Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 24, 2019

U. Wisser
The Swedish Internet Infrastructure Foundation

March 23, 2019

Registry Lock Extension for the Extensible Provisioning Protocol (EPP) draft-wisser-registrylock-00

Abstract

This extensions defines an additional protective layer for changes to domain [RFC5731], host [RFC5732] and contact [RFC5733] objects managed through EPP.

EPP allows changes to objects only by the sponsoring client. EPP objects are usually managed by the sponsoring client on behalf of the sponsoring clients customers. There is no protection in EPP to changes to an object by the sponsoring client that are not authorized by the the customer.

This extension defines a protective layer that aims to break automated changes and work flows by requiring manual intervention by the sponsoring client or it's customers.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 24, 2019.

Copyright Notice

Table of Contents

1. Introduction

This extensions defines an additional protective layer for changes to domain [RFC5731], host [RFC5732] and contact [RFC5733] objects managed through EPP.

EPP allows changes to objects only by the sponsoring client. EPP objects are usually managed by the sponsoring client on behalf of the sponsoring clients customers. There is no protection in EPP to changes to an object by the sponsoring client that are not authorized by the the customer.

This extension defines a protective layer that aims to break automated changes and work flows by requiring manual intervention by the sponsoring client or it's customers.

1.1. Conventions Used in This Document

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 [RFC2119].

XML is case sensitive. Unless stated otherwise, XML specifications and examples provided in this document MUST be interpreted in the character case presented in order to develop a conforming implementation.

In examples, "C:" represents lines sent by a protocol client and "S:" represents lines returned by a protocol server. Indentation and white space in examples are provided only to illustrate element relationships and are not a REQUIRED feature of this protocol.

"regLock" is used as an abbreviation for "urn:ietf:params:xml:ns:epp:registryLock-1.0". The XML namespace prefix "reglock" is used, but implementations MUST NOT depend on it and instead employ a proper namespace-aware XML parser and serializer to interpret and output the XML documents.

2. Object Protection

This extension provides additional protection to objects managed by a sponsoring client on behalf of a registrant. This is achieved by requiring additional authorization for transform commands.

Solutions can be broadly categorized as in-band or out-of-band authorizations. Where in-band authorizations would provide authorization through EPP. Whereas out-of-band solutions provide authorization by some other means.

2.1. In-band Authorization

In-band authorization uses the authorization possibilities provided by EPP Standards [RFC5730], [RFC5731], [RFC5732] and [RFC5733].

2.2. Out-of-band Authorization

Out-of-band Authorization is not covered in this document. By definition out of band authorization will not use EPP and therefor is not subject of consideration here.

2.3. Command Execution Restrictions

Once an object has Registry Lock enabled all transform commands except <renew> MUST only be executed if

proper authorization is provided
the object is unlocked out-of-band

Otherwise the command MUST be rejected with EPP result code 2201 "Authorization error" [RFC5730] section 3.

Additionally the following EPP flags [RFC5731], [RFC5731], [RFC5731] must be set.

serverDeleteProhibited
serverTransferProhibited
serverUpdateProhibited

If the object is unlocked the flags SHOULD be cleared and the server should answer to an <info> request with the according information. However, if the object is only temporarily unlocked, the flags SHOULD be cleared, but in an <info> response the server should still indicate that the object is under registry lock.

OPEN QUESTION: If a domain is under registry lock, can a subordinate host be update?

3. Object Attributes

3.1. Locking Status

Locking Status information indicates if the additional protection of Registry Lock is enabled for an object.

Boolean values MUST be represented in the XML Schema format described in Part 2 of the W3C XML Schema recommendation [W3C.REC-xmlschema-2-20010502].

4. EPP Command Mapping

A detailed description of the EPP syntax and semantics can be found in the EPP core protocol specification [RFC5730].

4.1. EPP Query Commands

4.1.1. EPP <check> Command

This extension does not add any elements to the EPP <check> command or <check> response described in the EPP mappings [RFC5731], [RFC5732] or [RFC5733].

4.1.2. EPP <info> Command

This extension does not add any elements to the EPP <info> command described in the EPP domain mapping [RFC5731], host mapping [RFC5732] or contact mapping [RFC5733] However, additional elements are defined for the <info> response.

When an <info> command has been processed successfully, the EPP <resData> element MUST contain child elements as described in the EPP object mappings.

In addition, the EPP <extension> element SHOULD contain a child <regLock:infData> element that identifies the extension namespace the epp client has indicated support for the extension in the <login> command.

The <regLock:infData> element contains the following child elements:

Exactly one <locked> element that indicates if Registry Lock is enabled for the object.
An OPTIONAL <unlockedUntil> element if the object currently can be changed by the sponsoring client. The field indicates the time stamp when further changes will be impossible.

Example <domain:info> Response

```
S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
S:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
S:     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
S:  <response>
S:    <result code="1000">
S:      <msg>Command completed successfully</msg>
S:    </result>
S:    <resData>
S:      <domain:infData
...
S:      </domain:infData>
S:    </resData>
S:    <extension>
S:      <regLock:infData
xmlns:regLock="urn:ietf:params:xml:ns:epp:registryLock-1.0">
S:        <regLock:locked>1</regLock:locked>
S:        <regLock:unlockedUntil>20000101T000000+0000</regLock:unlockedUntil>
S:      </regLock:infData>
S:    </extension>
S:    <trID>
S:      <clTRID>ABC-12345</clTRID>
S:      <svTRID>54322-XYZ</svTRID>
S:    </trID>
S:  </response>
S:</epp>
```

Example <host:info> Response

```
S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
S:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
S:  <response>
S:    <result code="1000">
S:      <msg>Command completed successfully</msg>
S:    </result>
S:    <resData>
S:      <host:infData
S:       xmlns:host="urn:ietf:params:xml:ns:host-1.0">
...
S:      </host:infData>
S:    </resData>
S:    <extension>
S:      <regLock:infData
xmlns:regLock="urn:ietf:params:xml:ns:epp:registryLock-1.0">
S:        <regLock:locked>1</regLock:locked>
S:        <regLock:unlockedUntil>20000101T000000+0000</regLock:unlockedUntil>
S:      </regLock:infData>
S:    </extension>
S:    <trID>
S:      <clTRID>ABC-12345</clTRID>
S:      <svTRID>54322-XYZ</svTRID>
S:    </trID>
S:  </response>
S:</epp>
```

Example <contact:info> Response

```
S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
S:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
S:  <response>
S:    <result code="1000">
S:      <msg>Command completed successfully</msg>
S:    </result>
S:    <resData>
S:      <contact:infData
...
S:      </contact:infData>
S:    </resData>
S:    <extension>
S:      <regLock:infData
xmlns:regLock="urn:ietf:params:xml:ns:epp:registryLock-1.0">
S:        <regLock:locked>1</regLock:locked>
S:        <regLock:unlockedUntil>20000101T000000+0000</regLock:unlockedUntil>
S:      </regLock:infData>
S:    </extension>
S:    <trID>
S:      <clTRID>ABC-12345</clTRID>
S:      <svTRID>54322-XYZ</svTRID>
S:    </trID>
S:  </response>
S:</epp>
```

4.1.3. EPP <transfer> Command

This extension does not add any elements to the EPP <transfer> command or <transfer> response described in the EPP domain mapping [RFC5731], [RFC5732] or [RFC5733].

4.2. EPP Transform Commands

4.2.1. EPP <create> Command

This extension does not add any elements to the EPP <create> response described in the EPP mappings [RFC5731], [RFC5732] or [RFC5733].

If the object is locked, the EPP <create> command MUST be rejected with EPP response code 2201 "Authorization error" [RFC5730] section 3. See Section 2.3

Example <domain:create> command

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
C:  <command>
C:    <create>
C:      <domain:create
C:       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
C:        <domain:name>example.com</domain:name>
C:        <domain:period unit="y">2</domain:period>
C:        <domain:ns>
C:          <domain:hostObj>ns1.example.net</domain:hostObj>
C:          <domain:hostObj>ns2.example.net</domain:hostObj>
C:        </domain:ns>
C:        <domain:registrant>jd1234</domain:registrant>
C:        <domain:contact type="admin">sh8013</domain:contact>
C:        <domain:contact type="tech">sh8013</domain:contact>
C:        <domain:authInfo>
C:          <domain:pw>2fooBAR</domain:pw>
C:        </domain:authInfo>
C:      </domain:create>
C:    </create>
C:    <extension>
C:      <regLock:lock
xmlns:regLock="urn:ietf:params:xml:ns:epp:registryLock-1.0">
C:        <regLock:unlock>outofband</locked>
C:      </regLock:lock>
C:    </extension>
C:    <clTRID>ABC-12345</clTRID>
C:  </command>
C:</epp>
```

Example <host:create> command

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
C:  <command>
C:    <create>
C:      <host:create
C:       xmlns:host="urn:ietf:params:xml:ns:host-1.0">
C:        <host:name>ns1.example.com</host:name>
C:        <host:addr ip="v4">192.0.2.2</host:addr>
C:        <host:addr ip="v4">192.0.2.29</host:addr>
C:        <host:addr ip="v6">1080:0:0:0:8:800:200C:417A</host:addr>
C:      </host:create>
C:    </create>
C:    <extension>
C:      <regLock:lock
xmlns:regLock="urn:ietf:params:xml:ns:epp:registryLock-1.0">
C:        <regLock:unlock>outofband</locked>
C:      </regLock:lock>
C:    </extension>
C:    <clTRID>ABC-12345</clTRID>
C:  </command>
C:</epp>
```

Example <contact:create> command

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
C:  <command>
C:    <create>
C:      <contact:create
C:       xmlns:contact="urn:ietf:params:xml:ns:contact-1.0">
...
C:      </contact:create>
C:    </create>
C:    <extension>
C:      <regLock:lock
xmlns:regLock="urn:ietf:params:xml:ns:epp:registryLock-1.0">
C:        <regLock:unlock>outofband</locked>
C:      </regLock:lock>
C:    </extension>
C:    <clTRID>ABC-12345</clTRID>
C:  </command>
C:</epp>
```

4.2.2. EPP <delete> Command

This extension does not add any elements to the EPP <delete> command or <delete> response described in the EPP mappings [RFC5731], [RFC5732] or [RFC5733].

The EPP <delete> command MUST be rejected with EPP response code 2201 "Authorization error" [RFC5730] section 3. See Section 2.3

4.2.3. EPP <renew> Command

This extension does not add any elements to the EPP <renew> command or <renew> response described in the EPP mappings [RFC5731], [RFC5732] or [RFC5733].

Execution of the EPP <renew> command is not restricted by this extension.

4.2.4. EPP <transfer> Command

This extension does not add any elements to the EPP <transfer> command or <transfer> response described in the EPP mappings [RFC5731], [RFC5732] or [RFC5733].

The EPP <transfer> command MUST be rejected with EPP response code 2201 "Authorization error" [RFC5730] section 3. See Section 2.3

4.2.5. EPP <update> Command

This extension does not add any elements to the EPP <update> response described in the EPP mappings [RFC5731], [RFC5732] or [RFC5733].

If the object is locked, the EPP <update> command MUST be rejected with EPP response code 2201 "Authorization error" [RFC5730] section 3. See Section 2.3

Example <domain:update> Response

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
C:  <command>
C:    <update>
C:      <domain:update
C:       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
C:        <domain:name>example.com</domain:name>
C:      </domain:update>
C:    </update>
C:    <extension>
C:      <regLock:lock
xmlns:regLock="urn:ietf:params:xml:ns:epp:registryLock-1.0">
C:        <regLock:unlock>outofband</locked>
C:      </regLock:lock>
C:    </extension>
C:    <clTRID>ABC-12345</clTRID>
C:  </command>
C:</epp>
```

Example <host:update> Response

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
C:  <command>
C:    <update>
C:      <host:update
C:       xmlns:host="urn:ietf:params:xml:ns:host-1.0">
C:        <host:name>ns1.example.com</host:name>
C:      </host:update>
C:    </update>
C:    <extension>
C:      <regLock:lock
xmlns:regLock="urn:ietf:params:xml:ns:epp:registryLock-1.0">
C:        <regLock:unlock>outofband</locked>
C:      </regLock:lock>
C:    </extension>
C:    <clTRID>ABC-12345</clTRID>
C:  </command>
C:</epp>
```

Example <contact:update> Response

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
C:  <command>
C:    <update>
C:      <contact:update
C:       xmlns:contact="urn:ietf:params:xml:ns:contact-1.0">
C:        <contact:id>sh8013</contact:id>
C:      </contact:update>
C:    </update>
C:    <extension>
C:      <regLock:lock
xmlns:regLock="urn:ietf:params:xml:ns:epp:registryLock-1.0">
C:        <regLock:unlock>outofband</locked>
C:      </regLock:lock>
C:    </extension>
C:    <clTRID>ABC-12345</clTRID>
C:  </command>
C:</epp>
```

5. Formal Syntax

One schema is presented here that is the EPP Registry Lock Extension schema.

The formal syntax presented here is a complete schema representation of the object mapping suitable for automated validation of EPP XML instances. The BEGIN and END tags are not part of the schema; they are used to note the beginning and ending of the schema for URI registration purposes.

5.1. Registry Lock Extension Schema

```
BEGIN
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:se:iis:xml:epp:registryLock-1.0"
          xmlns:registryLock="urn:se:iis:xml:epp:registryLock-1.0"
          xmlns:xs="http://www.w3.org/2001/XMLSchema"
          elementFormDefault="qualified">

    <xs:annotation>
      <xs:documentation>
        Registry Lock Extension to the Extensible Provisioning Protocol v1.0
      </xs:documentation>
    </xs:annotation>

    <xs:element name="lock" type="registryLock:lockType" />

    <xs:complexType name="lockType">
      <xs:sequence>
            <simpleType name="unlock">
          <restriction base="token">
            <enumeration value="outofband"/>
            <enumeration value="password"/>
          </restriction>
        </simpleType>
      </xs:sequence>
    </xs:complexType>

    <xs:element name="infData" type="registryLock:infDataType"/>

    <xs:complexType name="infDataType">
      <xs:sequence>
        <xs:element name="locked" type="xs:boolean" />
        <xs:element name="unlockedUntil" type="xs:dateTime" minOccurs="0" />
      </xs:sequence>
    </xs:complexType>

</xs:schema>
END
```

6. IANA Considerations

6.1. XML Namespace

This document uses URNs to describe XML namespaces and XML schemas conforming to a registry mechanism described in [RFC3688]. The following URI assignment is requested of IANA:

Registration request for the registryLock namespace:

URI: urn:ietf:params:xml:ns:epp:registryLock-1.0
Registrant Contact: IESG
XML: None. Namespace URIs do not represent an XML specification.

Registration request for the registryLock XML schema:

URI: urn:ietf:params:xml:schema:epp:registryLock-1.0
Registrant Contact: IESG
XML: See the "Formal Syntax" section of this document.

6.2. EPP Extension Registry

The EPP extension described in this document should be registered by the IANA in the EPP Extension Registry described in [RFC7451]. The details of the registration are as follows:

Name of Extension: "Registry Lock Extension for the Extensible Provisioning Protocol (EPP)"

Document status: Standards Track

Reference: (insert reference to RFC version of this document)

Registrant Name and Email Address: IESG, <iesg@ietf.org>

TLDs: Any

IPR Disclosure: None

Status: Active

Notes: None

7. Implementation Status

Note to RFC Editor: Please remove this section and the reference to RFC 7942 [RFC7942] before publication.

TBD

8. Security Considerations

The security properties of EPP from [RFC5730] are preserved.

This extensions introduces an additional security layer for changes of objects managed through EPP. The overall security of these measures depends on policies and procedures not covered in this document.

9. Acknowledgements

The authors wish to thank the following persons for their feedback and suggestions:

10. 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>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC5730] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)", STD 69, RFC 5730, DOI 10.17487/RFC5730, August 2009, <https://www.rfc-editor.org/info/rfc5730>.

[RFC5731] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Domain Name Mapping", STD 69, RFC 5731, DOI 10.17487/RFC5731, August 2009, <https://www.rfc-editor.org/info/rfc5731>.

[RFC5732] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Host Mapping", STD 69, RFC 5732, DOI 10.17487/RFC5732, August 2009, <https://www.rfc-editor.org/info/rfc5732>.

[RFC5733] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Contact Mapping", STD 69, RFC 5733, DOI 10.17487/RFC5733, August 2009, <https://www.rfc-editor.org/info/rfc5733>.

[RFC7451] Hollenbeck, S., "Extension Registry for the Extensible Provisioning Protocol", RFC 7451, DOI 10.17487/RFC7451, February 2015, <https://www.rfc-editor.org/info/rfc7451>.

[RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205, RFC 7942, DOI 10.17487/RFC7942, July 2016, <https://www.rfc-editor.org/info/rfc7942>.

[W3C.REC-xmlschema-2-20041028] Biron, P. and A. Malhotra, "XML Schema Part 2: Datatypes Second Edition", World Wide Web Consortium Recommendation REC-xmlschema-2-20041028, October 2004, <http://www.w3.org/TR/2004/REC-xmlschema-2-20041028>.

Appendix A. Change History

A.1. Change from 00 to 01

1. None yet :-)

Author's Address

Ulrich Wisser
The Swedish Internet Infrastructure Foundation
Box 92073
Stockholm 12007
SE

Email: ulrich.wisser@internetstiftelsen.se
URI: https://www.internetstiftelsen.se