

Trusted Federated Identity Management in services and SDN

Carolina Gonçalves, Bruno Sousa, Nuno Antunes
University of Coimbra, CISUC, DEI – Coimbra, Portugal
mcarolina@dei.uc.pt, bmsousa@dei.uc.pt, nmsa@dei.uc.pt

Abstract—Federated Identity Management (FIM) is a topic that has attracted the research community and enterprises to build different solutions, suited to specific needs. A few examples include: the Security Assertion Markup Language (SAML), the Open Authentication (OAuth 2.0), and OpenID Connect (OIDC) as a solution to support authentication and identification of users.

Identity management solutions include mechanisms and architectures to exchange identity information between organisations that are federated for authentication purposes. This has the advantage inherent to the Single Sign On (SSO) process, where an user does not need to replicate login information over multiple systems.

The evolution of 5G towards 6G will enable multiple access contexts, associated with the support of heterogeneous networks, with the support edge and cloud computing models. In such context, current FIM solutions mainly focus identity management and do not consider the possible context environments where services require user information for authentication and authorization purposes.

Index Terms—Federated Identity Management; OpenID Connect; SDN; SAML; OpenDayLight; Keycloak

I. INTRODUCTION

This document provides the information for an ISCC'22 tutorial proposal.

The tutorial aims to provide insights on how a user can differentiate the access to data based on the trust level, that can rely on context information, for instance if accessing in a public WiFi network.

II. OBJETIVES OF THE TUTORIAL

The objectives of the tutorial are:

- 1) Provide insights regarding current solutions for Federated Identity Management (SAML, OpenIDConnect, Oauth).
- 2) Present a comprehensive description of mechanisms to enable trust for access control considering context information of users.
- 3) Hands-on on KeyCloak and OpenDayLight SDN controller to accommodate policies for access control.

III. TUTORIAL PRESENTERS

The Name, affiliation, and short biography of each tutorial presenter are as presented bellow.

Carolina Gonçalves is an Msc. Student in Communications, Services and Infrastructures at the Department of Informatics Engineering. She is also working as a research student for the Center for Informatics and Systems of the

University of Coimbra (CISUC). Her research interests are network security, data privacy and secure communications.

Bruno Sousa is a professor at the Department of Informatics Engineering at the University of Coimbra, researcher at CISUC. He has obtained his PhD in 2014 at the University of Coimbra and has around 50 scientific publications in journals and international conferences. He has participated in several European and national research projects, such as MobiTrust, SALUS, Mobile Cloud Networking and FI-WARE. He is currently involved in ARCADIAN-IoT, AIDA, SNOB-5G, ELEGANT and Smart5Grid projects. His research interests include resilience mechanisms in networks and applications/services, and intrusion detection and prevention in 5G networks and for reputation and attestation mechanisms for Internet of Things (IoT).

Nuno Antunes is an Assistant Professor at the University of Coimbra, where he received his PhD in Information Science and Technology in 2014. He is a researcher with the Centre for Informatics and Systems of the University of Coimbra (CISUC) since 2008, working in Security and Dependability topics. His expertise includes testing techniques, fault injection, vulnerability injection and benchmarking, which are applied to the assessment of virtualized environments, intrusion detection systems, web services, web and mobile applications, and data management systems. Nuno was PC co-Chair of ISSRE 2020, and he has authored or co-authored multiple book chapters and papers in refereed journals and conferences in dependability, reliability, security and services. He is the PI of the METRICS project (funded by FCT) and has contributed to many national and international research projects, namely H2020: PoSeID-on, ATMOSPHERE, EUBra-BIGSEA and EUBrasilCloudFORUM; and FP7: DEVASSES, CECRIS and Critical-STEP.

IV. DESCRIPTION OF TOPICS

A description of the topics that the tutorial will address, emphasizing their motivations and timeliness are provided bellow

The topics covered with the tutorial are the following:

- 1) **Secure computing and secure architectures** (as per the ISCC call for tutorials). The motivation of the tutorial is aligned with the need for mechanisms to enhance the authentication and access control processes, considering federated Identity Management. User needs to be provided with mechanisms that promote a higher

control of user data, for instance, how it can be accessed/processed by third party services, but also how it can be processed according the context where the access to data is requested (if trusted or not). Services in secure architectures can be orchestrated using different paradigms, as Virtual Network Functions (VNFs), as Container Network Functions (CNFs), through the support of SDN. In this sense, the access control to SDN controllers needs to consider the robust authentication, accounting and authorization (AAA) mechanisms.

- 2) **6G and wireless Communication technologies** (as per the ISCC call for tutorials). The motivation in this topic is aligned with the current evolution of 5G, for URLLC to enhance the deployment of services with stringent latency requirements and high reliability. In addition, 5G is already promoting the virtualization of services, in the VNF paradigm, with a tendency to move to CNF deployment paradigm, several projects propose solutions for Open RAN based on container technologies, as the example of SD-RAN from ONF. This tutorial aims to consolidate the know-how on how identify of users can be managed in a scalable fashion.
- 3) **Smart cities** (as per the ISCC call for tutorials). The motivation in this topic in aligned with services, which are accessed by devices owned by users, and which can have different trust levels. For instance, a professional device (e.g., laptop) can have associated stringent security policies, which leads the user to trust more in this device, as opposed to a mobile device (e.g. Android based) that an user uses to connect to public networks.
- 4) **Software Defined Networks and Network Functions (NF)**. The motivation in this topic is aligned the need to have enhanced AAA mechanisms in critical resources like SDN controllers, managing networks with service's network functions

V. PROJECTED AUDIENCE AND EXPECTED BACKGROUND

The audience of the tutorial is for researchers, students, professionals working on network management topics, dealing with authentication and access control in networks.

Tutorial attendees should have background knowledge on networking concepts such as routing and Internet applications and services. In addition, some knowledge on Federated Identity Management solutions like OAuth, OpenID connect is also desirable.

VI. TUTORIAL OUTLINE

An outline of the tutorial content, including its tentative schedule and the potential presenters for the different parts of the tutorial is as follows:

- 1) Introduction
 - a) Objectives
 - b) Motivation for Federated Identity Management
 - c) Motivation for Software Defined Networks
- 2) Services in Smart Cities
 - a) Modelling services

- b) Advances in communication technologies (5G)
- c) Services and Identity management issues

- 3) Federated Identity Management (FIM)
 - a) Standardization in FIM
 - b) SAML
 - c) OpenID Connect & OAuth
 - d) Solutions for Identify Management & AAA (Key-Cloak)
 - e) Issues in Federated Identity Management solutions
- 4) Trust in Services and SDN
 - a) Modelling trust
 - b) SDN and approaches for AAA
 - c) Secure transport solutions
- 5) Case Studies
 - a) Smart Cities use cases (OREOS and SNOB5G)
 - b) Identity management and AAA (ARCADIAN-IoT and AIDA)
 - c) Hands on practical use case (with OpenDayLight and KeyCloak)
- 6) Discussion

The program will be delivered by three speakers: **Carolina Gonçalves [CG]**, **Bruno Sousa (BS)**, and **Nuno Antunes (NA)**. The description of the planned program is as follows:

1) Introduction (15 minutes)

This module aims at motivating the attendees to the topics addressed in the tutorial.

- a) Objectives [NA]
This module provides information regarding the goals of the tutorial
- b) Motivation for Federated Identity Management [BS]
This module provides information regarding the motivation for Federated Identity Management in 2 main scenarios, with demanding requirements. This module also presents examples on how Federated Identity Management can enhance the security of services in Smart Cities.
- c) Motivation for Software Defined Networks [BS]
This module provides information regarding the motivation for SDN in 2 main scenarios, with demanding requirements. This module also presents examples on how SDN can enhance the management of services in Smart Cities and next generation networks.

2) Services in Smart Cities (30 minutes)

This topic aims to provide information regarding the complexity of services, in particular when they involve, security of data and robust authentication and authorization approaches for the different services.

- a) Modelling services [NA]
This module details aspects related with the requirements of critical services, and how reliability, availability, security aspects can be modelled. For instance, reliability is modelled in Service Level

Agreement (SLA) perspective, such as 99.99% availability, also includes information regarding the protection model of Service Function (e.g. fully redundant, or in a primary-backup model). Aspects related with the modelling and architecting services and identifying critical functionalities are discussed in this sub-topic.

- b) Advances in communication technologies (5G) [BS]
The advances in communication technologies like Ultra Reliable low latency communications (URLLC) in 5G, Direct Mode, Mission Critical Push to Talk (MCPTT) are discussed in this module. The information covered in this module focus mainly, safety services, with communications with high requirements of reliability and low latency. This module also conveys information regarding the support of heterogeneous technologies in 5G and beyond networks (mmWave, WiFi).
- c) Services and Identity management issues [BS]
The issues in managing efficiently the authentication and access control in services is introduced in this module. This module will introduce issues related with the identity management of users and devices in services of SmartCities.

3) Federated Identity Management (45 minutes)

This topic aims to introduce FIM solutions currently used.

- a) Standardization in FIM [BS]
This module aims to present the current work on foundations like OpenID, OASIS regarding the specifications of solutions for authentication, authorization in federated scenarios.
- b) SAML [BS]
This module aims to introduce SAML, promoted by OASIS and its support for the eXtensible Access Control Markup Language (XACML) to handle user identities in federated environments.
- c) OpenID Connect & OAuth [BS]
This module aims to introduce OAuth standardized by IETF, OpenID Connect promoted by OpenID foundation to handle user identities in federated environments. This module also covers current enhancements, regarding the support of OpenID and Verifiable Credentials support.
- d) Solutions for Identity Management & AAA (KeyCloak) [BS]
This module aims to introduce the KeyCloak as a solution to manage the identity of users and to perform authentication of users/devices and to perform access control.
- e) Issues in Federated Identity Management solutions [BS]
This module aims to introduce the limitations in FIM solutions and possible research directions to overcome the identified limitations.

4) Trust in Services and SDN (30 minutes)

This topic aims to describe the approaches to enable trust in Services and SDN.

- a) Modelling trust [NA]
This module includes information regarding the modelling of trust in services, considering the interactions between users and services, the context where such interactions occur. For instance, which devices are employed, and the underlying communication networks that provide access to the services.
- b) SDN and approaches for AAA [BS]
This module provides information on how authentication can be performed in service functions and SDN controllers, using federated mechanisms enabled by OpenID Connect. The authentication aspects, supported by OAuth 2 are also considered here, and their interconnection with Software Defined Networks (SDN).
- c) Secure transport solutions [BS]
This module provides information regarding the transport protocols, like HTTPS which provide support to OpenID Connect approaches. The evolution of HTTPS, including HTTP/3 based on QUIC (UDP-based transport protocol) is introduced here.

5) Case Studies (45 minutes)

This topic describes case studies of projects where the author and presenter of this tutorial is leading research activities.

- a) Smart Cities use cases (OREOS and SNOB5G) [BS]
These projects aim to enable an orchestration platform for services in smart cities using diverse technologies like 5G, mmWave. These projects aim to enable orchestration exploits multihoming aspects (multiple and heterogeneous connections to the core network), and considering the restrictions services involved with the safety of people (pedestrians crossing streets).
- b) Identity management and AAA (ARCADIAN-IoT and AIDA) [CG]
These projects tackle authentication mechanisms, using different approaches, biometrics and OpenID connect, to security in communications. The project ARCADIAN-IoT, also considers the heterogeneity of devices and the need for attestation mechanisms to build trust and reputation of diverse entities (services, nodes, persons).
- c) Hands on practical use case (with OpenDayLight and KeyCloak) [CG]
This module aims to introduce the attendees of the workshop in a simple scenario where users can configure a set of policies to specify the access control regarding resources in topologies managed by the OpenDayLight controller. The attendees

will also configure the authentication process in OpenDayLight to support OpenID Connect.

6) Discussion (15 minutes) [all]

This topic briefly summarizes the topics previously discussed in the tutorial and provides guidelines for the next steps towards the implementation of Federated Identity Management solutions in Smart Cities.

VII. VIRTUAL PRESENTATION

Yes, there is the possibility of and suitability for a virtual presentation of the tutorial

VIII. PAST/RELEVANT EXPERIENCE OF THE SPEAKER(S)

Authors have delivered a tutorial in ISCC'21, entitled "Trusted Service Function Chaining for Mission Critical Services", more information available at: tutorial2