Workgroup: Registration Protocols Extensions
Internet-Draft: draft-wisser-registrylock-04
Published: 7 July 2021
Intended Status: Standards Track
Expires: 8 January 2022
A U. Wisser
uThe Swedish Internet Foundation
t
h
o
r
s
:

Registry Lock Extension for the Extensible Provisioning Protocol (EPP)

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. All of these interactions are ususally fully automated.

In case of a system breach, there is no protection in EPP to changes to any object by the intruder.

This extension defines a protective layer that aims to break automated changes and work flows by requiring manual intervention.

The actual form of manual intervention is out-of-scope for this document. By whom and how changes can be made is up to the registry and registrars to decide.

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 8 January 2022.

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. All of these interactions are ususally fully automated.

In case of a system breach, there is no protection in EPP to changes to any object by the intruder.

This extension defines a protective layer that aims to break automated changes and work flows by requiring manual intervention.

The actual form of manual intervention is out-of-scope for this document. By whom and how changes can be made is up to the registry and registrars to decide.

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 [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.

- either by temporarily unlocking the object for changes
- or by authorizing pending changes after they have been submitted to the server

2.1. 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 therefore is not subject of consideration here.

Registries must provide means for the registrar or registrant to temporarily unlock the domain, to remove registry lock or ro authorize changes submitted to the server through some means than EPP.

2.2. In-band Authorization

Currently defined authorization schemes are not deemed secure enough for in-band change authorization. Therefore this document does not allow in-band authorization. This is left as a future development once secure enough authorization schemes have been defined.

The current defined authorization scheme is based on static passwords. This would mean that once a password is known any change can be made. Security here is once again dependend on the security of all automatic systems invloved.

2.3. Command Execution Restrictions

Once an object has Registry Lock enabled all transform commands except <renew> MUST only be executed if a proper authorization has been made.

Otherwise the command MUST be rejected with EPP result code 2201 "Authorization error" or 1001 "Command completed successfully; action pending" [RFC5730] section 3 in depending on the chosen out-of-band authorization.

if the server has returned a 1001 "Command completed successfully; action pending" answer, it MUST follow [RFC5731], [RFC5732], [RFC5733] in handling succeeded or failed commands.

The following EPP flags 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.

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

- *I got one "no" answer - hosts might not be owned by domain owner
- *In .se/.nu all subordinary hosts are automatically owned by the domain owner and locked if the domain is locked.

We need more input!

If the object is temporarily unlocked only <update> commands are allowed. <delete> and <transfer> are explicitly not allowed. For the time of the temporary unlock the serverUpdateProhibited status should be cleared.

2.4. Temporary Unlock

While an object is locked some situations could require a change. To fully unlock the object would remove all protection and could not provide any guarantee that the object is protected again after the desired changes have been made.

Temporarily unlocking the object allows for a more fine grained security model for all objects.

Any temporary unlocking of the object has to be time limited. After that time has passed no further changes are possible.

Additionally the number of allowed EPP commands can be specified to further limit the changes possible.

Registries and registrars can further limit the possibles changes, e.g. not allowing owner changes even for temporarily unlocked Domain objects.

IS THE LAST PARAGRAPH A GOOD IDEA? INPUT NEEDED!!!

When an object is temporarily unlocked the serverUpdateProhibited SHOULD be cleared while changes are possible.

When either the time for the temporary unlock has passed or the maximum amount of EPP changes has been made the object MUST return to a fully locked status. The serverUpdateProhibited flag MUST be set again and the infData response MUST no longer contain a <unlockedUntil> element.

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-2-20041028].

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 the lock will become active again.
- An OPTIONAL <eppCmdCount> attribute that indicates the number of EPP <update> commands that will be executed.

Example <domain:info> Response, domain not locked

```
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
S:        xmlns:regLock="urn:ietf:params:xml:ns:epp:registryLock-1.0">
S:        <regLock:locked>0</regLock:locked>
S:      </regLock:infData>
S:    </extension>
S:    <trID>
S:      <clTRID>ABC-12345</clTRID>
S:      <svTRID>54322-XYZ</svTRID>
S:    </trID>
S:  </response>
S:</epp>
```

Example <domain:info> Response, domain locked

```
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
S:        xmlns:regLock="urn:ietf:params:xml:ns:epp:registryLock-1.0">
S:        <regLock:locked>1</regLock:locked>
S:      </regLock:infData>
S:    </extension>
S:    <trID>
S:      <clTRID>ABC-12345</clTRID>
S:      <svTRID>54322-XYZ</svTRID>
S:    </trID>
S:  </response>
S:</epp>
```

Example <domain:info> Response, domain temporary unlocked

```
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
S:        xmlns:regLock="urn:ietf:params:xml:ns:epp:registryLock-1.0">
S:        <regLock:locked>1</regLock:locked>
S:<regLock:unlockedUntil eppCmdCount="1">20000101T000000+0000
S:</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 mapping [RFC5731], [RFC5732] or [RFC5733].

4.2. EPP Transform Commands

4.2.1. EPP <create> Command

This extension is intended to be used within the scope of the object creation. It does not define a <create> command of its own.

This extension adds elements to the EPP <create> command as described in the EPP [RFC5730].

When submitting a <create> command to the server, the client MAY include in the <extension> element a <registryLock:lock> element to create the domain in a locked state. The extension includes the following element:

*A <regLock:lock> element indicating that the domain MUST be created in a locked state.

When a <create> command has been processed successfully, the EPP response is as described in the EPP objects mappings [RFC5731], [RFC5732], [RFC5733].

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
C:        xmlns:regLock="urn:ietf:params:xml:ns:epp:registryLock-1.0" />
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].

If the object is locked, 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].

If the object is locked, 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 adds elements to the EPP <update> command as described in [RFC5730].

If the object is not locked, the <update> command can be used to lock the object, similarly to the <create> command.

If the object is in locked state, but temporarily unlocked, the server MUST execute the command as if the object were unlocked.

If the object is locked the server can handle <update> commands in two ways

- answering the command with EPP response code 1001 "Command completed successfully; action pending" [RFC5730] section 3
- rejecting with EPP response code 2201 "Authorization error" [RFC5730] section 3

Registries can narrow down allowed changes when a domain is locked. Registries could prohobit changes of registrant for doamins even if the domain is temporatily unlocked or password authorization is given.

When a <update> command has been processed successfully, the EPP response is as described in the EPP objects mappings [RFC5731], [RFC5732], [RFC5733].

Example <domain:update> command, locking domain

```
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
C:        xmlns:regLock="urn:ietf:params:xml:ns:epp:registryLock-1.0" />
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:ietf:params:xml:ns:epp:registryLock-1.00"
  xmlns:regLock="urn:ietf:params:xml:ns: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>


  <!-- child elements found in EPP commands -->

  <xs:element name="lock" />

  <!-- child elements found in EPP responses -->

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

  <!-- child element of the response -->

  <xs:complexType name="infDataType">
    <xs:sequence>
      <xs:element name="locked" type="xs:boolean"/>
      <xs:element name="unlockedUntil" type="xs:dateTime" minOccurs="0">
        <xs:complexType>
          <xs:attribute name="eppCmdCount" type="xs:positiveInteger" min
        </xs:complexType>
      </xs:element>
    </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.

Implemented by .SE since 2019.

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 the security of the out-of-band authorization. Registries and registrars are therefore adviced to select secure forms of authorization.

Current EPP authorizations schemes are not secure enough to allow in-band authorization. Registries and registrars therefore MUST not implent in-band command authorization.

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, 28 October 2004, <https://www.w3.org/TR/2004/REC-xmlschema-2-20041028>.

Appendix A. Change History

A.1. Change from 00 to 01

1. Corrected information for the <create/> command.
2. Minor fixes in wording.
3. Introduces resData element.

A.2. Change from 01 to 02

1. Multiple spelling errors fixed.
2. Moved response from resData to extension part of the EPP response.
3. Clarification of password and out-of-band usage.
4. Updated XML schema and examples
5. Changed security considerations for password authorization.
6. Added unlockUntil to create command

7. Forbid temporarily unlock for password authorization.

A.3. Change from 02 to 03

1. Fix list styles for better readability
2. Fix reference to W3C XML Schema

A.4. Change from 03 to 04

1. Remove references to in-band authorization
2. Remove special response elements
3. Add command counter to temporary unlock
4. Fix formatting and XML schema

Author's Address

Ulrich Wisser
The Swedish Internet Foundation
Box 92073
SE-12007 Stockholm
Sweden

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