D3.1

D3.1 Analyses and Feedback on Architecture Requirements and Goals

WP3 – Network and System Security

SIFIS-Home

Secure Interoperable Full-Stack Internet of Things for Smart Home

Due date of deliverable: 31/05/2021
Actual submission date: 31/05/2021

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

28/05/2021
Version 1.1

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-02-2020 GA 952652

Authors: Marco Tiloca (RISE), Rikard Höglund (RISE), Göran Selander (Ericsson), Paolo Mori (CNR), Andrea Saracino (CNR)

Approved by: Luca Ardito (POL), Joni Jämsä (CEN)

Revision History

Version	Date	Name	Partners	Section Affected Comments
0.1	18/03/2021	M. Tiloca	RISE	Document created
0.2	23/03/2021	M. Tiloca	RISE	Executive summary and conclusion
0.3	24/03/2021	M. Tiloca	RISE	Detailed placeholders throughout the document; initial glossary
0.4	25/03/2021	M. Tiloca	RISE	Structure and format completed; ready to include the content
0.5	28/03/2021	M. Tiloca	RISE	Included original requirements from D1.1
0.6	29/03/2021	M. Tiloca	RISE	Included background description for most of WP3 topics
0.7	31/03/2021	R. Höglund	RISE	Background on DDoS mitigation and OSCORE key usage limits
0.8	13/04/2021	R. Höglund and M. Tiloca	RISE	Filling tables for requirements analysis and new requirements
0.9	17/04/2021	M. Tiloca	RISE	Introduction; table captions; editorial improvements
0.10	24/04/2021	M. Tiloca	RISE	Less new functional requirements; editorial fixes
1.0	28/04/2021	M. Tiloca and A.Saracino	RISE/CNR	Ready for review
1.01	04/05/2021	R. Höglund & M. Tiloca	RISE	Updated according to feedback from Joni Jämsä
1.02	14/05/2021	R. Höglund & M. Tiloca	RISE	Updated according to feedback from Luca Ardito
1.1	28/05/2021	R. Höglund	RISE	Ready to Submit

Executive Summary

This document provides WP1 "Distributed System Architecture" with feedback and additional input, based on an analysis of the deliverable D1.1 "Initial Architecture Requirements Report" carried out in WP3 "Network and System Security". The contribution of this document is twofold. First, it provides feedback about and request for adaptations of the requirements defined in D1.1. Second, it provides additional requirements related to network & system security, to be additionally considered in the final SIFIS-Home system and its architecture. Both contributions have considered the planned network & system security solutions to be developed in WP3, and will be seminal for the deliverable D1.2 "Final Architecture Requirements Report", which in turn will be a guideline for the development of the security solutions in WP3. The present document has the same purpose fulfilled by the companion deliverable D4.1 "Analyses and Feedback on Architecture Requirements and Goals" in WP4 “Privacy-Aware Analytics for Security and Privacy Services”.

Table of contents

1 Introduction

The main objective of the SIFIS-Home project is to provide a secure-by-design and consistent software framework for improving resilience of interconnected smart home systems at all stack levels. To address this goal, the software framework shall ensure correct functionality of the smart home system as well as security, privacy and safety of all SIFIS-Home users. This requires for eliciting requirements - especially focused on security and privacy aspects - to be considered and ultimately fulfilled by the SIFIS-Home system.

The SIFIS-Home deliverable D1.1 “Initial Architecture Requirements Report” has provided a set of initial requirements for the SIFIS-Home system. These have been classified as Functional, Non-Functional and Security requirements, as well as according to different priority levels. This first set of requirements has been provided as input to WP3 and WP4, in order for them to produce feedback, requests of amendments as well as further new requirements to be included in the intended final set to be specified by WP1 in its later deliverable D1.2 "Final Architecture Requirements Report".

This document is the first deliverable from WP3 and provides WP1 with such an aggregated feedback, resulting from a revision of the original requirements in the light of the network & system security solutions developed in WP3. For consistency, the same taxonomy and requirement priorities considered in D1.1 have been used in this document. In particular, the contribution of this document consists of and is organized as follows.

First, Section 3 provides a high-level overview of the different technical areas related to network & system security covered in WP3, and a focus for developing security solutions for the SIFIS-Home system. These are especially related to the activities carried out in the three Tasks of WP3, and their preliminary version will be documented in deliverable D3.2 “Preliminary Report on Network and System Security Solutions”.

Second, Section 4 provides a collection of detailed feedback and requests for amendments about the initial set of requirements elicited in WP1 and documented in deliverable D1.1. In particular, feedback and requests for amendment are provided separately for the initial Functional Requirements (see Section 4.1), Non-Functional Requirements (see Section 4.2) and Security Requirements (see Section 4.3) from deliverable D1.1.

Third, Section 5 provides a collection of newly defined requirements to be added to the final requirement set, in the light of the network & system security solutions developed in WP3. Consistently with deliverable D1.1, each of the new requirements have been assigned a priority level and have been associated with other pertinent relatable requirements from the initial set and/or the new set. In addition, the new Functional Requirements have been also mapped to the pertinent Use Cases elicited in Section 5.2 of deliverable D1.1, while the new Security Requirements have been further classified as either Testable or Non-Testable.

The contribution from this document will act as input to WP1, where it will be seminal for the deliverable D1.2, as intended to provide a final, refined set of requirements for the SIFIS-Home system. In turn, deliverable D1.2 will be a guideline for the development of the network & system security solutions in WP3.

Finally, this document has the same purpose fulfilled by the companion deliverable D4.1 "Analyses and Feedback on Architecture Requirements and Goals" in WP4 “Privacy-Aware Analytics for Security and Privacy Services”. Therefore, the final set of requirements to be specified in deliverable

D1.2 will effectively take into account feedback and new input from both WP3 and WP4, as aligned with their technical activities.

2 Addressed Security Areas and Related Work Topics

This section considers the technical areas covered in WP3 “Network and System Security” and provides a brief overview of the related security solutions currently under development in the same Work Package.

The following highlights the overall scope, functionality and goals of the security solutions under development. These are later taken into account in Section 4, when providing feedback and request for adaptations to requirements defined in deliverable D1.1 “Initial Architecture Requirements Report”, as well as in Section 5 when providing new additional requirements.

2.1 *End-to-end secure communication, with support for groups*

The below security solutions are developed in Task T3.1 “Secure Interoperable and Robust Communication”.

Group OSCORE to secure group communication for CoAP – The security protocol Group Object Security for Constrained RESTful Environments (Group OSCORE) is currently under development, in order to protect communications when the Constrained Application Protocol (CoAP) [Shelby, 2014] is used in a group communication environment [Rahman, 2014]. That is, a CoAP client can send a request intended to multiple recipients (e.g., over IP multicast), each of which can reply with an individual response. Group OSCORE builds on the OSCORE security protocol [Selander, 2019], i.e. it uses the same core components CBOR [Bormann, 2020] and COSE [Schaad, 2017], and provides end-to-end security of CoAP messages at the application layer. In particular, it aims at providing source authentication of all messages exchanged in the group, and at ensuring secure binding between a request and all the associated responses.

Setup, configuration and discovery of OSCORE groups – Secure group communications based on the security protocol Group Object Security for Constrained RESTful Environments (Group OSCORE) rely on a Group Manager. Among other things, the Group Manager is responsible to drive the joining process of new group members, as well as to provide possible assistance to current group members. However, two additional services are required to cover the full group lifecycle. First, authorized Administrators must be able to create and configure OSCORE groups at the Group Manager. Second, just deployed devices must be able to discover an OSCORE group, and especially which Group Manager they should contact in order to join it.

Support for proxying in (secure) group communication – The Constrained Application Protocol (CoAP) [Shelby, 2014] natively supports the use of intermediaries, such as proxies, between a client endpoint and a server endpoint. These can, among other things, serve cached responses or perform protocol translation across different legs. When one-to-many group communication for CoAP is considered [Rahman, 2014], several processing steps at intermediaries are left open. Work is ongoing on defining how forward-proxies and reverse-proxies forward a group request to multiple servers, and then forward back the multiple individual responses to the original client. Support must be ensured also in case group communications are protected end-to-end with the security protocol Group Object Security for Constrained RESTful Environments (Group OSCORE).

Support for (secure) one-to-many notifications in group communications – The Constrained Application Protocol (CoAP) [Shelby, 2014] has been enriched with the "Observe" extension [Hartke, 2015]. This allows a client to register its interest at a server's resource, thus automatically getting notification responses from the server when the resource representation changes. This is currently being enabled also in group communication scenarios [Rahman, 2014], where one client endpoint can simultaneously observe a shared group resource at multiple servers. However, some group

applications (e.g., publish-subscribe) would benefit of a reversed pattern, i.e. when multiple client all observe the same resource at one server. Work is ongoing to define how a server can provide such a functionality, by sending one single notification response (which is currently not specified for CoAP) targeting all the observer clients at once (e.g. over IP multicast). Support must be ensured also in case intermediaries (e.g. proxies) are used, and in case group communications are protected end-to-end with the security protocol Group Object Security for Constrained RESTful Environments (Group OSCORE).

Cacheable OSCORE responses – The security protocol Object Security for Constrained RESTful Environments (OSCORE) [Selander, 2019] does not normally make it possible to cache protected responses at intermediaries like proxies. In fact, two identical plain requests result in two different OSCORE-protected requests, hence never producing a cache hit. Work is ongoing to enable cacheability of OSCORE responses, building on the "deterministic request" concept. In applications providing content distribution, this would allow intermediaries to serve several clients' requests from their own cache, thus incurring in less traffic and accesses at the origin servers, as well as achieving considerable improvements in terms of performance.

2.2 *Adaptive reaction against (Distributed) Denial of Service*

The below security solutions are developed in Task T3.1 “Secure Interoperable and Robust Communication”.

Context-aware reactive DDoS mitigation – Denial of Service (DoS) attacks aim at making the targeted device unavailable for other devices trying to reach it, thus hindering the system from serving legitimate clients. In Internet of Things (IoT) scenarios where devices are often constrained in terms of resources and power, these kinds of attacks can be particularly effective. A solution is being developed to mitigate the impact of these attacks. It relies on a reactive, adaptive and host-based approach that takes as input information about ongoing attacks from used communication layers, such as DTLS [Rescorla, 2021]. By understanding when an attack is in progress and its severity, the victim device can react by trading service availability and quality of service against attack exposure. Under severe attack conditions, this can involve an intermediary for holding and relaying messages, and the usage of low-power modes of operation to limit the impact on energy consumption.

2.3 *Authentication and Authorization for access control*

The below security solutions are developed in Task T3.2 “Security Lifecycle Management”.

OSCORE profile and Group OSCORE profile of ACE – The ACE Framework for Authentication and Authorization in Constrained Environments (ACE) [Seitz, 2021] delegates to separate specifications the details about secure communication between the ACE entities, and especially Clients and Resource Servers. Work is ongoing to define different profiles of ACE, to enable secure communication between Client and Resource Servers as based on the OSCORE security protocol [Selander, 2019]; or based on the Group OSCORE security protocol, when the ACE client is a member of an OSCORE group and access control is enforced for accessing resources at ACE Resource Servers in the same OSCORE group. Both profiles aim at providing mutual authentication of Client and Resource Server, as well as proof-of-possession of involved secret keys.

Notification of revoked access credentials – The ACE Framework for Authentication and Authorization in Constrained Environments (ACE) [Seitz, 2021] relies on Access Tokens as authorization credentials. These may not only expire but also be explicitly revoked. However, discovering about revoked Access Tokens is limited to ACE Resource Servers, through an actively started “introspection” of one Access Token at a time. The design of a solution is ongoing to enable

automatic and efficient notification of revoked, although still unexpired, Access Tokens to any device using ACE, supporting different levels of granularity in the reported information. This in turn can act as a building block to enforce usage control through the dynamic revocation of access credentials, following changes in the evaluation of access control policies.

2.4 *Establishment and provisioning of cryptographic keying material*

The below security solutions are developed in Task T3.2 "Security Lifecycle Management".

The EDHOC protocol with optimizations for OSCORE – Ephemeral Diffie-Hellman Over COSE (EDHOC) is under development to enable lightweight establishment of key material between two constrained devices, using CBOR Object Signing and Encryption (COSE) [COSE] as its core building block. The goal is for EDHOC to also provide mutual authentication of the two peers and perfect forward secrecy of the established secret. Its main use case is to establish a Security Context that the two peers can use to run the application-layer security protocol OSCORE [OSCORE]. Specific optimizations are also under development, especially to merge on one hand the last EDHOC message, and on the other hand the first OSCORE request protected with the Security Context derived through the EDHOC execution in question.

Key provisioning for Group OSCORE using ACE – The ACE Framework for Authentication and Authorization in Constrained Environments (ACE) is being used to enable the distribution of key material for group communication to be protected with Group OSCORE. In particular, a candidate member that wishes to join an OSCORE group acts as an ACE client, and provides its authorization credentials to the OSCORE Group Manager acting as an ACE Resource Server. As a result, the authorized candidate member joins the OSCORE group, and receives from the Group Manager the key material to communicate with other group members using Group OSCORE. Further operations at the Group Manager are also defined for current group members.

Limits of key usage for OSCORE and related rekeying – Object Security for Constrained RESTful Environments (OSCORE) provides application-layer end-to-end protection between endpoints communicating with the Constrained Application Protocol (CoAP) [Shelby, 2014]. OSCORE uses AEAD algorithms to ensure integrity and confidentiality of the exchanged messages. Based on security analysis of AEAD algorithms [Günther, 2021], issues have been identified that can allow forgery attacks against such algorithms. Thus, limits must be considered as to how many times a certain key is used for encryption, or how many failed decryptions should be allowed for one key. If these limits are exceeded, further use of the keys can allow breaking the security properties of the algorithms. Work is ongoing on how to take these limits into account when using OSCORE. This includes defining appropriate limits for OSCORE, updating the message processing steps, and defining actions to take if the limits are exceeded (e.g., by efficiently renewing the OSCORE key material).

2.5 *Dynamic handling of security and safety policies*

Work on the below security solutions is being carried out partly in Task T3.2 "Security Lifecycle Management" and especially in Task T3.3 "Dynamic Multi-Domain Security and Safety Policy Handling". The work of Task T3.3 focuses on definition and handling of security and safety policies which regulate access rights to resources and functionalities of the SIFIS-Home framework. Pairing with the access control functionalities considered in Task T3.2 and mostly based on the ACE framework, Task T3.3 focuses on policies definition and evaluation, facing the challenge of managing mutable conditions. The policies used in Task T3.3 build on the ABAC (Attribute Based Access Control) mode, exploiting XACML for policy definition and verification.

Assessment of policies based on dynamic parameters – The policies that will be used in Task T3.3 are based on an extension of the classical ABAC model, namely Usage Control (UCON) [Park, 2004], as capable to reactively handle conditions with mutable attributes, i.e., policies that are based on attributes whose value might change over time. The UCON policies are enforced over time, hence a specific resource usage which has been granted at a point in time can be revoked if the attribute values change and do not match the previous policies' access condition anymore. This poses requirements for subscription to attribute value changes or for the implementation of a periodic polling mechanism to timely detect value changes and accordingly take action.

3 Feedback and Request for Adaptations to the Requirements Defined in D1.1

This section analyses the requirements defined in D1.1 in the light of the security solutions that will be designed in WP3. As a reminder, the requirements are grouped into three different categories associated to their priority level, namely Critical (C), Standard (S) and Optional (O).

For each considered security requirement, an overall feedback is provided under the "Feedback" column of the pertaining table, with one of the following values defined below. When appropriate, side comments are provided under the "Comments" column of the pertaining table.

- **OK** – The considered requirement is fine as is.
- **Refine** – The considered requirement can be improved to be more accurate and comprehensive, as explained by the side comments.
- **Amend** – The considered requirement conflicts with new requirements related to security solutions from WP3 as listed later in Section 5, and/or with the network & system security solutions as such (see Section 2). Thus, the requirement has to be updated in order to solve the conflict, as explained by the side comments.
- **Delete** – The considered requirement is not appropriate and has to be removed, due to the reasons explained by the side comments.

3.1 *Functional Requirements Analysis*

The following Table 1 provides a list of feedback and request of amendments to the functional requirements defined in Section 6.1 of D1.1.

Req	Req. Description	Priority	Feedback	Comments
F-01	The SIFIS-Home framework shall provide a means of identifying the users inside the smart home through biometrics.	C	Refine	Which kinds of users is this intended for? Presumably all, but UC1 mentions only Restricted User and Administrator as "Primary, Secondary Actors". This might play a role for access control of users/devices and consistent provisioning of key material.
F-02	The SIFIS-Home system shall provide a means of authentication to the resident users and administrators inside the smart home.	S	Refine	Presumably, the resident users and the administrators are provided with a means to authenticate any user in

				the home, which in turn relies on the biometric-based identification. Correct? Is authentication about "You're not in a deny-list"? This seems very tight to F-01. Shouldn't this be also Critical? This might play a role for access control of users/devices and consistent provisioning of key material.
F-03	The SIFIS-Home system shall match read biometrics with a database of stored ones.	S	OK	
F-04	The system shall activate features based on the user identity.	S	OK	
F-05	The system shall activate a guest profile when the identity of the biometrics is not recognised.	S	Refine	First possible interpretation: anyone that "managed to get in" is fine to be at least a Guest user. Then, this requirement should be critical. Second possible interpretation: by default, a non-identified user does not get any profile at all, but it is still fine to possibly give them a Guest profile. In either case, this sounds like assuming that a first gate of physical access has been successfully passed (through some other means). This might play a role for access control of users/devices and consistent provisioning of key material.
F-06	The SIFIS-Home system shall provide a means of recognition of	C	Refine	Is this about physical access to the premises? Is it

	allowed users in the smart home.			also based on biometrics? It can be more explicit, and it would connect with F-05 (see related comment). This might play a role for access control of users/devices and consistent provisioning of key material.
F-07	The SIFIS-Home system shall provide Automatic Speech Recognition (ASR) to provide the residents the facility to control their home appliances through their speech.	C	Refine	Is it intentional to not cover also Administrators, Restricted Users and Guests? This might play a role for access control of users/devices and consistent provisioning of key material.
F-08	The SIFIS-Home system shall receive and interpret the voice commands provided by the user.	C	OK	
F-09	The SIFIS-Home system shall be able to execute all the recognisable voice commands.	C	OK	
F-10	The SIFIS-Home system shall signal the presence of an intruder when their identity is not recognised and no residents are at home.	C	OK	
F-11	The SIFIS-Home system shall record intruder actions through cameras.	S	OK	
F-12	The SIFIS-Home system shall store the identity of the intruder if the face is recognised.	O	Amend	What about a recognized user that somehow got physically in, but is blacklisted and not welcome (e.g. well-known stalker)? They are not an intruder but still an undesired presence. This does not appear to be covered, and it should be. This might play a role for access control of users/devices and consistent provisioning of key material.
F-13	The SIFIS-Home system may grant the access to recording to the maintainer.	S	Refine	Proposed rephrasing: "The SIFIS-Home system should allow the Administrators to

				possibly grant access to the video recording to the maintainer". Shouldn't this actually be Critical? This might play a role for access control of users/devices and consistent provisioning of key material.
F-14	The SIFIS-Home system may allow to contact police to receive assistance in case of intrusions.	O	Refine	To which users may the system allow this? This might play a role for access control of users/devices and consistent provisioning of key material.
F-15	The SIFIS-Home system shall provide a means of identifying anomaly behaviours inside the smart home.	C	OK	
F-16	The SIFIS-Home system shall provide a means of recognition of allowed users in unusual locations or performing dangerous actions.	S	Refine	To which users should the system provide these means? Such beneficiaries are likely to be the (few) ones defining what is unusual and dangerous. This might play a role for access control of users/devices and consistent provisioning of key material.
F-17	The SIFIS-Home system shall provide a means of recognising the prohibited objects inside the smart home.	S	Refine	To which users should the system provide these means? Such beneficiaries are likely to be the (few) ones defining what objects are prohibited. This might play a role for access control of users/devices and consistent provisioning of key material.
F-18	The SIFIS-Home system shall provide a means of recognition of	O	Refine	To which users should the system provide these

	allowed objects in unusual positions.			means? Such beneficiaries are likely to be the (few) ones defining what positions are unusual for what objects.
F-19	The SIFIS-Home system shall identify and isolate infected devices.	C	Refine	Before identifying them, these devices have to be detected in the first place, to prevent them, e.g., to continue communicating. Also, what does "isolate" a device mean? While still generic enough, perhaps "silence and deaf"/"disable"/"neutralize" might be better.
F-20	The SIFIS-Home system shall notify the user when malware is detected.	C	Refine	Which types of users should be notified? This might play a role for access control of users/devices and consistent provisioning of key material.
F-21	The SIFIS-Home system may execute self-healing algorithms to transfer functionalities of isolated devices to the others.	C	OK	
F-22	The SIFIS-Home system may allow means of verifying that the malware has not spread to other devices.	S	OK	
F-23	The SIFIS-Home system shall allow the resident user to register a new device.	C	Amend	This probably means just to "register one more component in the system." Other particular registration concerning that device (e.g., related to access control) are better left only to administrators and possibly delegated to selected resident users. This might play a role for access control of users/devices and consistent provisioning of key material.
F-24	The SIFIS-Home system shall provide a list of the registered	C	Refine	To which kinds of users?

	devices to the user along with their characteristics.			This might play a role for access control of users/devices and consistent provisioning of key material.
F-25	The SIFIS-Home system shall allow the user to unregister a registered device.	C	Amend	Same comment as for F-23, here about de-registration. This might play a role for access control of users/devices and consistent provisioning of key material.
F-26	The SIFIS-Home systems shall expose a section where the resident users and administrators can configure the devices.	C	Amend	By default, a device should be possible to configure only by the administrator and the exact user that registered it. They should also be the only one possibly enabling other users to do this. This might play a role for access control of users/devices and consistent provisioning of key material.
F-27	The SIFIS-Home system shall prompt the user when unsolicited configuration changes are propagated to the devices.	S	Amend	Which users are prompted? This might play a role for defining groups of users/devices receiving these notifications, and possibly the associated key material to process them.
F-28	The SIFIS-Home system must provide a marketplace function for the download of third-party applications on smart devices.	C	Refine	Is it admitted to install 3rd party applications that do not come from the Marketplace? Shouldn't this cover also the installation process? If not, then a requirement is probably missing, since UC8 is actually about *installing* 3rd party applications. This might play a role for following access control,

				key material required, and identity credential to perform these operations.
F-29	The SIFIS-Home system shall provide information about the safety and security aspects of an application to the user.	C	OK	
F-30	The SIFIS-Home system must provide a feature to show the administrator a list of currently active policies.	S	OK	
F-31	The SIFIS-Home system must allow the administrator to configure the policies to restrict/enable access to functionalities.	C	OK	
F-32	The SIFIS-Home system must allow the administrator to configure policies for groups of users.	S	OK	
F-33	The SIFIS-Home system must allow the administrator to configure policies for group of devices.	S	OK	
F-34	The SIFIS-Home system must allow the administrator to see the list of features/resources that are allowed or forbidden for all groups of users.	S	Refine	Hardly enforceable. Usually, if something is not stated or admitted by default, it is not allowed. This might play a role for access control to users/devices and consistent provisioning of key material.
F-35	The SIFIS-Home system must allow the administrator to see the list of features/resources that are allowed or forbidden for all groups of devices.	S	Refine	Hardly enforceable. Usually, if something is not stated or admitted by default, it is not allowed. This might play a role for access control to users/devices and consistent provisioning of key material.
F-36	The SIFIS-Home system must provide the user with a feature to list all the currently available profiles.	S	Refine	Maybe a related requirement is missing. Who defines the set of possible profiles for a given user? This might play a role for access control to users/devices and

				consistent provisioning of key material.
F-37	The SIFIS-Home system must allow the user to configure its profiles.	S	OK	
F-38	The SIFIS-Home system must allow the user to switch his/her current profile.	O	OK	
F-39	The SIFIS-Home system should show the user a summary of the preferences associated to its current profile.	O	OK	
F-40	The SIFIS-Home system should show notifications to the user when the current profile is changed.	O	OK	
F-41	The SIFIS-Home system should offer aggregate analytics and statistics about the usage of devices to the administrator.	S	OK	
F-42	The SIFIS-Home system should offer aggregate analytics and statistics about the usage of profiles to the administrator.	S	OK	
F-43	The SIFIS-Home system must offer remote log-in features to a configurer/maintainer of user profiles.	S	OK	
F-44	The SIFIS-Home system shall offer a panel with the remote houses that can be managed by a maintainer.	S	Refine	To which kinds of users is this panel provided? This might play a role for access control to users/devices and consistent provisioning of key material.
F-45	The SIFIS-Home system must offer the maintainer a panel to react in case of intrusions.	S	OK	
F-46	The SIFIS-Home system shall store personal resident information (video, audio, text).	C	OK	

Table 1: List of feedback to the original Functional Requirements for the SIFIS-Home system.

3.2 *Non-Functional Requirements Analysis*

The following Table 2 provides a list a list of feedback and request of amendments to the non-functional requirements defined in Section 6.2 of D1.1.

Req	Req. Description	Priority	Feedback	Comments
PE-01	The user authentication shall happen in less than 2s.	C	OK	
PE-02	The user recognition	C	OK	

	(identification) shall happen in less than 2s.			
PE-03	Identification through biometrics should be performed in less than 5 seconds.	S	OK	
PE-04	Biometric-based authentication should be performed in less than 5 seconds.	S	OK	
PE-05	Activation of features based on user identity (biometric recognition) should be performed in less than 5 seconds.	S	OK	
PE-06	Recognition of the start of an interaction through voice command should be performed in less than 2 seconds.	S	OK	
PE-07	The interpretation of the voice commands provided by the user should be performed in less than 2 seconds.	S	OK	
PE-08	The execution of the commands should be performed in less than 5 seconds.	S	OK	
PE-09	The maintainer must be able to access and watch the recording in less than one minute.	S	OK	
PE-10	The SIFIS-Home system shall contact police to receive assistance in less than 30 seconds.	O	OK	
PE-11	Identification of installed malware should be completed in less than 60 seconds from the execution of malware.	O	OK	
PE-12	The user should be informed of the presence of a malware in 5 seconds after the malware is recognised.	S	OK	
PE-13	Self-healing algorithms should be started in less than 60 seconds if available when malware is recognised.	C	OK	
PE-14	The registration of a new device should be completed in less than 30 seconds.	S	OK	
PE-15	The list of registered devices shall be shown by the SIFIS-Home system in less than 30 seconds.	S	OK	
PE-16	The de-registration of a device should be completed in less than 30 seconds.	S	OK	

PE-17	The configuration changes should be propagated successfully in less than 30 seconds.	C	Refine	The configuration change might not be completed successfully. More generally, what has to be propagated is the result of the attempted configuration change. Does "propagated successfully" mean correctly received by all the interested parties? Or is it simply about a first sending attempt? This is relatable to (secure) communication in the network.
PE-18	The current configuration of a device should be retrieved in less than 10 seconds.	S	OK	
PE-19	The marketplace should be accessed in less than 60 seconds.	S	OK	
PE-20	The configuration of policies for groups of users should be applied in less than 60 seconds.	C	Refine	What does “apply” mean? Become enforced? This may require revocation of current access credentials within that time limit. This might play a role for access control of users/devices and consistent provisioning of key material.
PE-21	The configuration of policies for groups of devices should be applied in less than 60 seconds.	C	Refine	What does “apply” mean? Become enforced? This may require revocation of current access credentials within that time limit. This might play a role for access control to users/devices and consistent provisioning of key material.
PE-22	The list of policies should be retrieved in less than 30 seconds.	S	OK	
PE-23	The configuration of profiles	C	Refine	What does “apply” mean?

	should be applied in less than 60 seconds.			Become enforced? This may require revocation of current access credentials within that time limit. This might play a role for access control of users/devices and consistent provisioning of key material.
PE-24	The change of current profile should be performed in less than 60 seconds.	C	Refine	What's the difference with respect to PE-23? This might play a role for access control of users/devices and consistent provisioning of key material.
PE-25	The statistics about usage of devices should be presented to the administrator in less than 30 seconds.	S	OK	
PE-26	The statistics about usage of profiles should be presented to the administrator in less than 30 seconds.	S	OK	
PE-27	Remote log-in should be performed in less than 60 second.	C	OK	
RE-01	The system shall not fail more than once a week (on average).	C	OK	
RE-02	The system shall not take more than one day to be repaired (on average).	C	OK	
AV-01	The system shall be available 99% of the time.	C	OK	
AV-02	The SIFIS-Home system shall ensure basic services availability in case of system failures.	C	OK	
US-01	The system shall be easy to use for average tech users.	C	OK	
US-02	The SIFIS-Home system shall anticipate strange, dangerous, or critical situations and raise an alert.	C	OK	
US-03	The SIFIS-Home system shall be autonomous and learn based on the users' habits.	C	OK	
US-04	The SIFIS-Home system shall consider special cases in its	O	OK	

	design, such as colour blindness.			
US-05	The SIFIS-Home system shall preserve consistency among all devices, related database and constraints.	C	OK	
US-06	The SIFIS-Home hardware components should be easy to use for the elderly and users with no engineering background.	O	OK	
US-07	The SIFIS-Home system shall have an explorable interface.	S	OK	
US-08	Proper and easy hardware installation should be considered.	S	Refine	If this is something beyond the simple HW placement and switching on, e.g. it covers logical bootstrapping and registration, it does affect safe assumptions for security solutions on WP3, and it must definitely be Critical.
US-09	The identification through biometrics should be performed by the system in a radius of at least 10 metres from the device.	S	OK	
US-10	An untrained user should be able to recognise an intrusion in the SIFIS-Home system and contact the authorities in less than 1 minute.	C	OK	
US-11	An untrained user should be able to recognise a software intrusion in less than one minute.	C	OK	
US-12	An untrained user should be able to perform the device registration procedure in less than 5 minutes.	S	OK	
US-13	An untrained user should be able to perform the device de-registration procedure in less than 5 minutes.	S	OK	
US-14	An untrained user should be able to perform the configuration of devices in less than 5 minutes.	S	OK	
US-15	An untrained user should be able to perform the installation of an application in less than 5 minutes.	S	OK	
US-16	An untrained user should be able to complete the configuration of policies for groups of users in less than 5 minutes.	S	OK	
US-17	An untrained user should be able	S	OK	

	to complete the configuration of policies for groups of devices in less than 5 minutes.			
US-18	An untrained user should be able to complete the configuration of profiles in less than 5 minutes.	S	OK	
US-19	An untrained user should be able to perform a profile change in less than 30 seconds.	S	OK	
US-20	An untrained user should be able to visualize and interpret the statistics in less than 5 minutes.	S	OK	
DE-01	The identification through biometrics should be performed correctly in more than 95% cases.	C	OK	
DE-02	The start of interaction command should be recognised properly in more than 99% of cases.	C	OK	
DE-03	The commands to execute should be recognised properly in more than 95% of cases.	C	OK	
DE-04	Record of intrusions must be available for six months after the recording.	S	OK	
DE-05	Identity of the intruders must be available for six months after the recording.	S	OK	
DE-06	Core functionalities should be replicated on multiple devices to avoid single points of failure.	C	OK	
DE-07	The registration of a new device should be successful in at least 99% of the cases.	C	OK	
DE-08	The de-registration of a new device should be successful in at least 99% of the cases.	C	OK	
DE-09	The configuration changes should be propagated successfully to the devices in more than 99% of times.	C	OK	
DE-10	The SIFIS-Home system should be able to restore the previous configurations if there is an error in the application of configuration changes.	S	OK	
DE-11	The installation of the selected app should be completed successfully in at least 95% of cases.	C	OK	
DE-12	The application of policies should be completed successfully in at	C	OK	

	least 99% of cases.			
DE-13	The configuration of profiles should be completed successfully in at least 99% of cases.	C	OK	
DE-14	The change of current profile should be completed successfully in at least 99% of cases.	C	OK	
DE-15	The statistics must be shown correctly in at least 99% of cases.	C	OK	
DE-16	Remote log-in for the configurer should be successful in at least 99% cases.	C	OK	
DE-17	The SIFIS-Home system should be able to distribute processing among multiple machines in different places if required.	C	OK	
DE-18	The SIFIS-Home system is required to be fault tolerant, it should continue to operate, even if one or more of the nodes fail.	C	OK	
DE-19	The SIFIS-Home system is required to be scalable dynamically by adding or removing nodes according to demand.	C	OK	

Table 2: List of feedback to the original Non-Functional Requirements for the SIFIS-Home system.

3.3 *Security Requirements Analysis*

The following Table 3 provides a list of feedback and request of amendments to the security requirements defined in Section 6.3 of D1.1.

ID	Req. Description	Priority	Feedback	Comments
SE-01	APIs for the communication with internal devices must be secured.	Critical	OK	
SE-02	APIs for the communication with external devices must be secured.	Critical	OK	
SE-03	Personal data stored must be encrypted.	Critical	OK	
SE-04	The system shall protect and avoid disclosure of sensitive information.	Critical	OK	
SE-05	The SIFIS-Home system shall prevent data alteration or deletion.	Critical	OK	
SE-06	WiFi access should be protected against known WiFi security attacks.	Critical	OK	
SE-07	Biometrics must be stored safely in the SIFIS-Home database.	Critical	OK	
SE-08	Log-in information should be stored in a protected database.	Critical	OK	
SE-09	The information about the	Critical	OK	

	registered devices, their characteristics and their configurations should be stored in a protected database.			
SE-10	The information about policies should be stored in a protected database.	Critical	OK	
SE-11	The information about user profiles and configuration aspects should be stored in a protected database.	Critical	OK	
SE-12	Data paths should be identified to allow data tracking and detect data leaving the smart-home perimeter, according to policies.	Critical	Amend	It would be good to expand on "Data path" and give examples? Does it mean "traffic pattern" and "communication flows"? One can detect that "any data" is leaving, but not what exact data, as you are supposed to have (different extents of) end-to-end security in your communication channels. That is, traffic inspection at the level of specific data should not be possible even for the home gateway. As part of the answer, how is this tested?
SE-13	Data confidentiality shall be ensured all the time.	Critical	Amend	That applies to data that do require confidentiality and for which it is possible to provide it (e.g. one often cannot for error messages of a key establishment protocol)
SE-14	The system should not be affected by MITM attacks.	Critical	Refine	Is this intended for any possible pair of communicating entities in the system? "Being affected" strongly depends on the exact building blocks composing the system and its protocols. Does it cover only internal entities, or also external entities?

				Is this intended for any possible interaction at any layer? At least at this level of abstraction, it is not testable. It can become testable, if one describes a concrete MITM attack mounted against a particular protocol.
SE-15	Software and apps shall only be installed with authorisation of the smart home administrator or resident users.	Critical	Refine	This seems to mean: administrator and resident users are "pre-authorized" to do this, and they can authorize further users. Is that correct?
SE-16	Users must be able to configure and allow the usage of data by the SIFIS-Home framework and third party software.	Critical	Amend	Which type of user can allow to do what to the framework or third party software? Does this apply only to data produced by exactly that user? Is the data owner only the user that produced and uploaded it?
SE-17	Anomalous device behaviours should be identified and signalled in less than 60 seconds.	Critical	Refine	Assuming that the system detects those, whom does it signal them to? To which users?
SE-18	Minimum needed privilege principle must always be enforced.	Critical	Amend	To which point in time does this refer? First case: when policies and permissions are assigned, e.g. by the administrator. Then this is just a good recommendation, and not a requirement for the system. Second case: after policies and permissions are set and ready to be enforced, they are just supposed to be followed without thinking. It may make sense to still think in terms of

				"minimum" at this point, e.g. to build detailed policies at runtime by filling underspecified templates and default indications, thus taking a conservative approach. This in turn requires conservative-oriented patterns to derive concrete policy points.
SE-19	Access to devices functionalities should be protected and controlled.	Critical	Amend	Why not testable?
SE-20	Access to critical functionalities and services of the SIFIS-Home framework shall be protected and controlled.	Critical	Amend	Why not also for non-critical functionalities? Everything is supposed to be protected and accessible only for the intended entities/users. Why not testable?
SE-21	Privacy preferences shall be configurable for data, analytics and functionalities.	Critical	Amend	By whom and to what extent? Is this limited to the owner of some data, or can one have a say on others' data?
SE-22	Analytics shall be able to work with anonymized data when possible.	Critical	OK	
SE-23	The SIFIS-Home architecture shall be resilient to network-based attacks.	Critical	Refine	This is "Not Testable", since one can come up with metrics to assess how good/bad the system is going under certain attack conditions. This should start with the premise "Under the strongest expected adversary, ..."
SE-24	The SIFIS-Home architecture shall be resilient DoS attacks.	Critical	Refine	This is "Not Testable", since one can come up with metrics to assess how good/bad the system is going under certain attack conditions. This should start with the premise "Under the strongest expected adversary, ..."

SE-25	The SIFIS-Home architecture shall be resilient to sybil attacks.	Critical	Refine	This is "Not Testable", since one can come up with metrics to assess how good/bad the system is going under certain attack conditions. This should start with the premise "Under the strongest expected adversary, ..."
SE-26	The SIFIS-Home architecture shall be resilient to device compromising attacks.	Critical	Refine	This is "Not Testable", since one can come up with metrics to assess how good/bad the system is going under certain attack conditions. This should start with the premise "Under the strongest expected adversary, ..."
SE-27	The SIFIS-Home architecture shall be resilient to Internet connection failure.	Critical	Refine	In what respect? Is this about continuing to guarantee minimum services even if offline? If so, this will require to define a set of minimum guaranteed services.
SE-28	The SIFIS-Home architecture shall be resilient to physical device damage or failure.	Critical	Refine	In what respect? Is this about continuing to guarantee particular services even if offline?
SE-29	Devices must have unique identifiers.	Critical	Refine	Suggested rephrase: "The SIFIS-Home system shall be able to uniquely identify each device." This is due to the fact that: a device may have multiple identifiers, related to different services and protocols; those identifiers may be reused globally, as long as they are unique in their domain of pertinence (e.g. a security group under a specific responsible Group Manager).

Table 3: List of feedback to the original Security Requirements for the SIFIS-Home system.

4 Additional Requirements

This section defines new network & system security requirements that are requested for WP1 to be added in its next deliverable D1.2 “Final Architecture Requirements Report”.

These requirements have been formulated by taking into account the requirements originally defined in D1.1 “Initial Architecture Requirements Report”, as well as the scope, functionality and goals of the network & system security solutions to be developed in WP3.

The definition of new requirements adheres to the same taxonomy and classification of requirements introduced in Section 6 of D1.1. That is, the new requirements below are separately defined for the different subset “Functional requirements”, “Non-functional requirements” and “Security requirements”. Furthermore, also consistent with D1.1:

- The new functional requirements are mapped to the related use cases and non-functional requirements.
- The new non-functional and security requirements are mapped to the related functional requirements.
- The new security requirements are split into “Testable” and “Non-testable” security requirements.

Like for the original requirements defined in D1.1, the new requirements are also grouped into three different categories associated to their priority level, namely Critical (C), Standard (S) and Optional (O).

4.1 *New Functional Requirements*

The following Table 4 provides a list of new functional requirements to be added to the initial set defined in Section 6.1 of deliverable D1.1.

The table is composed of the following columns:

- **ID**: unique identifier assigned to the requirement.
- **Description**: description of the requirement.
- **UC**: identifier(s) of the use case(s) this requirement refers to. For a detailed description of the Use Cases, please refer to their definition in Section 5.2 of deliverable D1.1.
- **Priority**: priority of this requirement, i.e. critical, standard or optional.
- **NFR-ID**: unique identifier of the non-functional requirement(s) this requirement refers to.
- **NFR-Type**: type(s) of the corresponding non-functional requirement(s) under “NFR-ID”.

ID	Description	UC	Priority	NFR-ID	NFR-Type
F-47	Administrators and configurers shall be able to create, configure and delete security groups.	UC5 UC6 UC7 UC12	C	PE-30 PE-31	Performance Performance
F-48	Administrators and configurers shall be able to register security groups and thus make	UC5 UC6	C	PE-30 PE-31	Performance Performance

	them dynamically discoverable.	UC7 UC12			
F-49	There must be a means for Administrators and devices to discover security groups, including their properties, how to join them, as well as their associations with application groups and their resources.	UC5 UC6 UC7 UC12	C	PE-30 PE-31	Performance Performance
F-50	There must be a means for devices to join/leave a security group and retrieve/provide updated key material to communicate in the group	UC5 UC6 UC7 UC12	C	PE-30 PE-31	Performance Performance

Table 4: List of new Functional Requirements for the SIFIS-Home system.

4.2 *New Non-Functional Requirements*

The following Table 5 provides a list of new non-functional requirements to be added to the initial set defined in Section 6.2 of deliverable D1.1.

The table is composed of the following columns:

- **ID**: unique identifier assigned to the requirement.
- **Description**: description of the requirement.
- **FR-ID**: unique identifier of the non-functional requirement(s) this requirement refers to.
- **Priority**: priority of this requirement, i.e. critical, standard or optional.

ID	Description	FR-ID	Priority
PE-28	The used solutions for communication and system security shall be as much as possible lightweight to enforce in terms of performance, and especially feasible also for resource-constrained devices.	All	C
PE-29	The performance impact due to communication and system security shall not result in unacceptable impact on the user experience.	All	C
PE-30	The network infrastructure shall provide means also for one-to-many message delivery, e.g. over IP multicast.	F-47 F-48 F-49 F-50	C
PE-31	It must be possible to have multiple security groups simultaneously active in the system.	F-47 F-48 F-49 F-50	C
PE-32	When relevant, support shall be ensured for possible communication intermediaries performing, e.g., message forwarding and/or (transport-) protocol translation. This applies also in secure scenarios and also in (secure) group communication scenarios.	All	C
PE-33	When relevant, it shall be possible to enable one-to-many response messages, sent at once to multiple requesters. This applies also to secure communication scenarios, and also in presence of communication intermediaries.	All	C
PE-34	When relevant and limited to read-only operations, it shall be possible	All	C

	to enable cacheability of response messages at communication intermediaries, also when protected end-to-end.		
PE-35	Devices should, if available, utilize low-power modes of operation to further mitigate the performance impact of ongoing (D)DoS attacks.	All	S
PE-36	There should be a means to enable an optimized, combined establishment of a cryptographic secret with a first message protected with key material derived from that secret.	All	S
AV-03	Support should be ensured for devices to dynamically react to (D)DoS attacks, by gradually adapting their availability. This includes relying on communication intermediaries for traffic offloading during intense (D)DoS attacks.	All	S
AV-04	Devices under (D)DoS attacks should be able to continue providing a (best-effort) service to legitimate requests, i.e. by displaying a graceful degradation of quality of service.	All	S

Table 5: List of new Non-Functional Requirements for the SIFIS-Home system.

4.3 *New Security Requirements*

The following Table 6 provides a list of new security requirements to be added to the initial set defined in Section 6.3 of deliverable D1.1.

The table is composed of the following columns:

- **ID**: unique identifier assigned to the requirement.
- **Description**: description of the requirement.
- **FR-ID**: unique identifier of the non-functional requirement(s) this requirement refers to.
- **Testable**: whether this requirement is testable (yes) or non-testable (no).
- **Priority**: priority of this requirement, i.e. critical, standard or optional.

ID	Description	FR-ID	Testable	Priority
SE-30	Unless thoroughly assessed and acceptable for the specific application, communications in the networked environment shall be secured, by ensuring confidentiality/integrity/authenticity of messages, as well as protecting from replay protection.	General	T	C
SE-31	It shall be possible and feasible to provide devices with the necessary key material to establish their security associations and to communicate securely, with preference for automatic procedures.	General	T	C
SE-32	It shall be possible to achieve end-to-end protection of CoAP messages at the application layer, by ensuring confidentiality/integrity/authenticity of messages, as well as protecting from replay protection. This applies also in case communication intermediaries are used, as well as for both one-to-one and one-to-many (group) communication.	General	T	C
SE-33	Cryptographic binding between a protected request message and one or many corresponding protected	General	T	C

	response(s) shall be ensured.			
SE-34	Source authentication of protected messages shall be ensured, also in a group communication setup where one-to-many messages are exchanged.	General	T	C
SE-35	Cryptoagility shall be ensured, as a way to allow a seamless possible switch to different existing algorithms as well as a seamless possible migration to future algorithms.	General	T	C
SE-36	Operations related to the creation, configuration, deletion, registration and discovery of security groups shall be secured and shall be allowed only to authorized entities.	F-23 F-25 F-26 F-30 F-31 F-32 F-33 F-34 F-35 F-47 F-48 F-49	T	C
SE-37	When relevant, it shall be ensured that a possible communication intermediary can securely identify its adjacent communication hops.	General	T	C
SE-38	It shall be ensured that possible secure cacheable response messages do not break security properties that are critical for the application and specific communication exchanges.	General	T	C
SE-39	Devices should be able to detect ongoing (D)DoS attacks based on intensity and distribution of invalid traffic.	General	NT	S
SE-40	The system shall provide a means to enforce flexible, fine-grained and reactive authorized access control for devices to access remote resources at other devices.	General	T	C
SE-41	It shall be possible to establish security material to use for end-to-end secure (group) communication in an authorized way, achieving confirmation of the established material.	General	T	C
SE-42	The system shall provide a means for enabling devices to get agile and possibly automatic notification, in order to signal pertaining access credentials that have been revoked while still unexpired.	General	T	C
SE-43	There shall be means for two devices to securely establish a new cryptographic secret with perfect forward secrecy, while also achieving mutual authentication and confirmation of the established material.	General	T	C
SE-44	There shall be an authorization-based means to securely join/leave a security group and retrieve/provide updated key material to communicate in the group.	F-23 F-25 F-26 F-30	T	C

		F-31 F-32 F-33 F-34 F-35 F-50		
SE-45	There shall be a means to securely renew the key material in a security group, both periodically and in case the application requires backward/forward security.	F-19 F-23 F-25 F-26 F-50	T	C
SE-46	When limits on usage of cryptographic material for encryption and decryption are exceeded, devices owning that key material shall stop using it and specific actions shall be taken to acquire new material before possibly resuming communication. The just invalidated key material may be temporarily retained and used only for processing incoming messages for a limited, pre-configured amount of time.	General	T	C
SE-47	There shall be a means for two devices to securely update their pairwise key material.	General	T	C

Table 6: List of new Security Requirements for the SIFIS-Home system.

5 Mapping of Requirements to Use Cases

The following Table 7 summarizes the mapping of the new functional requirements defined in Section 5 to the Use Cases that were used to generate them. For a detailed description of the Use Cases, please refer to their definition in Section 5.2 of deliverable D1.1.

	UC-1	UC-2	UC-3	UC-4	UC-5	UC-6	UC-7	UC-8	UC-9	UC-10	UC-11	UC-12	UC-13	UC-14
F-47					x	x	x					x		
F-48					x	x	x					x		
F-49					x	x	x					x		
F-50					x	x	x					x		

Table 7: Mapping of new Functional Requirements to Use Cases.

6 Conclusions

This document is the first deliverable from WP3, and has provided WP1 with feedback as well as requests for amendment and additions to the initial set of requirements defined in deliverable D1.1 "Initial Architecture Requirements Report".

Feedback, requests for updates and new requirements to add have been especially brought up in the light of the planned network & system security solutions under development in WP3, of which a high-level overview has been already provided in this document. In particular, the same taxonomy and classification of requirements introduced in deliverable D1.1 has also been used in this document.

Together with the analogous feedback and input from WP4 provided in the deliverable D4.1 accompanying the present document, this contribution will be considered by WP1 to produce its next deliverable D1.2 "Final Architecture Requirements Report". Following on this joint effort, the security solutions developed in WP3 will keep taking into account the guidelines from WP1, and especially the

final set of requirements from its deliverable D1.2.

7 References

[Bormann, 2020] C. Bormann and P. Hoffman, “Concise Binary Object Representation (CBOR)”, RFC 8949 (Internet Standard), Internet Engineering Task Force, RFC Editor, December 2020.

[Günther, 2021] F. Günther, M. Thomson and C.A. Wood, "Usage Limits on AEAD Algorithms", Internet Draft draft-irtf-cfrg-aead-limits-02 (work in progress), IETF Secretariat, February 2021.

[Hartke, 2015] K. Hartke, “Observing Resources in the Constrained Application Protocol (CoAP)”, RFC 7641 (Proposed Standard), RFC Editor, September 2015.

[Park, 2004] J. Park and R. S. Sandhu, “The UCONABC usage control model.” ACM Transactions on Information and System Security, 7(1): 128-174, February 2004.

[Rahman, 2014] A. Rahman and E. Dijk, “Group Communication for the Constrained Application Protocol (CoAP)”, RFC 7390 (Experimental), Internet Engineering Task Force, RFC Editor, October 2014.

[Rescorla, 2021] E. Rescorla, H. Tschofenig and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", Internet Draft draft-ietf-tls-dtls13-41 (work in progress), IETF Secretariat, February 2021.

[Schaad, 2017] J. Schaad, “CBOR Object Signing and Encryption (COSE)”, RFC 8152 (Proposed Standard), RFC Editor, July 2017.

[Seitz, 2021] L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman and H. Tschofenig, “Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)”, Internet Draft draft-ietf-ace-oauth-authz-38 (work in progress), IETF Secretariat, March 2021.

[Selander, 2019] G. Selander, J. Mattsson, F. Palombini and L. Seitz, “Object Security for Constrained RESTful Environments (OSCORE)”, RFC8613 (Proposed Standard), Internet Engineering Task Force, RFC Editor, July 2019.

[Shelby, 2014] Z. Shelby, K. Hartke and C. Bormann, “The Constrained Application Protocol (CoAP)”, RFC 7252 (Proposed Standard), Internet Engineering Task Force, RFC Editor, June 2014.

Glossary

Acronym	Definition
ACE	Authentication and Authorization for Constrained Environments
AS	Authorization Server
CBOR	Concise Binary Object Representation
CoAP	Constrained Application Protocol
CoRE	Constrained RESTful Environments
COSE	CBOR Object Signing and Encryption
DHT	Distributed Hash Table
DoS	Denial of Service
DDoS	Distributed Denial of Service
DTLS	Datagram Transport Layer Security
FR	Functional Requirement
GM	Group Manager
HTTP	Hyper Text Transfer Protocol
HW	Hardware
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
JSON	Javascript Object Notation
LAKE	Lightweight Authenticated Key Establishment
LwM2M	Lightweight Machine-to-Machine
M2M	Machine-to-Machine (communications)
MiTM	Man in The Middle
NFR	Non-Functional Requirement
OMA	Open Mobile Alliance
OS	Operating System
OSCORE	Object Security for Constrained RESTful Environments
P2P	Peer to Peer
PSK	Pre-Share Key
REST	Representational State Transfer
RD	Resource Directory
RPK	Raw Public Key
RS	Resource Server
SIFIS-HOME	Secure Interoperable Full Stack Internet of Things for Smart Home
SW	Software
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UC	Use Case
UDP	User Datagram Protocol
US	User Story
WG	Working Group
WP	Work Package