

OID for Proxy Delegation Tracing

Abstract

This document defines the OID allocation from the IGTF used for experimental proxy certificate delegation tracing. It assigns OID arc 1.2.840.113612.5.5.1.1.1 for the use of identifying attributes in RFC 3820 proxy certificates that facilitate the tracing of delegations in a proxy certificate chain.

Table of Contents

1	Introduction	2
2	Proxy Tracing.....	2
2.1	The iGTFProxyTracingIssuerName Extension.....	2
2.2	The iGTFProxyTracingSubjectName Extension.....	3
3	Security Considerations	3
4	Assignment and Document Revision Process	3
5	Acknowledgements	3
6	References.....	3

1 Introduction

This document defines the OID allocation from the IGTF for proxy certificate delegation tracing.

The proxy tracing extensions defined in this document are experimental.

2 Proxy Tracing

The Proxy Tracing extensions are used for tracing a delegation chain and are primary intended for debugging operational problems in delegation based infrastructures.

The object identifier arc *id-pctrace* is assigned by the IGTF [IGTF] to these extension attributes:

```
id-igtf OBJECT IDENTIFIED ::= {iso(1) member-body(2) us(840)
                                esnet(113612) igtf(5)}

id-serv OBJECT IDENTIFIER ::= { id-igtf 5 }

id-attrobj OBJECT IDENTIFIER ::= { id-serv 1 }

id-authnattr OBJECT IDENTIFIER ::= { id-attrobj 1 }

id-pctrace OBJECT IDENTIFIER ::= { id-authnattr 1 }
```

2.1 The iGTFProxyTracingIssuerName Extension

A new extension, *iGTFProxyTracingIssuerName*, is defined in this subsection. This extension MAY be present in a proxy Certificate [RFC3820] to designate the entity that issued the proxy certificate that contains this extension.

```
iGTFProxyTracingIssuerName OBJECT IDENTIFIER ::= { id-pctrace 1 }

... iGTFProxyTracingIssuerName ::= GeneralNames
```

where the structure of *GeneralNames* is identical to the one used for *issuerAlternativeName*:

```
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
GeneralName ::= CHOICE {
    otherName                [0] AnotherName,
    rfc822Name                [1] IA5String,
    dNSName                   [2] IA5String,
    x400Address                [3] ORAddress,
    directoryName              [4] Name,
    ediPartyName               [5] EDIPartyName,
    uniformResourceIdentifier [6] IA5String,
    iPAddress                  [7] OCTET STRING,
    registeredID               [8] OBJECT IDENTIFIER }

AnotherName ::= SEQUENCE {
    type-id OBJECT IDENTIFIER,
    value ANY DEFINED BY type-id }
```



2.2 The iGTFProxyTracingSubjectName Extension

A new extension, iGTFProxyTracingSubjectName, is defined in this subsection. This extension MAY be present in a proxy Certificate [RFC3820] to designative the entity that is the designated target for delegation of the proxy certificate that contains this extension.

```
iGTFProxyTracingSubjectName OBJECT IDENTIFIER ::= { id-pctrace 2 }  
... iGTFProxyTracingSubjectName (2) ::= GeneralNames
```

where the structure of *GeneralNames* is identical to the one used for *subjectAlternativeName* (see above)

3 Security Considerations

The embedded attributes are asserted by the entity that signed the proxy certificate, i.e., the delegating entity. This implies that the attribute specifying the iGTFProxyTracingSubjectName is asserted by the Issuer, and not by the subject, and the iGTFProxyTracingIssuerName is a self-assertion.

The subject of the delegation may suggest the iGTFProxyTracingSubjectName attribute values to be included in the delegated proxy to the delegating entity using any possible method – this document does not limit the way in which this information is conveyed to the delegating entity (i.e. the issuer).

4 Assignment and Document Revision Process

Sub-delegations within this arc, and the specification for attributes to which OIDs are assigned must be documented in the IGTF Registry. Documented requests must be sent to the email address oid-manager@gridpma.org.

5 Acknowledgements

The proxy delegation tracing attributes were proposed by Akos Frohner (akos.frohner@cern.ch, European Organisation for Nuclear Research) and Joni Hahkala (joni.hahkala@hip.fi, University of Helsinki, Helsinki Institute of Physics).

6 References

- [IGTF] International Grid Trust Federation, <http://www.gridpma.org/>
[RFC3820] S. Tuecke et al. *Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile*

