D7.2

Preliminary Standardization Report

WP7 – Dissemination, Standardization and Exploitation

SIFIS-HOME

Secure Interoperable Full-Stack Internet of Things for Smart Home

Due date of deliverable: 31/03/2022
Actual submission date: 31/03/2022

Version 1.0

31/03/2022

Responsible partner:RISE
Editor: Marco Tiloca
E-mail address: marco.tiloca@ri.se

Project co-funded by the European Commission within the Horizon 2020 Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

The SIFIS-HOME Project is supported by funding under the Horizon 2020 Framework Program of the European Commission SU-ICT-2-2020 952652

Authors: Marco Tiloca (RISE), Rikard Höglund (RISE), Göran Selander (Ericsson)

Approved by: Marco Rasori (CNR), Tuuli Lindroos (FSC), Sean Robinson (FSC)

Revision History

Version	Date	Name	Partner	Section Affected Comments
0.1	2021-11-12	Initial content (to be revised)	RISE	All
0.2	2021-11-12	First completed version	RISE	All
0.3	2021-11-16	Initial remarks and comments for review	FSC	All
0.4	2021-11-16	Minor fixes; adopted comments	RISE	All
0.5	2021-12-07	Updated IETF document status	RISE	All
0.6	2022-02-17	Partner review comments	FSC	All
0.7	2022-02-22	Partner review comments	FSC	All
0.8	2022-03-03	Partner review comments	CNR	All
0.9	2022-03-08	Processed review comments	RISE	All
1.0	2022-03-30	Ready to submit	RISE	All

Executive Summary

This document summarizes the roles, initiatives, and achievements of SIFIS-Home partners with respect to standardization activities, during the first half of the project. The work includes 16 documents across 3 Working Groups within the Internet Engineering Task Force (IETF), the premier international standardization body for developing open Internet standards.

Table of contents

1 Introduction

Standardization is a major dissemination effort in the SIFIS-Home project, for which a specific Task T7.2 “Standardization” is dedicated in WP7 “Dissemination, Standardization and Exploitation”. This leverages the presence in the SIFIS-Home consortium of some partners with a strong participation and involvement in international standardization activities.

In particular, RISE and Ericsson have a long-term successful track record in the premier international body Internet Engineering Task Force (IETF), where for several years they have led the standardization of IoT security protocols, across multiple Working Groups. These Working Groups especially include “Constrained RESTful Environments” (CoRE), “Authentication and Authorization for Constrained Environments” (ACE) and “Lightweight Authenticated Key Exchange” (LAKE).

Such IETF contributions are strictly tied to SIFIS-Home activities that RISE and Ericsson carry out in WP3 “Network and System Security”. These include the design and development of solutions for secure (group) communication within T3.1 “Secure, Interoperable and Robust Communication”, as well as for access control and key management within T3.2 “Security Lifecycle Management”.

This document summarizes the roles, initiatives, and achievements that SIFIS-Home partners have had in the IETF standardization body during the first half of the SIFIS-Home project. This document will be updated and obsoleted by the Deliverable D7.5 “Final Standardization Report” due by the end of the SIFIS-Home project.

2 Overview of the Internet Engineering Task Force

The Internet Engineering Task Force (IETF) is the premier body developing open Internet standards through an open process, involving researchers, network designers, operators and vendors. In particular, "*the mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.*"

Standardization activities in the IETF take place within Working Groups (WGs), which are in turn organized into Areas. Inputs are provided in the form of written technical specifications, namely Internet Drafts, which are initially proposed as individual submissions. These may later be "adopted" by a WG as officially endorsed documents, which will be incrementally revised and advanced in a collective way. Eventually, an approved document is published in the series "Request For Comments" (RFC).

Each year, the IETF hosts three meetings, each of which occurs over five days and mostly consists of WG sessions. Each IETF meeting is preceded by a "Hackathon" event devoted to progress and test implementations of Internet Drafts and RFCs. In between the three main IETF meetings, several WG interim meetings are also scheduled, typically online.

The following overviews three IETF WGs referred to in the rest of this document.

- The IETF WG "Constrained RESTful Environments" (CoRE) provides solutions for resource-oriented applications intended to run on constrained IP networks. Typically, these networks are characterized by limited packet sizes and possible high packet loss. Besides, they could be largely composed of devices that are intermittently available and have limited capabilities in terms of computing power, memory resources, and energy availability (e.g., battery-powered devices). More details can be found at: https://datatracker.ietf.org/wg/core/about/

- The IETF WG "Authentication and Authorization for Constrained Environments" (ACE) provides a solution for authentication and authorization that enables authorized access to resources hosted on a resource server in constrained environments. Resource access is intended as based on REST operations, e.g., GET, PUT, POST, DELETE. The enforcement of access control policies is mediated by a non-constrained entity acting as authorization server. More details can be found at: https://datatracker.ietf.org/wg/ace/about/

- The IETF WG "Lightweight Authenticated Key Exchange" (LAKE) provides a lightweight authentication key establishment protocol suitable for resource-constrained devices, the main use case being applications using the security protocol Object Security for Constrained RESTful Environments (OSCORE). More details can be found at: https://datatracker.ietf.org/wg/lake/about/

3 Involvement of SIFIS-Home partners in the IETF

The SIFIS-Home partners RISE and Ericsson have a long-term and successful track record in IETF standardization of IoT security protocols, especially in the Working Groups CoRE, ACE, and LAKE.

Besides regularly participating as key contributors to such standardization activities, individuals from both RISE and Ericsson have taken additional responsibility roles. In particular:

- Francesca Palombini (Ericsson) is Area Director for the Area "Application and Real-Time" (ART).
- Marco Tiloca (RISE) is Chair of the WG CoRE. He is also a member of the Internet-of-Things Directorate and of the ART Area Review Team.

3.1. Ongoing Standardization Works

The following list includes the IETF documents with RISE and/or Ericsson as co-author. For each of them, a brief description and the current status are provided.

In the LAKE Working Group

Ephemeral Diffie-Hellman Over COSE (EDHOC)
A very compact and lightweight authenticated Diffie-Hellman key exchange with ephemeral keys, providing mutual authentication, forward secrecy, and identity protection. EDHOC is intended for constrained scenarios, and a main use case is to establish a Security Context for the security protocol Object Security for Constrained RESTful Environments (OSCORE).
https://datatracker.ietf.org/doc/draft-ietf-lake-edhoc/
***Status**: Adopted as Working Group document*

In the CoRE Working Group

Group Communication for the Constrained Application Protocol (CoAP)
Usage of the Constrained Application Protocol for group communication, using UDP/IP multicast as the underlying data transport.
https://datatracker.ietf.org/doc/draft-ietf-core-groupcomm-bis/
***Status**: Adopted as Working Group document*

Group OSCORE – Secure Group Communication for CoAP
A method for protecting group communication over CoAP, based on OSCORE.
https://datatracker.ietf.org/doc/draft-ietf-core-oscore-groupcomm/
***Status**: Adopted as Working Group document*

Observe Notifications as CoAP Multicast Responses
Method for a CoAP server to send (secure) observe notifications as response messages over IP multicast.
https://datatracker.ietf.org/doc/draft-ietf-core-observe-multicast-notifications/
***Status**: Adopted as Working Group document*

Profiling EDHOC for CoAP and OSCORE
Additional and optional features for the authenticated key establishment protocol EDHOC when run over the CoAP protocol. These especially include a method to efficiently combine the execution EDHOC with a following message exchange protected with OSCORE.
https://datatracker.ietf.org/doc/draft-ietf-core-oscore-edhoc/
***Status**: Adopted as Working Group document*

Key Update for OSCORE (KUDOS)
A method for two OSCORE peers to address the limits of the used AEAD algorithms, so that the security of their communications is preserved. This lightweight method enables the two peers to update their keying material and establish a new OSCORE Security Context.
https://datatracker.ietf.org/doc/draft-ietf-core-oscore-key-update/
***Status**: Adopted as Working Group document*

Discovery of OSCORE Groups with the CoRE Resource Directory
Method for a CoAP endpoint to use the CoRE Resource Directory for discovering OSCORE groups and acquiring information to join them.
https://datatracker.ietf.org/doc/draft-tiloca-core-oscore-discovery/
***Status**: Individual submission*

Proxy Operations for CoAP Group Communication
A method to enable CoAP forward-proxies to operate in group communication scenarios. The proxy forwards a client's request to multiple servers, e.g., over IP multicast. Then, it receives the servers' responses and forwards them back to the client, in such a way that the client is able to distinguish each response's origin.
https://datatracker.ietf.org/doc/draft-tiloca-core-groupcomm-proxy/
***Status**: Individual submission*

Cacheable OSCORE
A method to enable CoAP forward proxies to cache response messages protected with Group OSCORE.
https://datatracker.ietf.org/doc/draft-amsuess-core-cachable-oscore/
***Status**: Individual submission*

OSCORE-capable Proxies
A method for protecting CoAP messages with OSCORE also between an origin application endpoint and an intermediary, or between two intermediaries. This includes the possible double-protection of a message through "OSCORE-in-OSCORE", i.e., both end-to-end between origin application endpoints, as well as between an application endpoint and an intermediary.
https://datatracker.ietf.org/doc/html/draft-tiloca-core-oscore-capable-proxies

***Status**: Individual submission*

In the ACE Working Group

OSCORE profile of the Authentication and Authorization for Constrained Environments Framework
A profile for the ACE framework, which utilizes OSCORE in order to achieve communication security, server authentication, and proof-of-possession.
https://datatracker.ietf.org/doc/draft-ietf-ace-oscore-profile/
***Status**: Approved for publication as Proposed Standard*

Key Provisioning for Group Communication using ACE
Definition of message formats and procedures based on the ACE framework, to request and distribute group keying material, which is then used to protect communications among members of a group.
https://datatracker.ietf.org/doc/draft-ietf-ace-key-groupcomm/
***Status**: Adopted as Working Group document*

Key Management for OSCORE Groups in ACE
A method to request and provision keying material in group communication scenarios where the group communication is based on CoAP and secured with Group OSCORE, building on the ACE framework for Authentication and Authorization.
https://datatracker.ietf.org/doc/draft-ietf-ace-key-groupcomm-oscore/
***Status**: Adopted as Working Group document*

Admin Interface for the OSCORE Group Manager
A RESTful admin interface at the OSCORE Group Manager, that allows an Administrator entity to create and delete OSCORE groups, as well as to retrieve and update their configuration. The ACE framework for Authentication and Authorization is used to enforce authentication and authorization of the Administrator at the Group Manager.
https://datatracker.ietf.org/doc/draft-ietf-ace-oscore-gm-admin/
***Status**: Adopted as Working Group document*

Notification of Revoked Access Tokens in the Authentication and Authorization for Constrained Environments (ACE) Framework
A method for the ACE framework to allow an authorization server to notify registered devices (i.e., clients and resource servers) about issued access tokens that have been revoked but are not expired yet.
https://datatracker.ietf.org/doc/draft-ietf-ace-revoked-token-notification/
***Status**: Adopted as Working Group document*

Group OSCORE Profile of the Authentication and Authorization for Constrained Environments Framework
A profile for the ACE framework, which utilizes Group OSCORE possibly together with OSCORE, to provide communication security between a client and (a group of) resource server(s), while achieving server authentication, proof-of-possession and proof of client's group membership.

https://datatracker.ietf.org/doc/draft-tiloca-ace-group-oscore-profile/
***Status**: Individual submission*

4 Conclusion

This document has summarized the roles, activities, and achievements of SIFIS-Home partners within the international standardization body Internet Engineering Task Force (IETF), during the first half of the project. This document will be updated and obsoleted by the Deliverable D7.5 “Final Standardization Report” to be released at the end of the project.

5 Annex A: Glossary

Acronym	Definition
ACE	Authentication and Authorization for Constrained Environments
AEAD	Authenticated Encryption with Associated Data
ART	Application and Real-Time
CBOR	Concise Binary Object Representation
CoAP	Constrained Application Protocol
CoRE	Constrained RESTful Environments
COSE	CBOR Object Signing and Encryption
EDHOC	Ephemeral Diffie-Hellman over COSE
IETF	Internet Engineering Task Force
IP	Internet Protocol
LAKE	Lightweight Authenticated Key Exchange
OSCORE	Object Security for Constrained RESTful Environments
REST	REpresentational State Transfer
RFC	Request For Comments
SIFIS-Home	Secure Interoperable Full Stack Internet of Things for Smart Home
UDP	User Datagram Protocol
WG	Working Group