

ACE Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 26, 2019

S. Gerdes
O. Bergmann
C. Bormann
Universitaet Bremen TZI
October 23, 2018

C3DC -- Constrained Client/Cross-Domain Capable Authorization Profile
for Authentication and Authorization for Constrained Environments (ACE)
[draft-gerdes-ace-c3dc-00](#)

Abstract

Resource-constrained nodes come in various sizes and shapes and often have constraints on code size, state memory, processing capabilities, user interface, power and communication bandwidth ([RFC 7228](#)).

This document specifies a profile that describes how two autonomous resource-constrained devices, a client and a server, obtain the required keying material and authorization information to securely communicate with each other. Each of the devices is coupled with a less-constrained device, the authorization manager, that helps with difficult authentication and authorization tasks. The constrained devices do not need to register with authorization managers from other security domains. The profile specifically targets constrained clients and servers. It is designed to consider the security objectives of the owners on the server and the client side.

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 April 26, 2019.

Internet-Draft

C3DC

October 2018

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
1.1.	Terminology	5
2.	Protocol	5
2.1.	Overview	5
2.2.	Details for the C3DC profile as an instance of the DTLS profile	7
2.3.	Details for the C3DC profile as an instance of the OSCORE profile	7
3.	IANA Considerations	7
4.	Security Considerations	7
5.	Acknowledgements	7
6.	References	7
6.1.	Normative References	7
6.2.	Informative References	8
	Authors' Addresses	8

[1.](#) Introduction

The ACE framework [[I-D.ietf-ace-oauth-authz](#)] describes how a client obtains authorization to access a (probably constrained [[RFC7228](#)]) server from the server's authorization manager. Without additional support, constrained clients will have difficulties to communicate with authorization managers from other security domains. They need to be configured with the necessary keying material to securely communicate with the AS. Manual configuration is not a feasible solution for the Internet of Things where the large number of nodes

makes scalability a special concern. Also, constrained devices often lack user interfaces and displays and have slow response times, which make their configuration tedious. Therefore, the configuration of the client is best done using a less-constrained device that mediates between the constrained device and its overseeing principal, i.e.,

the human being that is configuring the device (such as its owner or user).

In the Constrained Client Cross-Domain Authorization Profile (C3DC), each constrained device initially only requires a security association with its own authorization manager; it does not need to register with authorization managers from other security domains. The constrained device and its authorization manager belong to the same security domain, which makes their security association easier to maintain. As the managers are less-constrained, they can perform more difficult authentication and authorization tasks such as storing large numbers of keys, using less-constrained-level protocols such as HTTP or TLS, processing TLS certificates, etc. In this way, the authorization managers authenticate each other and validate each other's authorization. They vouch for their own constrained devices' attributes and keying material and negotiate the details of the secure communication between client and server. If the overseeing principals of both security domains approve of the communication, the managers provide the necessary keying material and authorization information to their respective constrained devices: The client is provided with a claim set from its authorization manager (CAS) that contains the necessary keying material, and, if necessary, the resources and actions it may perform on the server. The server is provided with a claim set from its manager (AS) that contains the keying material and the client's access permissions. The effort for clients and servers is thereby minimized.

Summarizing, the role that is termed "Client" in [\[I-D.ietf-ace-oauth-authz\]](#) is split into the actual constrained client, "C", and its authorization manager, "CAS". This is summarized in Figure 1.

Internet-Draft

C3DC

October 2018

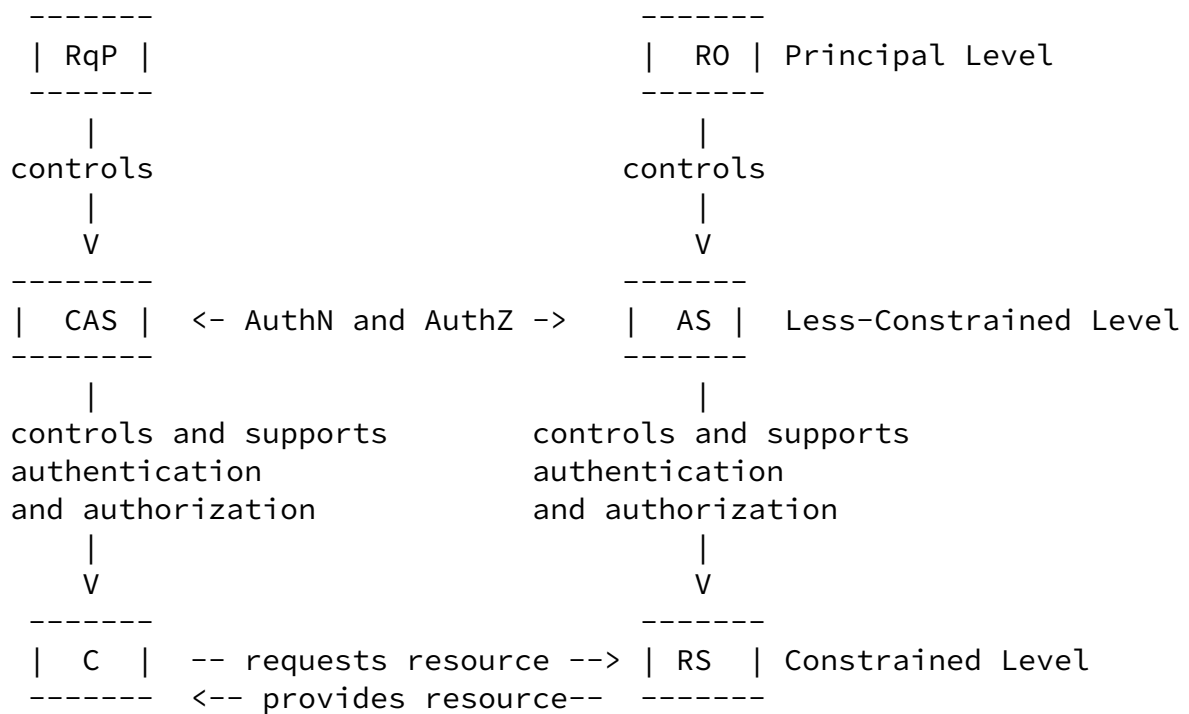


Figure 1: Overall architecture

Authorization Managers may be responsible for large numbers of devices. The overseeing principals only need to configure the authorization manager which will then provide the respective authentication and authorization information to the constrained devices it manages. The management of constrained devices thereby becomes much more comfortable.

The benefits of the C3DC profile include:

- o Constrained devices only require a security association with their own authorization manager.
- o Constrained clients are not required to authenticate authorization servers from other security domains.
- o Authentication and authorization on the client side can be dynamic.
- o Both RqP's and RO's interests are considered.
- o Constrained devices without a real-time clock that are not time-synchronized can be supported.

[1.1.](#) Terminology

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.

Readers are assumed to be familiar with the terms and concepts defined in [[I-D.ietf-ace-actors](#)].

The official pronunciation of "C3DC" rhymes with "curtsy".

[2.](#) Protocol

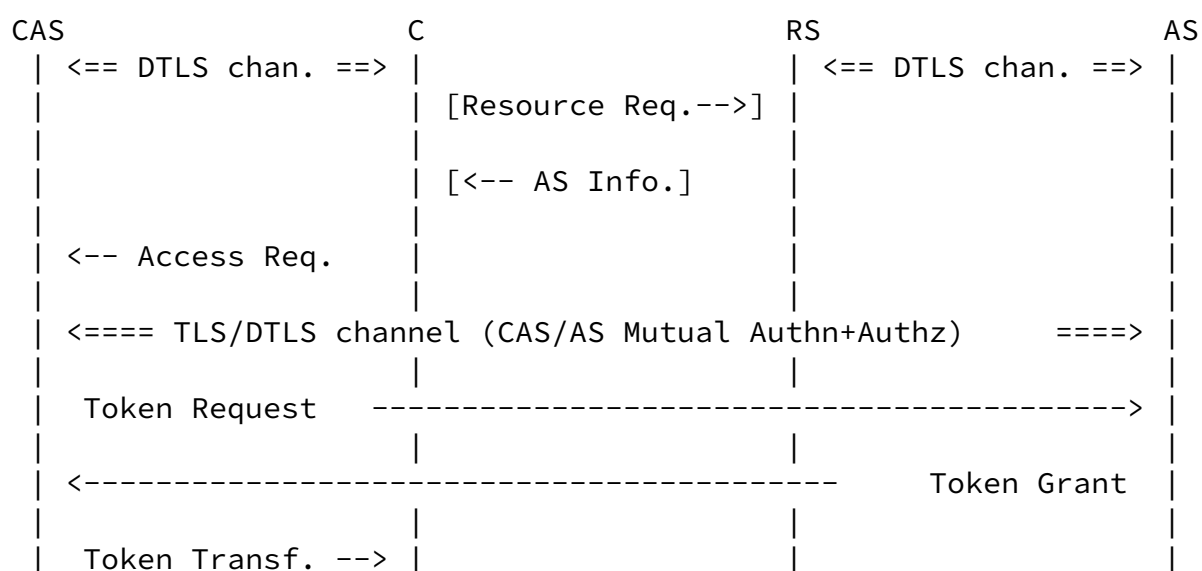
The C3DC profile comprises three parts:

1. transfer of authentication and, if necessary, authorization information between AS and RS;
2. transfer of authentication and, if necessary, authorization information between CAS and C;

3. establishment of a security association between C and RS.

2.1. Overview

Figure 2 depicts the C3DC protocol flow (messages in square brackets are optional):



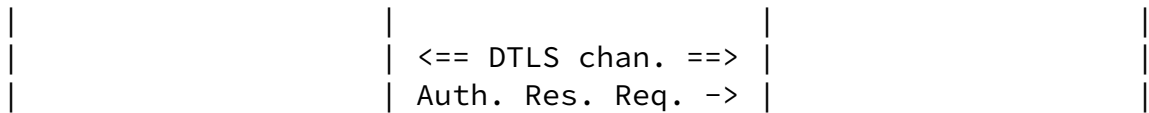


Figure 2: Protocol Overview

As in the ACE framework, the client (C) may send an unauthorized resource request to the resource server (RS) to obtain the address of the authorization server (AS) that is responsible for the server. The client then contacts its own authorization manager (CAS) with which it already has a security association. As described in [\[I-D.ietf-ace-actors\]](#), C and CAS are expected to belong to the same security domain.

The requesting party (RqP), i.e., the human being that is responsible for C and CAS, provisions CAS with authorization information. This enables CAS to decide which resource servers the client is allowed to communicate with, and which authorization servers are allowed to provide information about the RS. If CAS has information that RqP approves of the communication, CAS and AS authenticate each other. As they are less-constrained devices, they may use less-constrained level protocols such as TLS to authenticate each other. AS obtains from its overseeing principal, the resource owner (RO) if CAS is authorized to provide information (e.g., keying material) about C and if CAS's client is authorized to communicate with RS.

After AS and CAS thus validated each others' authorization, AS generates an access token for RS. In the response to CAS, the AS may also specify access information that contains the keying material meant for C. The access token and access information must securely be provided to CAS.

RqP may further specify the resources and actions that C may perform on RS. In this case, CAS adds this information to the access information. It then securely provides the access token and access information to C. Since C has a security association with CAS, it can authenticate the message. Also, CAS can provide C with validity information that even a constrained C is able to interpret.

As in the usual ACE framework protocol flow, the client keeps the

access information and provides the access token to the resource server. The resource server already has a security association with its AS and thus can validate that the token actually stems from an authorization server that is authorized by its overseeing principal RO. The client and the server then use the obtained information to communicate securely.

[2.2.](#) Details for the C3DC profile as an instance of the DTLS profile

[2.3.](#) Details for the C3DC profile as an instance of the OSCORE profile

[3.](#) IANA Considerations

TBD

[4.](#) Security Considerations

TBD

[5.](#) Acknowledgements

[6.](#) References

[6.1.](#) Normative References

[I-D.ietf-ace-oauth-authz]

Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)", [draft-ietf-ace-oauth-authz-16](#) (work in progress), October 2018.

[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>>.

[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>>.

[6.2.](#) Informative References

[I-D.ietf-ace-actors]

Gerdes, S., Seitz, L., Selander, G., and C. Bormann, "An architecture for authorization in constrained environments", [draft-ietf-ace-actors-07](#) (work in progress), October 2018.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", [RFC 7228](#), DOI 10.17487/RFC7228, May 2014, <<https://www.rfc-editor.org/info/rfc7228>>.

Authors' Addresses

Stefanie Gerdes
Universitaet Bremen TZI
Postfach 330440
Bremen D-28359
Germany

Phone: +49-421-218-63906
Email: gerdes@tzi.org

Olaf Bergmann
Universitaet Bremen TZI
Postfach 330440
Bremen D-28359
Germany

Phone: +49-421-218-63904
Email: bergmann@tzi.org

Carsten Bormann
Universitaet Bremen TZI
Postfach 330440
Bremen D-28359
Germany

Phone: +49-421-218-63921
Email: cabo@tzi.org