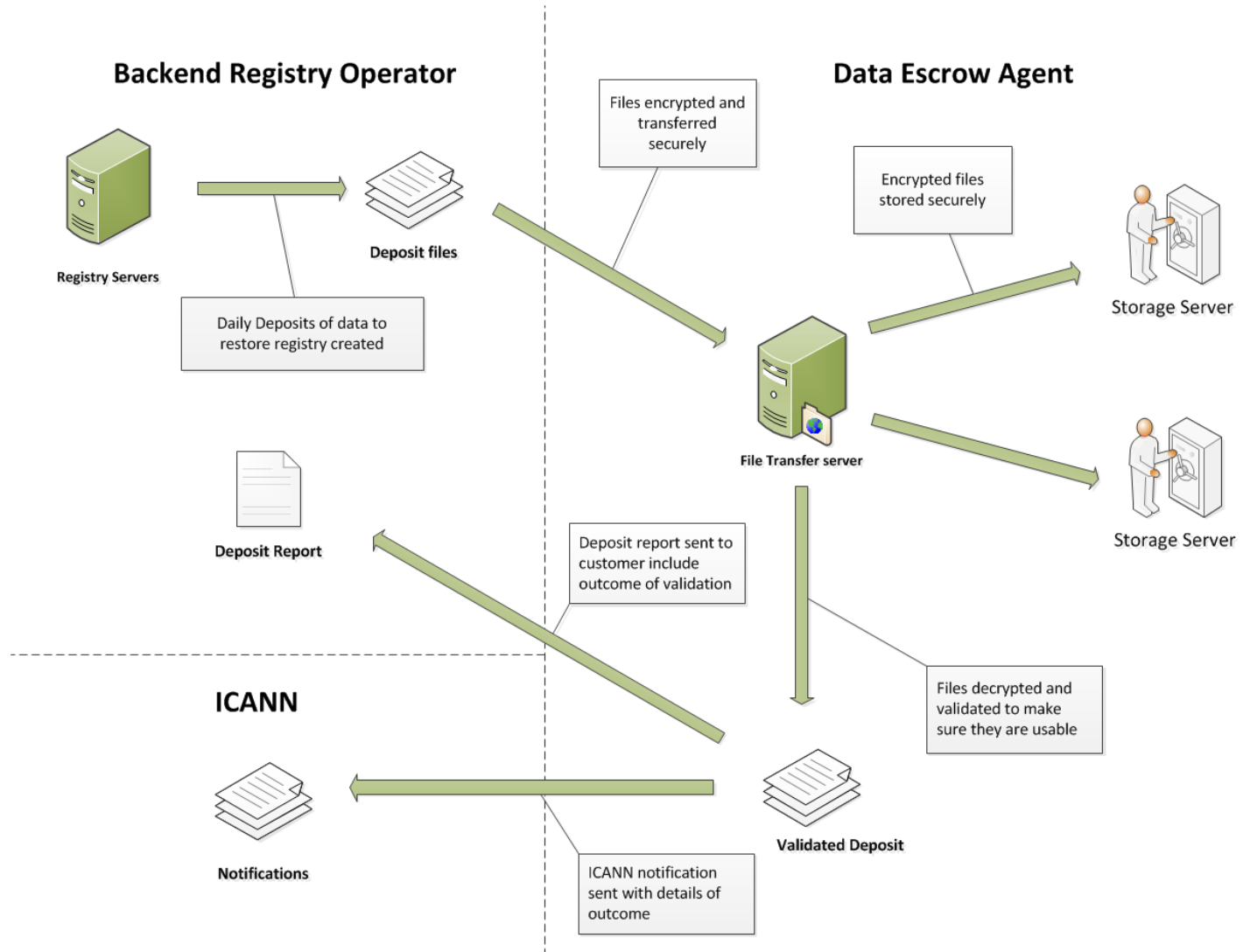
Latest ICANN requirements

New gTLDs

- Daily deposits of data

- Data MUST conform to agreed ICANN format

- Deposits MUST be validated by the Escrow Agent using ICANN rules

- Deposit notifications are sent to ICANN and the Registry operator

- Emergency Back End Registry Operators to resume services

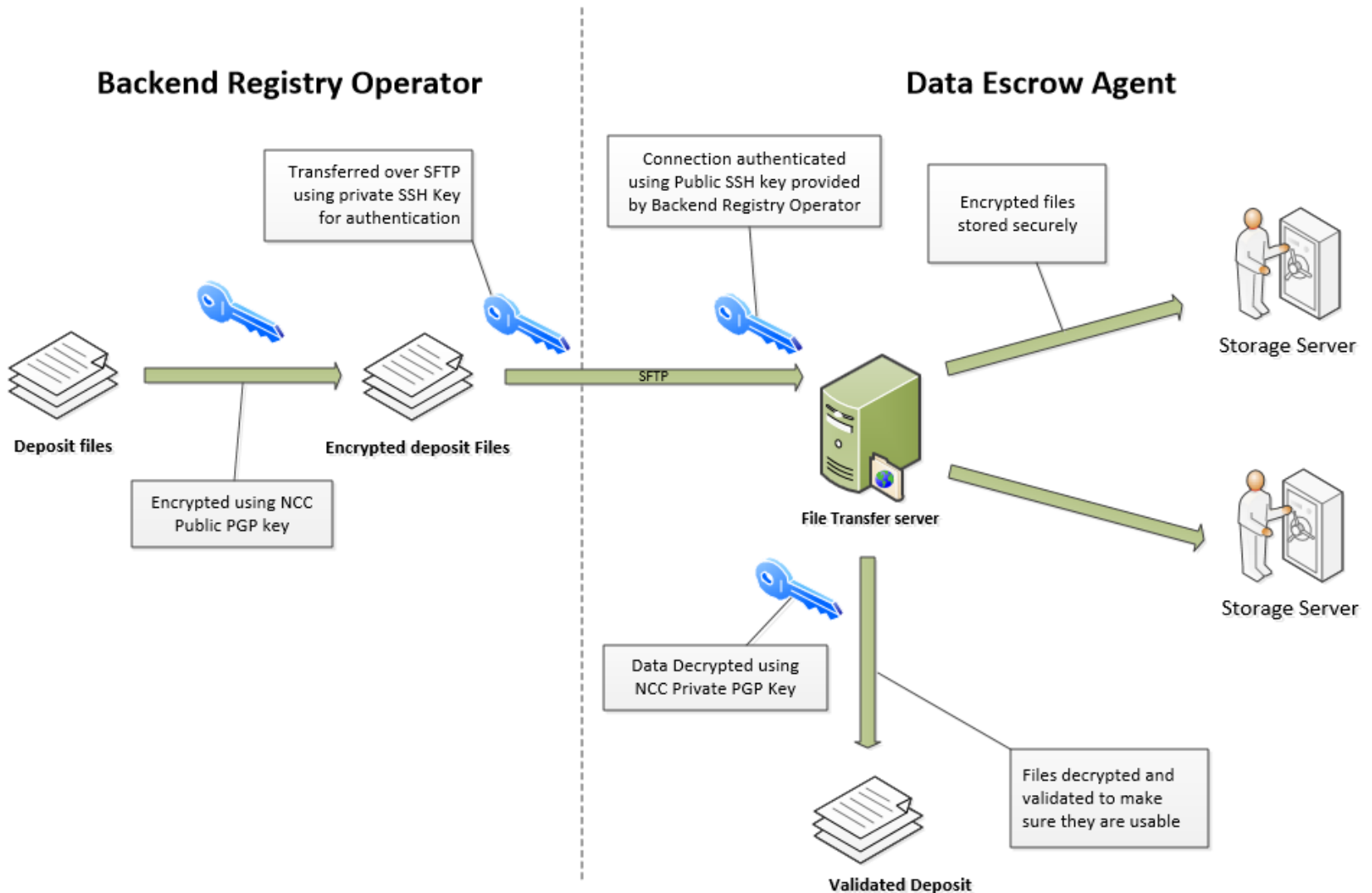# Latest ICANN requirements

Data Security

How to secure the data

Transfer Protocols	SFTP/FTPS/HTTPS
Authentication	SSH keys/User/Password
Data Encryption	PGP(GPG)
File Integrity	Digital Signatures

Diagram of Escrow Security Process

Backend Registry Operator

Data Escrow Agent

Transferred over SFTP using private SSH Key for authentication

Connection authenticated using Public SSH key provided by Backend Registry Operator

Encrypted files stored securely

Deposit files

Encrypted deposit Files

SFTP

Storage Server

Encrypted using NCC Public PGP key

File Transfer server

Storage Server

Data Decrypted using NCC Private PGP Key

Files decrypted and validated to make sure they are usable

Validated Deposit

9

Data Integrity

How to ensure Data Integrity

- Digital Signatures using file checksums

- Schema checks

- Verification of contents

ICANN Extended Verification

1. Check deposit validates to schemas defined

2. Count the objects and validate that number of objects is equal to the number objects reported in the <header> element of the escrow deposit

3. All contacts linked to domain names are present.

4. All registrars linked to other objects are present.

5. An FQDN exists only as a domain name or NNDN.

6. The elements listed in the <policy> element are present.

7. All idnTableRef definitions linked from other objects are present.

Deposit Formats (XML)

```xml
<?xml version="1.0" encoding="UTF-8"?>
<rde:deposit type="FULL" id="20101017001" prevId="20101010001"
  xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
  xmlns:rde="urn:ietf:params:xml:ns:rde-1.0"
  ...
  xmlns:epp="urn:ietf:params:xml:ns:epp-1.0">

  <rde:watermark>2010-10-17T00:00:00Z</rde:watermark>
  <rde:rdeMenu>
    <rde:version>1.0</rde:version>
    <rde:objURI>urn:ietf:params:xml:ns:rdeHeader-1.0</rde:objURI>
    <rde:objURI>urn:ietf:params:xml:ns:rdeContact-1.0</rde:objURI>
    <rde:objURI>urn:ietf:params:xml:ns:rdeHost-1.0</rde:objURI>
    <rde:objURI>urn:ietf:params:xml:ns:rdeDomain-1.0</rde:objURI>
    <rde:objURI>urn:ietf:params:xml:ns:rdeRegistrar-1.0</rde:objURI>
    <rde:objURI>urn:ietf:params:xml:ns:rdeIDN-1.0</rde:objURI>
    <rde:objURI>urn:ietf:params:xml:ns:rdeNNDN-1.0</rde:objURI>
    <rde:objURI>urn:ietf:params:xml:ns:rdeEppParams-1.0</rde:objURI>
  </rde:rdeMenu>

  <!-- Contents -->
  <rde:contents>
    <!-- Header -->
    <rdeHeader:header>...</rdeHeader:header>
    <rdeDom:domain>...</rdeDom:domain>
    <rdeDom:domain>...</rdeDom:domain>
    <rdeHost:host>...</rdeHost:host>
    <rdeContact:contact>...</rdeContact:contact>
    <rdeRegistrar:registrar>...</rdeRegistrar:registrar>
    <rdeIDN:idnTableRef id="pt-BR">...</rdeIDN:idnTableRef>
    <rdeNNDN:NNDN>...</rdeNNDN:NNDN>
    <rdeEppParams:eppParams>...</rdeEppParams:eppParams>
    <rdePolicy:policy element="rdeDom:registrant" />
  </rde:contents>
</rde:deposit>
```

```xml
<rdeDom:domain>
  <rdeDom:name>example1.test</rdeDom:name>
  <rdeDom:roid>Dexample1-TEST</rdeDom:roid>
  <rdeDom:status s="ok"/>
  <rdeDom:registrant>jd1234</rdeDom:registrant>
  <rdeDom:contact type="admin">sh8013</rdeDom:contact>
  <rdeDom:contact type="tech">sh8013</rdeDom:contact>
  <rdeDom:ns>
    <domain:hostObj>ns1.example.com</domain:hostObj>
    <domain:hostObj>ns1.example1.test</domain:hostObj>
  </rdeDom:ns>
  <rdeDom:clID>RegistrarX</rdeDom:clID>
  <rdeDom:crRr client="jdoe">RegistrarX</rdeDom:crRr>
  <rdeDom:crDate>1999-04-03T22:00:00.0Z</rdeDom:crDate>
  <rdeDom:exDate>2015-04-03T22:00:00.0Z</rdeDom:exDate>
</rdeDom:domain>
```

Deposit Formats (CSV)

```xml
<?xml version="1.0" encoding="UTF-8"?>
<rde:deposit
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:rde="urn:ietf:params:xml:ns:rde-1.0"

   xmlns:csvIDN="urn:ietf:params:xml:ns:csvIDN-1.0"

   type="FULL"
   id="20101017001" prevId="20101010001">
   <rde:watermark>2010-10-18T00:00:00Z</rde:watermark>
   <rde:rdeMenu>
    <rde:version>1.0</rde:version>
    <rde:objURI>urn:ietf:params:xml:ns:csvDomain-1.0</rde:objURI>
    <rde:objURI>urn:ietf:params:xml:ns:csvHost-1.0</rde:objURI>
    <rde:objURI>urn:ietf:params:xml:ns:csvContact-1.0</rde:objURI>
    <rde:objURI>urn:ietf:params:xml:ns:csvRegistrar-1.0</rde:objURI>
    <rde:objURI>urn:ietf:params:xml:ns:csvIDN-1.0</rde:objURI>
   </rde:rdeMenu>
   <rde:contents>
    <csvDomain:contents>...</csvDomain:contents>
    <csvHost:contents>...</csvHost:contents>
    <csvContact:contents>...</csvContact:contents>
    <csvRegistrar:contents>...</csvRegistrar:contents>
    <csvIDN:contents>...</csvIDN:contents>
   </rde:contents>
</rde:deposit>
```

```xml
<csvContact:contents>
   <rdeCsv:csv name="contact">...</rdeCsv:csv>
   <rdeCsv:csv name="contactStatuses">...</rdeCsv:csv>
   <rdeCsv:csv name="contactPostal">...</rdeCsv:csv>
   <rdeCsv:csv name="contactTransfer">...</rdeCsv:csv>
   <rdeCsv:csv name="contactDisclose">...</rdeCsv:csv>
</csvContact:contents>
```

Deposit Formats (CSV)

```xml
<csvContact:contents>
    <rdeCsv:csv name="contact">...</rdeCsv:csv>
    <rdeCsv:csv name="contactStatuses">...</rdeCsv:csv>
    <rdeCsv:csv name="contactPostal">...</rdeCsv:csv>
    <rdeCsv:csv name="contactTransfer">...</rdeCsv:csv>
    <rdeCsv:csv name="contactDisclose">...</rdeCsv:csv>
</csvContact:contents>
```

```xml
<rdeCsv:csv name="contactStatuses">
  <rdeCsv:sep>,</rdeCsv:sep>
  <rdeCsv:fields>
      <csvContact:fId/>
      <csvContact:fStatus/>
      <rdeCsv:fStatusDescription/>
      <rdeCsv:fLanguage/>
    <rdeCsv:fCrRr/>
    <rdeCsv:fCrID/>
    <rdeCsv:fCrDate/>
    </rdeCsv:fields>
  <rdeCsv:files>
    <rdeCsv:file
      cksum="1234567890 98765432">
      contactStatuses-YYYYMMDD.csv
    </rdeCsv:file>
  </rdeCsv:files>
</rdeCsv:csv>
```

```
sh8013,clientUpdateProhibited,"Disallow update",en,registrarX,clientY,2009-12-03T09:05:00.0Z
sh8013,clientDeleteProhibited,"Disallow delete",en,registrarX,clientY,2010-12-04T10:05:00.0Z
mycontactid,ok,,,registrarX,clientY,2011-10-03T09:05:00.0Z
```

Validating the deposit against the schema

```
<rdeDom:domain>
    <rdeDom:name>The quick brown fox jumps over the lazy dog</rdeDom:name>
    <rdeDom:roid>The quick brown fox jumps over the lazy dog</rdeDom:roid>
    <rdeDom:status s="ok"/>
    <rdeDom:registrant>The quick brown fox jumps over the lazy dog</rdeDom:registrant>
    <rdeDom:contact type="admin">The quick brown fox jumps over the lazy dog</rdeDom:contact>
    <rdeDom:contact type="tech">The quick brown fox jumps over the lazy dog</rdeDom:contact>
    <rdeDom:ns>
        <domain:hostObj>The quick brown fox jumps over the lazy dog</domain:hostObj>
        <domain:hostObj>The quick brown fox jumps over the lazy dog</domain:hostObj>
    </rdeDom:ns>
    <rdeDom:clID>The quick brown fox jumps over the lazy dog</rdeDom:clID>
    <rdeDom:crRr client="jdoe">The quick brown fox jumps over the lazy dog</rdeDom:crRr>
    <rdeDom:crDate>The quick brown fox jumps over the lazy dog</rdeDom:crDate>
    <rdeDom:exDate>The quick brown fox jumps over the lazy dog</rdeDom:exDate>
</rdeDom:domain>
```

Validating the deposit against the schema

```xml
<rdeDom:domain>
  <rdeDom:name>example1.test</rdeDom:name>
  <rdeDom:roid>Dexample1-TEST</rdeDom:roid>
  <rdeDom:status s="ok"/>
  <rdeDom:registrant>jd1234</rdeDom:registrant>
  <rdeDom:contact type="admin">*InvalidRef*</rdeDom:contact>
  <rdeDom:contact type="tech">sh8013</rdeDom:contact>
  <rdeDom:ns>
    <domain:hostObj>ns1.example.com</domain:hostObj>
    <domain:hostObj>ns1.example1.test</domain:hostObj>
  </rdeDom:ns>
  <rdeDom:clID>RegistrarX</rdeDom:clID>
  <rdeDom:crRr client="jdoe">RegistrarX</rdeDom:crRr>
  <rdeDom:crDate>1999-04-03T22:00:00.0Z</rdeDom:crDate>
  <rdeDom:exDate>2015-04-03T22:00:00.0Z</rdeDom:exDate>
</rdeDom:domain>
```

Extended Verification

- Count the objects and validate that number of objects is equal to the number objects reported in the <header> element of the escrow deposit

- All contacts linked to domain names are present.

- All registrars linked to other objects are present.

- An FQDN exists only as a domain name or NNDN.

- The elements listed in the <policy> element are present.

- All idnTableRef definitions linked from other objects are present.

Extended Verification

- Large files (Millions of records)

- Different formats CSV or XML

- Full, incremental and differential files

How to progress?

Extended verification
- Rules are in draft and allow for future updates

Heuristic analysis using notifications
- Use counts and alert if large change

IETF Forum discussions
- Place for the community to discuss validation steps
  http://www.ietf.org/mail-archive/web/ire

Keeping you informed

NCC Process

- Puts you the customer first

- Aggregates reports and billing to simplify

- Notifications by not only email but also by phone

- A quick clean portal to help with the resolution of failures

- NCC Welcomes feedback on how to make the process work for you

Ease of management

Ease of management

Ease of management

nccgroup
freedom from doubt

nccgroup *Escrow Portal*
freedom from doubt

Logged in as **depositor@nccgroup.com**   **Logout**

| Home | Contacts | FAQ | Contact Us |

Deposit - 1

Summary   ▲

Agreement Agreement 1
Recieved   04/04/2013 17:28:58
Type   Full
Watermark 04/04/2013 17:28:58
Status   ❌

**** Examining File 'ICANN deposit.xml' using schema 'RDE ****
01/01/2013 00:00:00 **** Validating Deposit ****
01/01/2013 00:00:00 **** Checking Schema ****
01/01/2013 00:00:00 **** Checking XML Schema Completed Total Errors=0 ****
01/01/2013 00:00:00 **** Check Object Counts ****
01/01/2013 00:00:00 Domains : Header=123456 Count=0 outcome=FAIL
01/01/2013 00:00:00 Hosts : Header=12345 Count=12345 outcome=PASS
01/01/2013 00:00:00 Contacts : Header=1234 Count=1234 outcome=PASS
01/01/2013 00:00:00 Registrars : Header=123 Count=123 outcome=PASS
01/01/2013 00:00:00 IDN : Header=1 Count=1 outcome=PASS
01/01/2013 00:00:00 NNDN : Header=1 Count=1 outcome=PASS
01/01/2013 00:00:00 EppParams : Header=1 Count=1 outcome=PASS

25

Summary

- **Why Registry Data Escrow is needed**

- **Latest ICANN requirements**

- **Data Security**

- **Data Integrity**

- **Keeping you informed**

Contact Us

Booth: 16

Tel: +44 (0)7976 013104

e-mail: registryescrow@nccgroup.com

Visit: www.nccgroup.com

Questions

UK Offices

Manchester - Head Office

Cheltenham

Edinburgh

Leatherhead

London

Thame

North American Offices

San Francisco

Atlanta

New York

Seattle

Chicago

Austin

Australian Offices

Sydney

European Offices

Amsterdam - Netherlands

Munich – Germany

Zurich - Switzerland