ACE Working Group
Internet-Draft
Intended status: Informational
Expires: April 21, 2016

S. Gerdes
Universitaet Bremen TZI
J. Cuellar
Siemens AG
O. Bergmann
Universitaet Bremen TZI

October 19, 2015

Solutions for the authorization in constrained environments
draft-cuellar-ace-solutions-00

Abstract

The Constrained Application Protocol (CoAP) is a transfer protocol that was designed to meet the special requirements of constrained environments.

This document introduces a common framework for conveying authorization information between the actors in the ACE architecture by defining classes of message types. It thus specifys a common authorization extension for CoAP.

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 http://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 21, 2016.

Copyright Notice

Table of Contents

1. Introduction

Resource-constrained nodes only have limited system resources such as memory, stable storage (such as disk space) and transmission capacity and often lack input/output devices such as keyboards or displays. They are often especially designed to perform a single, simple task in their application area. The various use cases (see [I-D.ietf-ace-usecases]) have varying requirements for the authentication and authorization solution. Due to the constrainedness of the devices, a single solution cannot address all these requirements.

In the Authentication and Authorization for Constrained Environments (ACE) working group, various proposals are discussed that cover different use-cases and application scenarios. This document explains how the specific solutions in the ACE WG fit together in a common framework. It defines classes of message types to convey authenticated authorization information between the actors in the ACE architecture. [I-D.ietf-ace-actors]

The description of each message type covers the effect this message has, the actors that send and receive the message and the kind of protection it requires. Solution designer can implement the message type classes with the effect they require for their solution.

1.1. Terminology

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

2. Overview

The ACE architecture as outlined in [I-D.ietf-ace-actors] introduces six actors - logical entities that have to perform specific security-related tasks; On the constrained level, client and server want to communicate securely. Their respective principals define authorization policies that need to be enacted. Each constrained device has a less-constrained device that can be entrusted with security-related tasks. One goal of the ACE WG is to enable entities on the constrained level to securely delegate some authorization-related tasks to an actor on the less-constrained level within the same security domain.

The ACE architecture facilitates various distinct application scenarios resulting in the following basic authorization message flows.

1. To access a resource on a server, the client presents an authorization token together with the request.

2. When a client tries to access a resource on a server, the server retrieves authorization information for this action.

3. The server disseminates encrypted data where the decryption key is bound to the client’s authorization.

In all cases, the authorization policies of both the client’s principal and the server’s principal must be considered to achieve their respective security goals. Depending on the selected authorization message flow, different actors need to exchange different information.

This document is structured as follows: Section 3 specifies 11 classes of Message Types that define how this information is securely conveyed over the network. Section 4 describes CoAP content formats that can be used to control the desired authorization message flow.

3. Message Type Classes

In the following, the classes of message types for authorization are listed. Each class consists of the effect this message has, the actors that send and receive this message, and the kind of protection

that such a message requires. Solutions can choose the message types they need to implement based on the effects they require.

3.1. Unauthorized Resource Request Message

Any resource request from C to S that is not covered by a valid ticket for C is treated as unauthorized request. If S decides to act upon an Unauthorized Resource Request it can reject the message and optionally inform C where it can ask for authorization, or, if S has authenticated C, S can directly ask SAM to authorize C’s request.

3.1.1. Effect

- S can act on the unauthorized request to determine if C is authorized, either by requesting authorization from SAM or by rejecting the request and optionally inform C about which SAM to contact in order to retrieve a valid authorization token.

- If S happens to be a gateway (GW) that serves content on behalf of another entity (called "origin server"), GW can act as previously described for S.

3.1.2. Actors

- C -> S

or, optionally,

- C -> GW

3.1.3. Protection Requirements

None.

3.2. SAM Information Message

A SAM Information Message can be used by S or a gateway (GW) that serves the requested resource on behalf of an origin server S to instruct C where it may retrieve authorization for a specific type of request. S (or GW, respectively) may optionally include requested data as an encrypted object with the SAM Information Message.

3.2.1. Effect

- C knows the address of SAM (where to request a ticket for S).

3.2.2. Actors

- S -> C

or optionally,

- GW -> C

3.2.3. Protection Requirements

If S/GW includes requested data with the SAM Information Message, it must provide for confidentiality and integrity of the data.

3.3. CAM Information Message

A CAM Information Message can be used by C to instruct S where it may retrieve an authorization token for C.

3.3.1. Effect

- S knows the address of CAM (where to request a ticket for C).

3.3.2. Actors

- C -> S

3.3.3. Protection Requirements

None.

3.4. Access Request Message

An Access Request Message is sent by C to request CAM to retrieve authorization information for a specific request. It includes information from a SAM Information message generated by S/GW.

3.4.1. Effect

- CAM knows the resources and actions C is requesting.
- CAM knows which SAM to contact.

3.4.2. Actors

- C -> CAM

3.4.3. Protection Requirements

- Integrity and Authenticity (CAM can validate that the message stems from C)
- Confidentiality (optional): the principals may not want others to know which resources and actions where requested.

3.5. Ticket Request Message

A Ticket Request message is sent by CAM on behalf of C to retrieve authorization from SAM for a specific action on S.

3.5.1. Effect

- SAM knows which actions on which resources are requested by CAM.
- SAM can determine permissions for CAM.
- SAM can generate an access ticket for C, which can be later used by C to demonstrate to S its authorization status.
- SAM can generate a verifier for C, which can be later used by C to verify that it is communicating with an appropriate S.

3.5.2. Actors

- CAM -> SAM

3.5.3. Protection Requirements

- Integrity and authenticity (SAM can validate that the message stems from CAM)
- Confidentiality (optional): the principals may not want others to know which resources and actions where requested.

3.6. Ticket Grant Message

A Ticket Grant message is sent by SAM to CAM to convey authorization information and a verifier that can be used by C to access protected resources on S.

3.6.1. Effect

- CAM received the Server Authorization Information (SAI)
- CAM received the verifier for C

- CAM can validate the origin of the ticket for C

3.6.2. Actors

- SAM -> CAM

3.6.3. Protection Requirements

- Confidentiality (SAM, CAM) (+ Integrity (implicit, the ticket already is integrity-protected))
- SAM knows the principal’s authorization policies for CAM

3.7. Ticket Transfer Message

The Ticket Transfer message is used by CAM to convey the authorization information and the verifier retrieved from SAM to C.

3.7.1. Effect

- C is able to prove its authorization status to S
- C is able to communicate securely with S

3.7.2. Actors

- CAM -> C

3.7.3. Protection Requirements

- Confidentiality (CAM, C) (+ Integrity if the ticket not already is integrity-protected)

3.8. Client Authorization Information Message

CAM can restrict the operations C performs on S by transferring Client Authentication Information (CAI) to C. This is specifically useful if S has requested additional information from C in order to proceed with C’s initial request.

3.8.1. Effect

- C gets the client authorization information (CAI) received from CAM
- C knows which information it is allowed to provide to S

3.8.2. Actors

- CAM -> C

3.8.3. Protection Requirements

- Integrity: attackers must not be able to manipulate the CAI.
- Confidentiality (optional): in some cases, principals might not want others to gain knowledge of the CAI.
- CAM knows the principal’s authorization policies for C.

3.9. Security Context Setup Between CAM and SAM

In the ACE architecture, the client may utilize an authorization manager (CAM) to contact the server-side authorization manager (SAM) and retrieve an authorization token for the intended action on a resource that SAM is responsible for. CAM needs to authenticate with SAM on behalf of C and must authenticate SAM. The message exchange between CAM and SAM establishes a security context that can be used to request authorization for CAM and transfer authorization policies for SAM.

3.9.1. Effect

- Mutual authentication (TODO: split)
- CAM can authenticate messages from SAM
- SAM can authenticate messages from CAM
- SAM can determine authorization policies for CAM
- CAM can determine authorization policies for SAM

3.9.2. Actors

- CAM <-> SAM

3.9.3. Protection Requirements

None.

3.10. Security Association between C and S

Once C has been authorized by SAM to access resources on S and by CAM to transmit data to S, both actors have a common security context that can be used to exchange further messages. The authorization information bound to this security context can be updated subsequently over a suitable interface provided by C and S.

3.10.1. Effect

- C can authenticate messages from S
- S can authenticate messages from C
- Further communication between C and S can be encrypted
- S knows the SAI for C

3.10.2. Actors

- C, S

3.10.3. Protection Requirements

- Integrity: Attackers must not be able to update the authorization information stored at S and C.
- Confidentiality (optional): Usually, only entities that are authorized to update the authorization information should be able to read that data.

3.11. Authorized Resource Request Message

Within the security association between C and S, request messages covered by the authorization information that is bound to the common security context are Authorized Resource Request messages that the receiver is allowed to process.

3.11.1. Effect

- S can process requests from C, C can process requests from S.

3.11.2. Actors

- C -> S

3.11.3. Protection Requirements

- Integrity
- Confidentiality (optional): the principals might not want others to know the requested resource.

3.12. Resource Response Message

Responses to Authorized Request messages are Resource Responses.

3.12.1. Effect

- C recieves the requested service from S.

3.12.2. Actors

- S -> C

3.12.3. Protection Requirements

- Integrity
- Confidentiality (optional): the principals might not want others to know the response content.

3.13. Server-Initiated Ticket Request Messages

TODO (see [I-D.gerdes-ace-dcaf-sitr])

4. Content Format

As the ACE working group aims at an authorization solution that follows a REST architecture style, the basic message flow is controlled by the content format that is used to convey authorization-specific data. For example, S might transfer the SAM Information message in content format 'application/cose+cbor' to indicate its capability of handling messages that use the COSE message syntax [I-D.ietf-cose-msg], or 'application/dcaf+cbor' to use the DCAF messaging format specified in [I-D.gerdes-ace-dcaf-authorize].

5. Security Considerations

TBD

6. IANA Considerations

This document has no actions for IANA.

7. Acknowledgements

The authors would like to thank Carsten Bormann for his valuable input and feedback.

8. Informative References

[I-D.gerdes-ace-dcaf-authorize]
Gerdes, S., Bergmann, O., and C. Bormann, "Delegated CoAP Authentication and Authorization Framework (DCAF)", draft-gerdes-ace-dcaf-authorize-03 (work in progress), September 2015.

[I-D.gerdes-ace-dcaf-sitr]
Gerdes, S., "Server-Initiated Ticket Request", draft-gerdes-ace-sitr-00 (work in progress), October 2015.

[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-02 (work in progress), October 2015.

[I-D.ietf-ace-usecases]
Seitz, L., Gerdes, S., Selander, G., Mani, M., and S. Kumar, "ACE use cases", draft-ietf-ace-usecases-09 (work in progress), October 2015.

[I-D.ietf-cose-msg]
Schaad, J., "CBOR Encoded Message Syntax", draft-ietf-cose-msg-06 (work in progress), October 2015.

Authors' Addresses

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

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

Jorge Cuellar
Siemens AG
CT RTC ITS

Email: jorge.cuellar @ siemens.com

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

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