VOMS Attribute Certificate Parsing Rules   
for Chained Identity Credentials

Status of This Document

Grid Recommendation (proposed)

Copyright Notice

Copyright © Open Grid Forum (2012). Some Rights Reserved. Distribution is unlimited.

Abstract

This document provides information to the Grid community on the interpretation of VOMS [GFD182] attribute certificates as represented in identity proxy certificate [RFC5755] chains. It addresses precedence, validity and scope of the resulting attribute set.

Contents

[Abstract 1](#_Toc337421513)

[Contents 1](#_Toc337421514)

[1 Introduction 2](#_Toc337421515)

[2 Notational Conventions 2](#_Toc337421516)

[3 VOMS proxy chain structure 2](#_Toc337421517)

[3.1 Validity period and renewal requirements 3](#_Toc337421518)

[3.2 Scoping requirements 3](#_Toc337421519)

[4 Parsing rules 3](#_Toc337421520)

[5 Security Considerations 4](#_Toc337421521)

[6 Contributors 4](#_Toc337421522)

[7 Acknowledgments 4](#_Toc337421523)

[8 Intellectual Property Statement 5](#_Toc337421524)

[9 Disclaimer 5](#_Toc337421525)

[10 Full Copyright Notice 5](#_Toc337421526)

[References 5](#_Toc337421527)

# Introduction

In this document we defined the parsing rules for VOMS attributes in chained identity credentials when evaluated for authorization purposes at the resource.

This document deals exclusively with the client-side interpretation of collated VOMS attribute certificates embedded in chained identity credentials. It does not discuss the expected behavior of any VOMS attribute authority or its distribution mechanism. It assumes that the entity constricting the chained identity credential rooted to a specific end-entity certificate (EEC) can *in some way* avail over any set of VOMS ACs which a VOMS attribute authority would be willing to bind to the EEC involved[[1]](#footnote-1).

# Notational Conventions

The key words ‘MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” are to be interpreted as described in RFC 2119 [BRADNER], except that the words do not appear in uppercase.

# VOMS proxy chain structure

The structure of the chained identity credentials (“proxy chains”) containing VOMS attribute certificates (AC) [GFD.I-182] past the end-entity certificate (EEC) can be represented as a tree, with the EEC as its root. The EEC itself[[2]](#footnote-2) and any proxy [RFC3820] derived thereof can contain zero or more ACs[[3]](#footnote-3).

VOMS ACs contain attributes assertions bound to the EEC (by means of the issuer entity name and the serial number in the baseCertificateID as per [RFC5755]) that contain:

* attribute certificate issuer
* attribute certificate validity period, with both start and end date
* the VOMS section, which can contain zero or more extensions
  + a sequence of one or more FQANs
  + a sequence of one or more tags (‘generalized attributes’)
  + an AC target (restricting the validity to the named recipients)
  + a list of CA certificates to validate the AC issuer certificate

For the purposes of this document, the FQANs (section 3.4.1 in GFD.I-182) and tags (section 3.6.4) can be treated as equivalent for the purposes of validation, and will be both referred to as ‘attributes’ in that context[[4]](#footnote-4). The AC target extension and the list of CA certificates are not relevant to the discussion on the interpretation and parsing rules discussed in this document.

It is common that credentials are delegated many times, because the work flow passes to a different processing entity to which the effective credential must be delegated. In addition, delegation may be ‘refreshed’ by being over-written with new delegations (with a expiration date further in the future) based on an existing longer-term delegation (‘long-term proxies’) in a credential store.

VOMS ACs may in this case be either added later in the chain derived from ‘undecorated’ long-term proxies, or the long-term proxy itself may contain a (potentially shorter-lived) VOMS AC.

## Validity period and renewal requirements

The maximum validity period of a VOMS AC is defined by the attribute authority, whereas the validity period of the chained identity credential proxy is defined by the EEC subject signing the proxy, and these may therefore be different. However, VOMS ACs can usually be re-issued (with a new expiry date) by the AA in an non-interactive way, whereas the validity of the proxy chain cannot be extended beyond the initial expiry date of the first proxy signed by the EEC, without the intervention of the EEC subject.

The parsing rules MUST allow for ‘refreshing’ of VOMS credentials in an existing credential chain without invalidating this chain or requiring intervention of the subject.

## Scoping requirements

When a user[[5]](#footnote-5) creates a VOMS proxy chain, one or more VOMS ACs are embedded together (in a sequence) and list a combined set of attributes associated with this credential. Since embedding VOMS ACs in a proxy chain can be considered a deliberate act by the user, and the user must be assumed to have knowledge of the usage intent of the credential, this set of attributes defines the (implicit) scope of the credential. The user should assume that resources taking any action based on the credential use the set of attributes bestowed on the credential[[6]](#footnote-6) by the user at this time.

The credential may be subsequently re-delegated several times, and to different actors outside the user’s direct control. It MUST NOT be possible for such entities to change the original intended limitation of the proxy by the user, thereby escaping any restrictions intended by the user at proxy creation time by specifically embedding or *not* embedding particular attributes[[7]](#footnote-7).

# Parsing rules

Based on the requirements specified in section 3.1 and 3.2, the following rules MUST be implemented when determining the currently valid set of attributes in a VOMS-enhanced chained identity credential.

Let us call the EEC cert0. The proxy generated from it is cert1, the proxy generated from cert1 is cert2, and so on until the latest delegation, called certN. The first proxy (certv0) is defined by the parsing the chain in order from 1 to N, and where certv0 is the first cert in which a VOMS AC is found. The encompassing and effective list (ELv0) of attributes in certv0 is defined by the ensemble of all attributes contained in all VOMS ACs embedded in certv0.

The effective list of attributes in certi, where *i* is increasing and *i*>*v0* and *i*<=*N*, and where certi has one or more VOMS ACs embedded, is the intersection of the effective encompassing list of certi-1, and the ensemble of all attributes contained in all VOMS ACs embedded in certi. If certi does not contain any VOMS ACs, the effective list of attributes of certi is equal to that of certi-1.

The effective set of VOMS attributes of a chained identity credential is thus *always* equal to or a subset of the encompassing list, and thus of the intent of the user.

For each attribute in the effective set, the validity is for each attribute is defined by the validFrom and validUntil dates of the AC containing each attribute of the last cert in the chain containing a VOMS AC.

Compliant validation implementations for authorization MUST consider only those attributes which are in the effective set.

Compliant validation implementations for authorization MUST consider only those attributes for which the *validUntil* date is in the future, MUST consider only those for which the *validFrom* date is past the current date.

# Security Considerations

The parsing rules specified in GFD.I-182 section 4.4 state that the last available ‘leaf’ AC in the proxy certificate chain is the only one which must be evaluated. In conjunction with the fact that the ACs are bound to the end-entity certificate (and not to any subsequent proxy certificates), and in the form stated there, it implies that the original delegator can not restrict the effective set of attributes once a VOMS-enhanced credential has been delegated. The delegatee can, by adding a single subsequent delegation, embed any VOMS AC for the original end-entity in this final delegation which will then take precedence over all others. This can also be a VOMS AC for a different VO, or one containing different groups, roles or generic attributes. The newly embedded VOMS AC can be obtained either from a VOMS server (by authenticating with a proxy) or through any other means on the client-side only. We consider this to be a security threat, which this Recommendation aims to address.

# Contributors

David Groep

Nikhef

P.O. Box 41882

1009 DB Amsterdam, The Netherlands

email: davidg@nikhef.nl

Mike Jones

University of Manchester

Manchester, United Kingdom

email:mike.jones@manchester.ac.uk

and Jens Jensen, STFC, Milan Sova, CESNET, and the membership of the VOMS-PROC WG.

# Acknowledgments

This work is supported by the Initiative for Globus in Europe (IGE), which is co-funded by the European Commission under contract RI-261560. This work is also part of the research programme of Nikhef, which is financially supported by the foundation for Fundamental Research on Matter (FOM) and the Netherlands Organisation for Scientific Research (NWO).

# Intellectual Property Statement

The OGF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the OGF Secretariat.

The OGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights, which may cover technology that may be required to practice this recommendation. Please address the information to the OGF Executive Director.

# Disclaimer

This document and the information contained herein is provided on an “As Is” basis and the OGF disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.

# Full Copyright Notice

Copyright (C) Open Grid Forum (2012). Some Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included as references to the derived portions on all such copies and derivative works. The published OGF document from which such works are derived, however, may not be modified in any way, such as by removing the copyright notice or references to the OGF or other organizations, except as needed for the purpose of developing new or updated OGF documents in conformance with the procedures defined in the OGF Document Process, or as required to translate it into languages other than English. OGF, with the approval of its board, may remove this restriction for inclusion of OGF document content for the purpose of producing standards in cooperation with other international standards bodies.

The limited permissions granted above are perpetual and will not be revoked by the OGF or its successors or assignees.

# References

[GFD.I-182] The VOMS Attribute Certificate Format, *Vincenzo Ciaschini et al.*, OGF 2011. <http://www.ogf.org/documents/GFD.182.pdf> (retrieved October 2012)

[RFC3820] Internet X.509 PKI Proxy Certificate Profile, *S. Tuecke et al.*, Internet Engineering Task Force 2004. <http://www.ietf.org/rfc/rfc3820.txt> (retrieved October 2012)

[RFC5755] An Internet Attribute Certificate Profile for Authorization, *S. Farrell et al.*, Internet Engineering Task Force 2010. <http://www.ietf.org/rfc/rfc5755.txt> (retrieved October 2012)

1. For example, the EEC can be used directly to authenticate to a VOMS server and have it release attribute certificates as requested, or it can be obtained by authenticating with an existing proxy (with or without already embedded VOMS ACs), or it can be extracted from another chain rooted in the same EEC. [↑](#footnote-ref-1)
2. Usually the EEC does not contain VOMS ACs, but if it does, the baseCertificateID should be known as it is also embedded both in the AC as well as in the EEC. [↑](#footnote-ref-2)
3. VOMS ACs targeting certificate authority credentials are out of scope and the processing thereof is unspecified. [↑](#footnote-ref-3)
4. In the definition of the ordering of FQANs and tags, they will need to be distinguished. [↑](#footnote-ref-4)
5. The term ‘user’ is deliberately ambiguous and used here it identity the entity who embeds the *first* VOMS AC in any proxy chain. It thus may mean a human individual, but it can also be a system acting on behalf of the human individual in creating such a VOMS-enabled delegation, e.g. a portal or credential management system. In either case, the system embedding this first VOMS AC has knowledge of the intended use of the credential thus created. [↑](#footnote-ref-5)
6. although besides the set of attributes in VOMS ACs also other attributes such as the EEC subject name, issuer, serial numbers, or other non-VOMS ACs may be used. [↑](#footnote-ref-6)
7. For example, a user wanting to act in a regular non-privileged more would specifically *not* includes an FQAN role like ‘…/Role=administrator’, and it *must not be possible* for any ‘downstream’ delegatees to retro-actively include such an FQAN. Similarly, it must not be possible to assume attributes or roles derived from another attribute authority to which the user may also happen to have associated attributes. [↑](#footnote-ref-7)