Industrial Internet Identifier Node (IIIN) Data Escrow Specification
draft-industrial-internet-identifier-data-escrow-02

Abstract

This document specifies the format and contents of data escrow
deposits targeted primarily for Industrial Internet Identifier Node
(IIIN) which provides identifier registration. However, this
specification was designed to be independent of the underlying
objects that are being escrowed, therefore it could be used for
purposes other than IIIN.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

   Industrial Internet Identifier Node (IIIN) Data Escrow is the
   process by which an IIIN periodically submits data deposits to a
   third-party called an escrow agent. These deposits comprise the
   minimum data needed by a third-party to resume operations if the
   IIIN cannot function and is unable or unwilling to facilitate an
   orderly transfer of service. For an IIIN, the data to be deposited
   would include all the objects related to registered identifier.

   The goal of data escrow is higher resiliency of registration
   services, for the benefit of Internet users. The beneficiaries of an
   IIIN are not just those registering information there, but all
   relying parties that need to identify the owners of objects.

In the context of industry identifier namespace, data escrow is a requirement for IIIN. There is also a similar requirement for IIIN accredited identifier registration node.

This document specifies a format for data escrow deposits independent of the objects being escrowed. A specification is required for each type of registry/set of objects that is expected to be escrowed.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Deposit. Deposits can be of two kinds: Full and Differential. For all kinds of deposits, the universe of registry objects to be considered for data escrow is those objects necessary in order to offer the registry services.

Differential Deposit. Contains data that reflects all transactions involving the database that were not reflected in the last previous Full, or Differential Deposit, as the case may be. Differential Deposit files will contain information from all database objects that were added, modified or deleted since the previous deposit was completed as of its defined Timeline Watermark.

Full Deposit. Contains the registry data that reflects the current and complete registry database and will consist of data that reflects the state of the IIIN as of a defined Timeline Watermark for the deposit.

Escrow Agent. The organization designated by the IIIN or the third-party beneficiary to receive and guard data escrow deposits from the IIIN.

Third-Party Beneficiary. Is the organization that, under extraordinary circumstances, would receive the escrow deposits the IIIN transferred to the escrow agent. This organization could be a backup IIIN, contracting party of the IIIN, etc.

Timeline Watermark. Point in time on which to base the collecting of database objects for a deposit. Deposits are expected to be consistent to that point in time.

3. General Conventions

The XML namespace prefix "inde" is used for the namespace
"urn:ietf:params:xml:ns:inde-1.0", but implementations MUST NOT
depend on it; instead, they should employ a proper namespace-aware
XML parser and serializer to interpret and output the XML documents.

The XML namespace prefix "indeObj1" and "indeObj2" with the
corresponding namespace "urn:ietf:params:xml:ns:indeObj1-1.0" and
"urn:ietf:params:xml:ns:indeObj2-1.0" are used as example data
escrow objects.

3.1. Date and Time

Numerous fields indicate "dates", such as the creation and expiry
dates for objects. These fields SHALL contain timestamp indicating
the date and time in UTC, specified in Internet Date/Time Format
(see [RFC3339], Section 5.6) with the time-offset specified as "Z".

3.2. IP Addresses

The syntax for IPv4 addresses described in this document MUST
conform to [RFC5730]. The syntax for IPv6 addresses described in
this document MUST conform to [RFC4291]. Practical considerations
for publishing IPv6 address information in zone files are documented
in [RFC2874] and [RFC3596]. A server MAY reject IP addresses that
have not been allocated for public use by IANA.

4. Protocol Description

The following is a format for data escrow deposits as produced by an
IIIN. The deposits are represented in XML. Only the format of the
objects deposited is defined, nothing is prescribed about the method
used to transfer such deposits between the IIIN and the escrow agent
or vice versa.

The protocol intends to be object agnostic allowing the "overload"
of abstract elements using the "substitutionGroup" attribute of the
XML Schema element to define the actual elements of an object to be
escrowed.

4.1. Root element <deposit>

The container or root element for an IIIN Data Escrow deposit is
<deposit>. This element contains the following child elements:
<watermark>, <indeMenu>, <deletes> and <contents> elements. This
element also contains the following attributes:

   o A REQUIRED "type" attribute that is used to identify the kind of
     deposit: FULL (Full), or DIFF (Differential).

   o A REQUIRED "id" attribute that is used to uniquely identify the
     escrow deposit. Each IIIN is responsible for maintaining its own
     escrow deposits identifier space to ensure uniqueness.

   o An OPTIONAL "prevId" attribute that can be used to identify the
     previous Differential or Full Deposit. This attribute MUST be
     used in Differential Deposits ("DIFF" type).

   o An OPTIONAL "resend" attribute that 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 IIIN
     for that specific date. The first time a deposit is generated the
     attribute is either omitted or MUST be "0". If a deposit needs
     to be generated again, the attribute MUST be set to "1", and so
     on.

   Example of a Full Deposit with the two example objects indeObj1 and
   indeObj2:

   <?xml version="1.0" encoding="utf-8"?>

   <inde:deposit xmlns:inde="urn:ietf:params:xml:ns:inde-1.0"
   xmlns:indeObj1="urn:ietf:params:xml:ns:indeObj1-1.0"
   xmlns:indeObj2="urn:ietf:params:xml:ns:indeObj2-1.0" type="FULL"
   id="20191017001">

     <inde:watermark>2019-12-20T00:00:00Z</inde:watermark>

     <inde:indeMenu>

       <inde:version>1.0</inde:version>

       <inde:objURI>urn:ietf:params:xml:ns:indeObj1-1.0</inde:objURI>

       <inde:objURI>urn:ietf:params:xml:ns:indeObj2-1.0</inde:objURI>

     </inde:indeMenu>

     <inde:contents>

       <indeObj1:indeObj1>

         <indeObj1:name>EXAMPLE1</indeObj1:name>

       </indeObj1:indeObj1>

```
      <indeObj2:indeObj2>

        <indeObj2:id>EXAMPLE2</indeObj2:id>

      </indeObj2:indeObj2>

    </inde:contents>

  </inde:deposit>
```

Example of a Differential Deposit with the two example objects
indeObj1 and indeObj2:

```
<?xml version="1.0" encoding="UTF-8"?>

  <inde:deposit

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

    xmlns:indeObj1="urn:ietf:params:xml:ns:indeObj1-1.0"

    xmlns:indeObj2="urn:ietf:params:xml:ns:indeObj2-1.0"

    type="DIFF" id="20191221001" prevId="20191220001">

    <inde:watermark>2019-12-21T00:00:00Z</inde:watermark>

    <inde:indeMenu>

      <inde:version>1.0</inde:version>

        <inde:objURI>

          urn:ietf:params:xml:ns:indeObj1-1.0

        </inde:objURI>

        <inde:objURI>

          urn:ietf:params:xml:ns:indeObj2-1.0

        </inde:objURI>

    </inde:indeMenu>

    <inde:deletes>

      <indeObj1:delete>
```

```
          <indeObj1:name>EXAMPLE1</indeObj1:name>

        </indeObj1:delete>

        <indeObj2:delete>

          <indeObj2:id>EXAMPLE2</indeObj2:id>

        </indeObj2:delete>

      </inde:deletes>

      <inde:contents>

        <indeObj1:indeObj1>

          <indeObj1:name>EXAMPLE3</indeObj1:name>

        </indeObj1:indeObj1>

        <indeObj2:indeObj2>

          <indeObj2:id>EXAMPLE4</indeObj2:id>

        </indeObj2:indeObj2>

      </inde:contents>

    </inde:deposit>
```

4.2. Child <watermark> element

A REQUIRED <watermark> element contains the data-time corresponding
to the Timeline Watermark of the deposit.

4.3. Child <indeMenu> element

This element contains auxiliary information of the data escrow
deposit. A REQUIRED <indeMenu> element contains the following child
elements:

o A REQUIRED <version> element that identifies the INDE protocol
   version.

o One or more <objURI> elements that contain namespace URIs
   representing the <contents> and <deletes> element objects.

4.4. Child <deletes> element

   This element SHOULD be present in deposits of type Differential. It
   contains the list of objects that were deleted since the base
   previous deposit. Each object in this section SHALL contain an
   identifier for the object deleted.

   This section of the deposit SHOULD NOT be present in Full Deposits.
   When rebuilding an IIIN it SHOULD be ignored if present in a Full
   Deposit.

   The specification for each object to be escrowed MUST declare the
   identifier to be used to reference the object to be deleted.

4.5. Child <contents> element

   This element of the deposit contains the objects in the deposit. It
   MUST be present in all type of deposits. It contains the data for
   the objects to be escrowed. The actual objects had to be specified
   individually.

   In the case of Differential Deposits, the objects indicate whether
   the object was added or modified after the base previous deposit. In
   order to distinguish between one and the other, it will be
   sufficient to check existence of the reference object of the
   previous deposit.

   When applying Differential Deposits (when rebuilding the IIIN from
   data escrow deposits) the relative order of the <deletes> elements
   is important, as is the relative order of the <contents> elements.
   All the <deletes> elements MUST be applied first, in the order that
   they appear. All the <contents> elements MUST be applied next, in
   the order that they appear.

   If an object is present in the <contents> section of several
   deposits (e.g. Full and Differential) the IIIN data from the latest
   deposit (as defined by the Timeline Watermark) SHOULD be used when
   rebuilding the IIIN.

5. Formal Syntax

5.1. INDE Schema

   Copyright (c) 2019 IETF Trust and the persons identified as authors
   of the code. All rights reserved.

   BEGIN

```
<?xml version="1.0" encoding="UTF-8"?>

<schema targetNamespace="urn:ietf:params:xml:ns:inde-1.0"

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

  xmlns="http://www.w3.org/2001/XMLSchema"

  elementFormDefault="qualified">

  <annotation>

    <documentation>

    Industrial Internet Identifier Node (IIIN) Data Escrow Schema

      </documentation>
```

```
      </annotation>

      <!-- Root element -->

      <element name="deposit" type="inde:escrowDepositType"/>

      <!-- INDE types -->

      <complexType name="escrowDepositType">

        <sequence>

          <element name="watermark" type="dateTime"/>

          <element name="indeMenu" type="inde:indeMenuType"/>

          <element name="deletes" type="inde:deletesType"
            minOccurs="0"/>

          <element name="contents" type="inde:contentsType"/>

        </sequence>

        <attribute name="type" type="inde:depositTypeType"
            use="required"/>

        <attribute name="id" type="inde:depositIdType"
            use="required"/>

        <attribute name="prevId" type="inde:depositIdType"/>

        <attribute name="resend" type="unsignedShort" default="0"/>

      </complexType>

      <!-- Menu type -->

      <complexType name="indeMenuType">

        <sequence>

          <element name="version" type="inde:versionType"/>

          <element name="objURI" type="anyURI" maxOccurs="unbounded"/>

        </sequence>

      </complexType>
```

```
    <!-- Deletes Type -->

    <complexType name="deletesType">

      <sequence minOccurs="0" maxOccurs="unbounded">

        <element ref="inde:delete"/>

      </sequence>

    </complexType>

    <element name="delete" type="inde:deleteType" abstract="true" />

    <complexType name="deleteType">

      <complexContent>

        <restriction base="anyType"/>

      </complexContent>

    </complexType>

    <!-- Contents Type -->

    <complexType name="contentsType">

      <sequence maxOccurs="unbounded">

        <element ref="inde:content"/>

      </sequence>

    </complexType>

    <element name="content"

    type="inde:contentType" abstract="true" />

    <complexType name="contentType">

      <complexContent>

        <restriction base="anyType"/>

      </complexContent>

    </complexType>
```

```
      <!-- Type of deposit -->

      <simpleType name="depositTypeType">

        <restriction base="token">

          <enumeration value="FULL"/>

          <enumeration value="DIFF"/>

        </restriction>

      </simpleType>

      <!-- Deposit identifier type -->

      <simpleType name="depositIdType">

        <restriction base="token">

          <pattern value="\w{1,13}"/>

        </restriction>

      </simpleType>

       <!--INDE version number is a dotted pair of decimal numbers -->

      <simpleType name="versionType">

        <restriction base="token">

          <pattern value="[1-9]+\.[0-9]+"/>

          <enumeration value="1.0"/>

        </restriction>

      </simpleType>

    </schema>

    END
```

6. Internationalization Considerations

Data escrow deposits are represented in XML, which provides native
support for encoding information using the Unicode character set and
its more compact representations including UTF-8. Conformant XML

processors recognize both UTF-8 and UTF-16. Though XML includes
provisions to identify and use other character encodings through use
of an "encoding" attribute in an <?xml?> declaration, use of UTF-8
is RECOMMENDED.

7. Security Considerations

This specification does not define the security mechanisms to be
used in the transmission of the data escrow deposits, since it only
specifies the minimum necessary to enable the rebuilding of an IIIN
from deposits without intervention from the original IIIN.

Depending on local policies, some elements or most likely, the whole
deposit will be considered confidential. As such the IIIN
transmitting the data to the escrow agent SHOULD take all the
necessary precautions like encrypting the data itself and/or the
transport channel to avoid inadvertent disclosure of private data.

It is also of the utmost importance the authentication of the
parties passing data escrow deposit files. The escrow agent SHOULD
properly authenticate the identity of the IIIN before accepting data
escrow deposits. In a similar manner, the IIIN SHOULD authenticate
the identity of the escrow agent before submitting any data.

Additionally, the IIIN and the escrow agent SHOULD use integrity
checking mechanisms to ensure the data transmitted is what the
source intended. Validation of the contents by the escrow agent is
RECOMMENDED to ensure not only the file was transmitted correctly
from the IIIN, but also the contents are also "meaningful".

8. IANA Considerations

This document uses URNs to describe XML namespaces and XML schemas
conforming to a registry mechanism described in [RFC3688]. Two URI
assignments need to be registered by the IANA.

Registration request for the INDE namespace:

     URI: urn:ietf:params:xml:ns:inde-1.0

   Registrant Contact: See the "Author's Address" section of this
document.

     XML: None. Namespace URIs do not represent an XML specification.

Registration request for the INDE XML schema:

       URI: urn:ietf:params:xml:schema:inde-1.0

       Registrant Contact: See the "Author's Address" section of this
    document.

       XML: See the "Formal Syntax" section of this document.

9. Privacy Considerations

   This specification defines a format that may be used to escrow
   personal data. The process of data escrow is governed by a legal
   document agreed by the parties, and such legal document must
   regulate the particularities regarding the protection of personal
   data.

10. References

10.1. Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
             Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119,
             March 1997, <https://www.rfc-editor.org/info/rfc2119>.
    [RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet:
              Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002,
              <https://www.rfc-editor.org/info/rfc3339>.
    [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119
              Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
              May 2017, <https://www.rfc-editor.org/info/rfc8174>.

10.2. Informative References

    [RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688,
              DOI 10.17487/RFC3688, January 2004,
              <https://www.rfc-editor.org/info/rfc3688>.
    [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing
              Architecture", RFC 4291, February 2006.
    [RFC5730] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)",
              STD 69, RFC 5730, August 2009.
    [RFC2874] Crawford, M. and C. Huitema, "DNS Extensions to Support
              IPv6 Address Aggregation and Renumbering", RFC 2874,July
              2000.
    [RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi,
              "DNS Extensions to Support IP Version 6", RFC 3596,
              October 2003.

11. Acknowledgments

    This document reference draft [draft-ietf-regext-data-escrow-03],
    thus, would like to thank the draft author G. Lozano. And would like
    to thank X. Fan, J. Chen, C. Ma, M. Chen, Z. Li who provided special
    important suggestions and invaluable comments. This document was
    prepared using 2-Word-v2.0.template.dot.

Authors' Address

    Hongjie Wu
    CAICT
    No.52 Huayuan North Road, Haidian District
    Beijing, Beijing, 100191
    China

    Phone: +86 186 0106 5934
    Email: wuhongjie@caict.ac.cn

    Jian Chen
    CAICT
    No.52 Huayuan North Road, Haidian District
    Beijing, Beijing, 100191
    China

    Phone: +86 138 1103 3332
    Email: chenjian3@caict.ac.cn

    Xiaotian Fan
    CAICT
    No.52 Huayuan North Road, Haidian District
    Beijing, Beijing, 100191
    China

    Phone: +86 134 0108 6945
    Email: fanxiaotian@caict.ac.cn

    Menlan Chen
    CAICT
    No.52 Huayuan North Road, Haidian District
    Beijing, Beijing, 100191
    China

    Phone: +86 139 1143 7301
    Email: chenmeilan@caict.ac.cn

Zhiping Li
CAICT
No.52 Huayuan North Road, Haidian District
Beijing, Beijing, 100191
China

Phone: +86 185 1107 1386
Email: lizhiping@caict.ac.cn