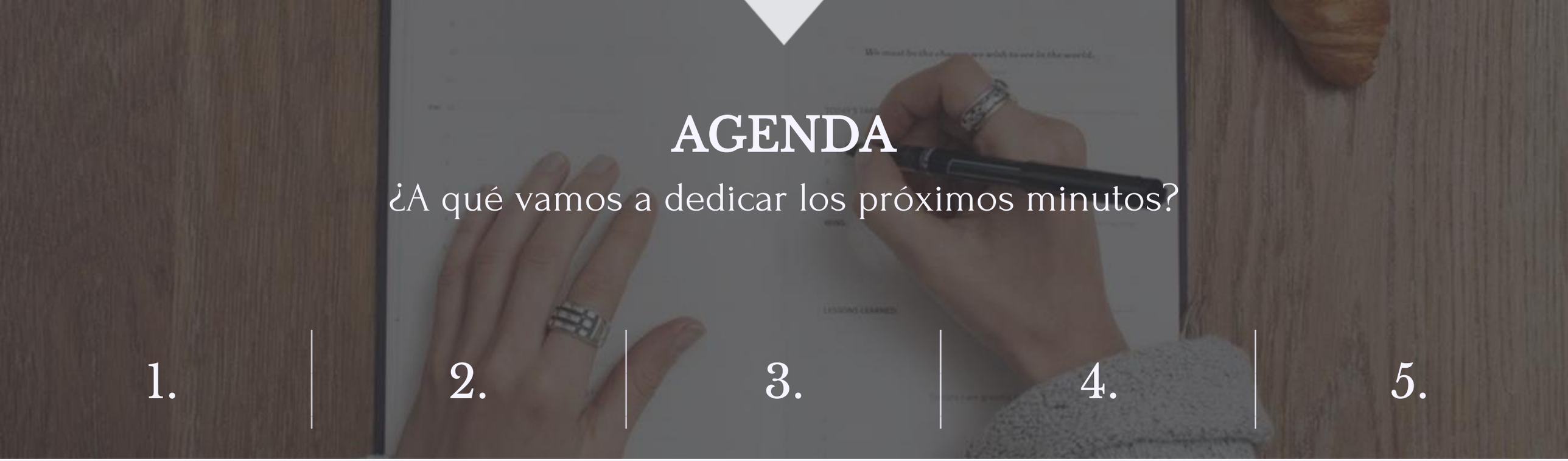
Nuevos (y viejos) enfoques para la gestión de identidades y accesos

MARTA BELTRÁN
marta.beltran@urjc.es | @experiencia_T



AGENDA

¿A qué vamos a dedicar los próximos minutos?

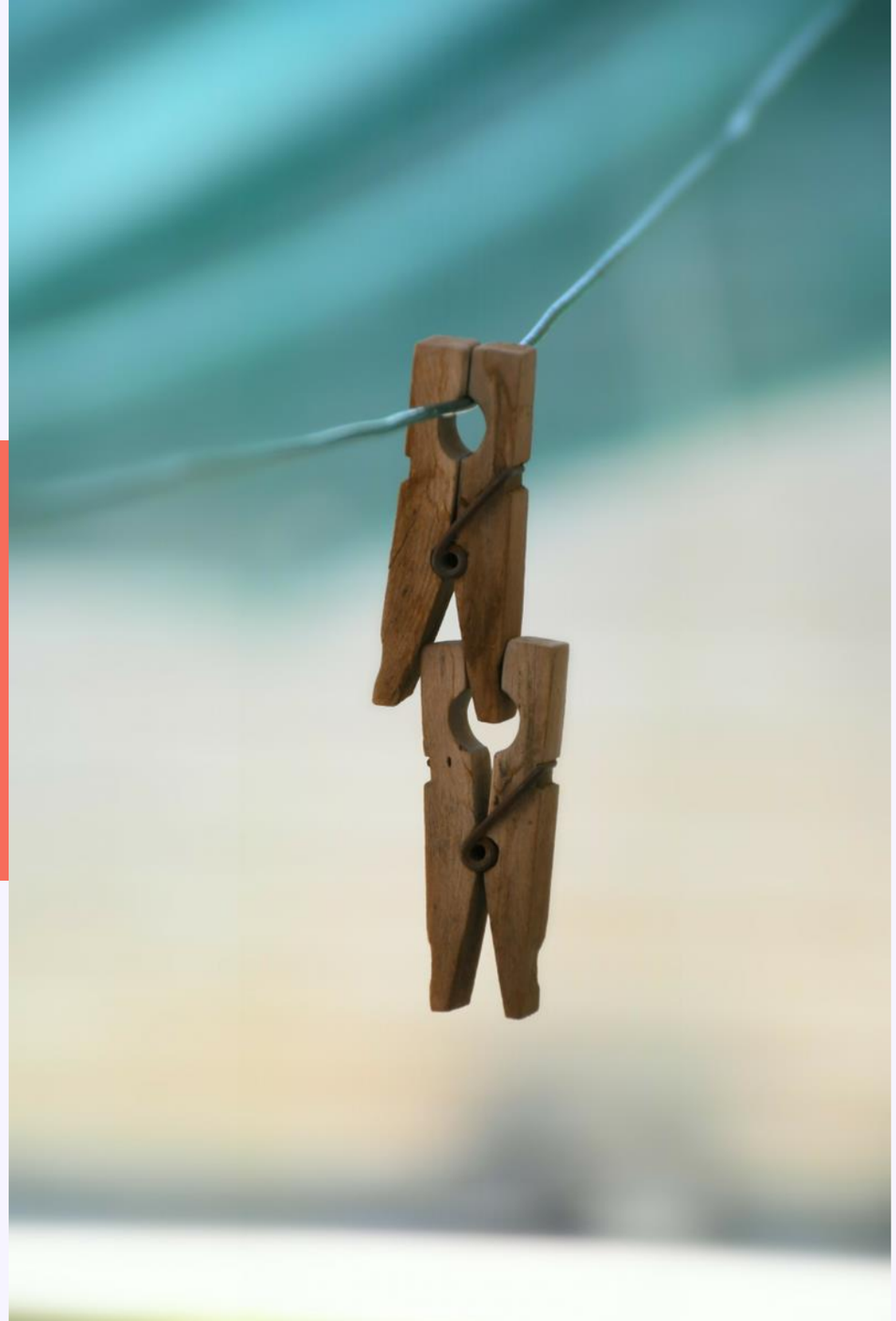
1.	2.	3.	4.	5.
Introducción	**Los proveedores de identidad**	**Las amenazas**	**Los retos**	**Conclusiones**

1 Introducción

Autenticación

Autorización

Auditoría



AAA

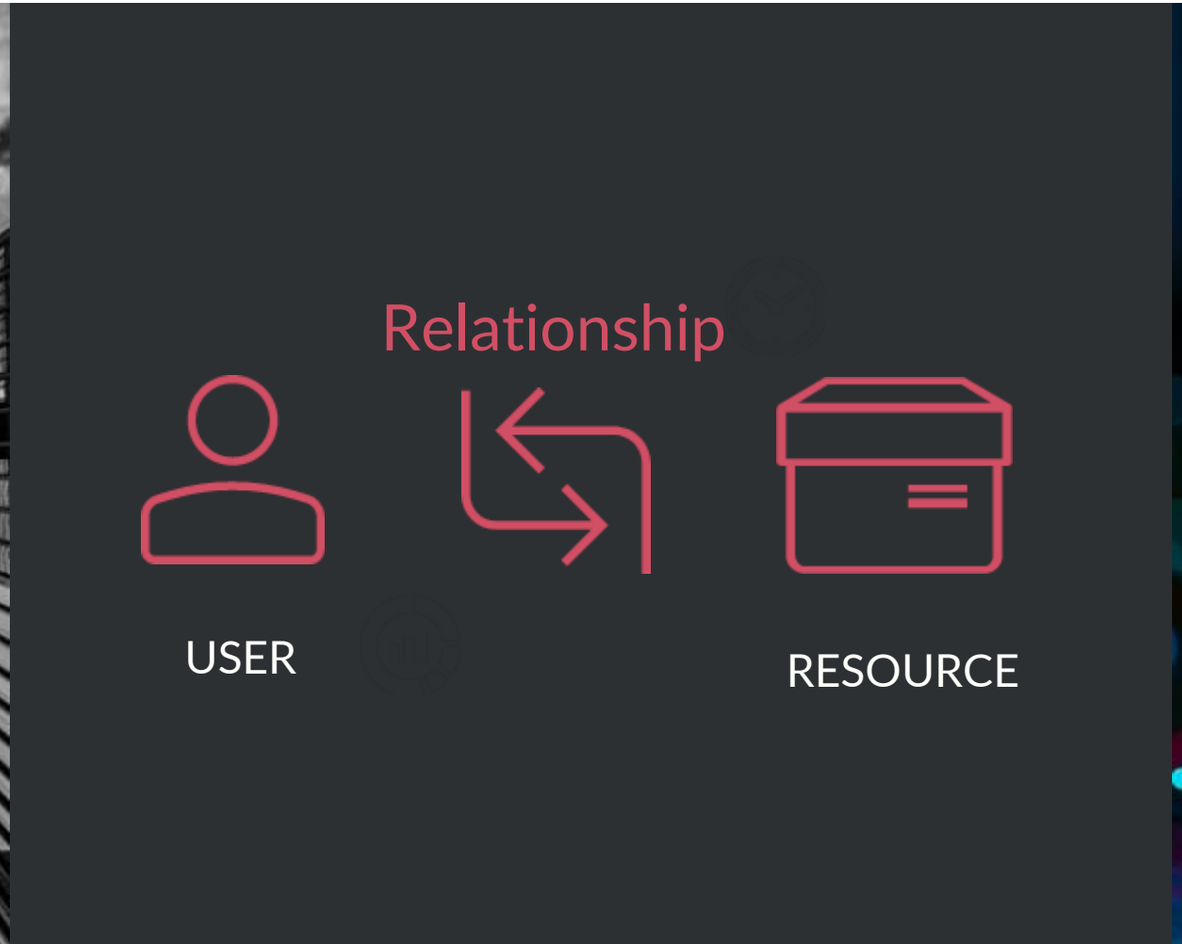
Mundo físico,
mundo virtual

¿QUIÉN SERÍA LA ENTIDAD ENCARGADA DE RESOLVER EL PROBLEMA AAA EN INTERNET?

¿CON QUÉ INFORMACIÓN ACERCA DE LOS USUARIOS?

En el nuevo contexto todo gira alrededor de las "relaciones"

Identity and Access Management: IAAA



IDENTIDAD DIGITAL

COBRA IMPORTANCIA HASTA EL PUNTO DE CONSIDERARSE "THE NEW MONEY"

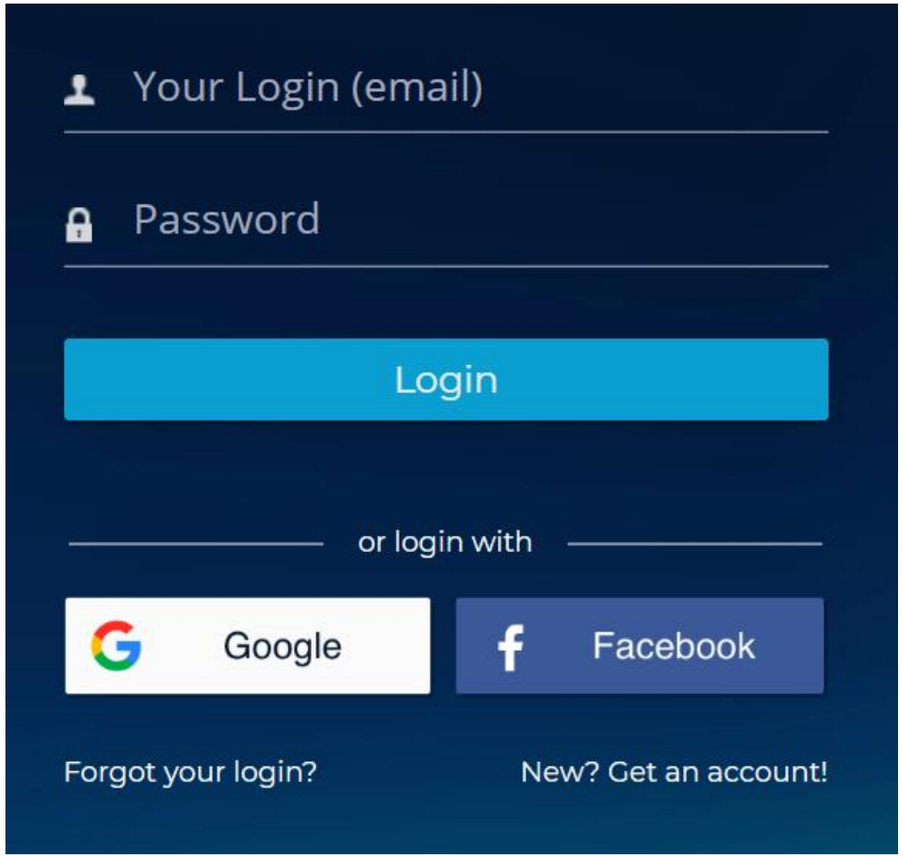
CONJUNTO DE ATRIBUTOS

SUELE INCLUIR PERSONALLY IDENTIFIABLE INFORMATION (PII) PERO NO SIEMPRE ES ASÍ

DEBE ASOCIARSE A UN IDENTIFICADOR Y A UNO O VARIOS AUTENTICADORES

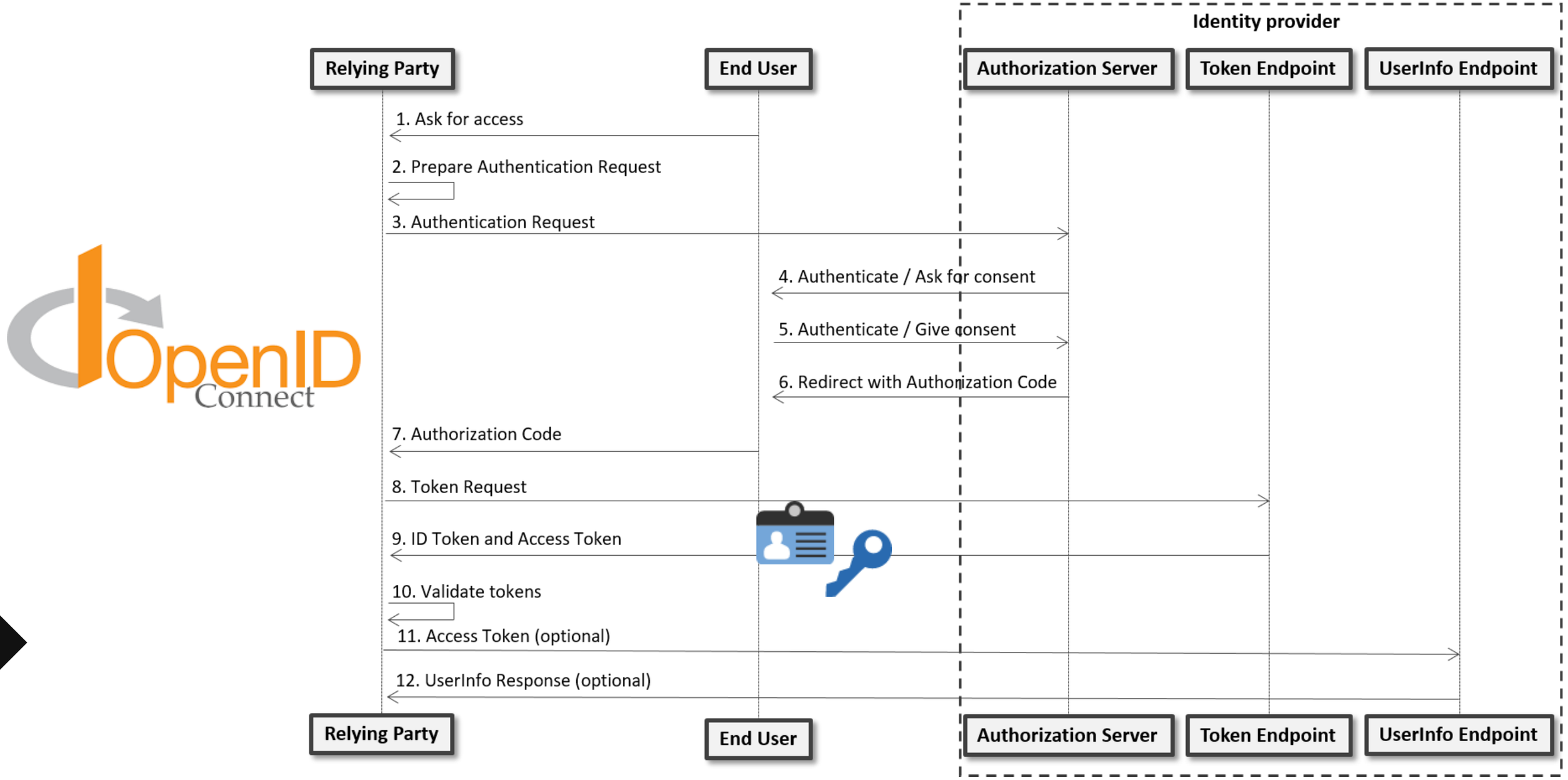
NO HAY ACUERDO EN UNA DEFINICIÓN ESTÁNDAR

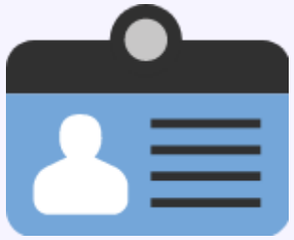
2 Los proveedores de identidad



Distribuida vs Centralizada vs Federada

Authorization Code Flow





```
{
“iss”:         “https://server.ejemplo.com”,
“sub”:         “24400320”,
“aud”:         “s6BhdRkqt3”,
“nonce”:       “n-0S6_WzA2Mj”,
“exp”:         1311281970,
“iat”:         1311280970,
“auth_time”:   1311280969,
“acr”:         “urn:mace:incommon:iap:silver”
}
```

ID token

JSON web token

El ID token es el que representa la identidad del usuario

Sólo incorpora unos sencillos campos estándar: cabecera + payload

Debe ir firmado

Es muy importante que se valide correctamente

AUTENTICADORES

Se pueden usar uno o más

Algo que sólo el usuario conoce

PIN, contraseña

Algo que sólo el usuario posee

Llave, token, smart card

Algo que sólo el usuario es/hace

Huella, cara, iris, gesto, patrón

Mobile Connect

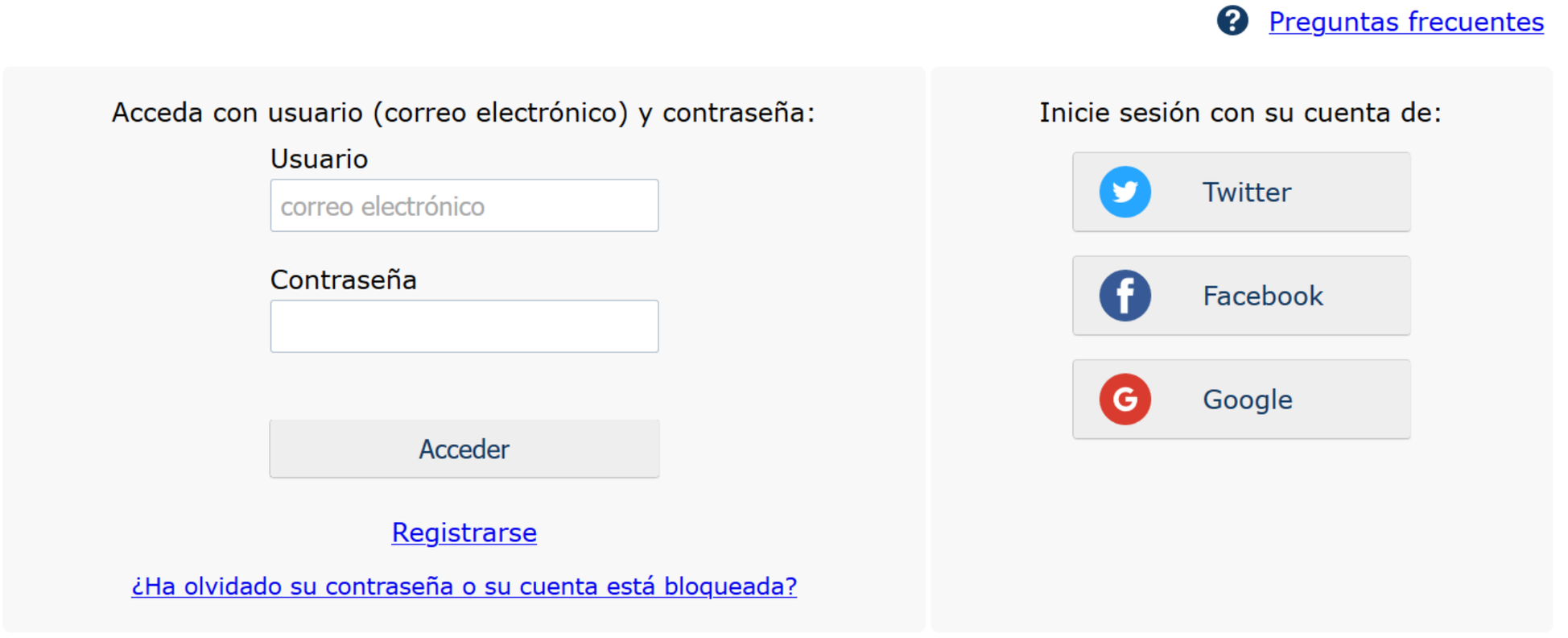
Las operadoras de telecomunicaciones también quieren ser proveedores de identidad

Nuestro teléfono móvil puede ser una herramienta muy potente para autenticarnos

La especificación propuesta por la GSMA se basa en OpenID Connect

¿Y cuando se trata de la relación con las administraciones públicas?

Ejemplo: www.boe.es



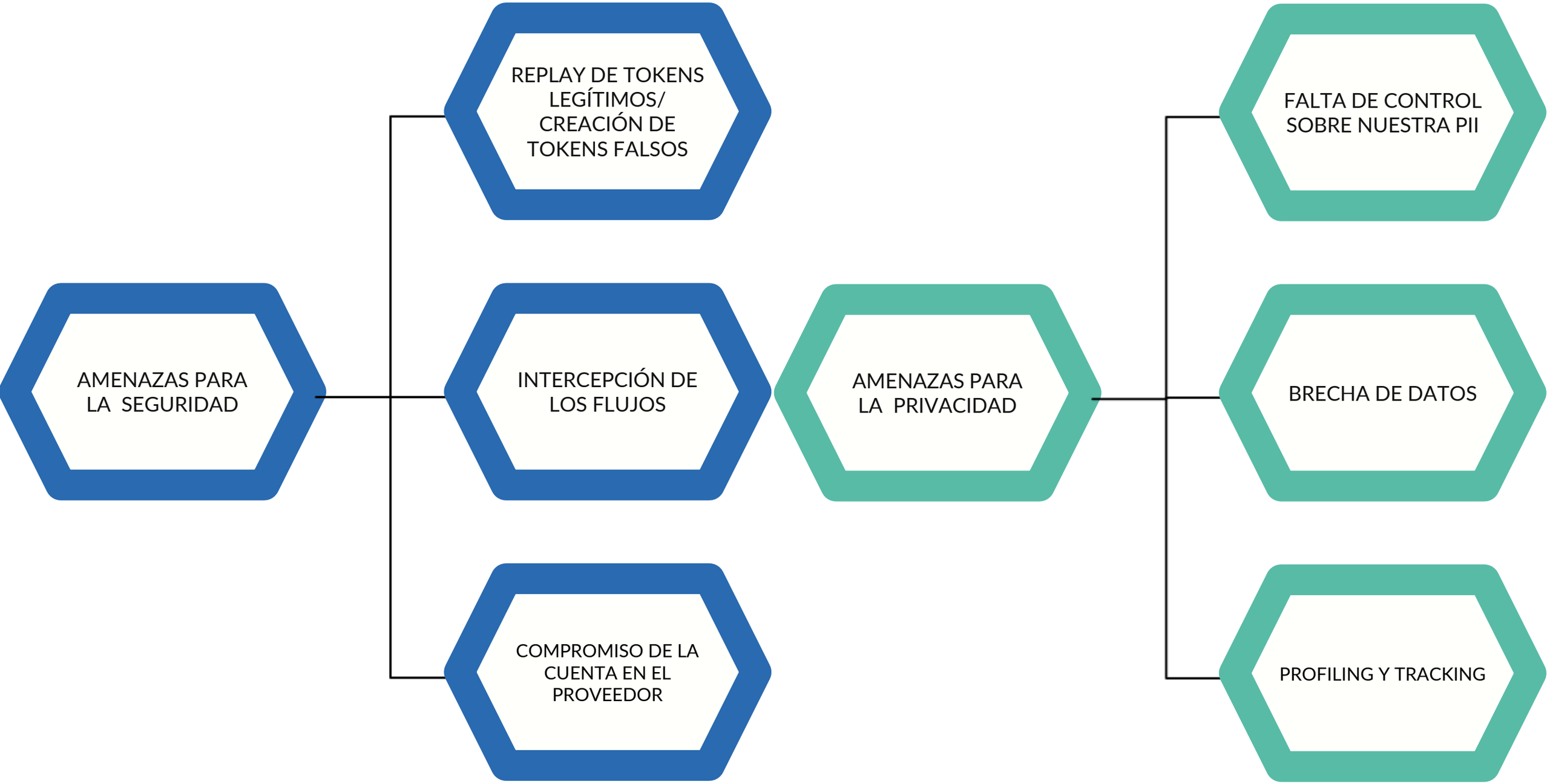
sweden connect

France Connect

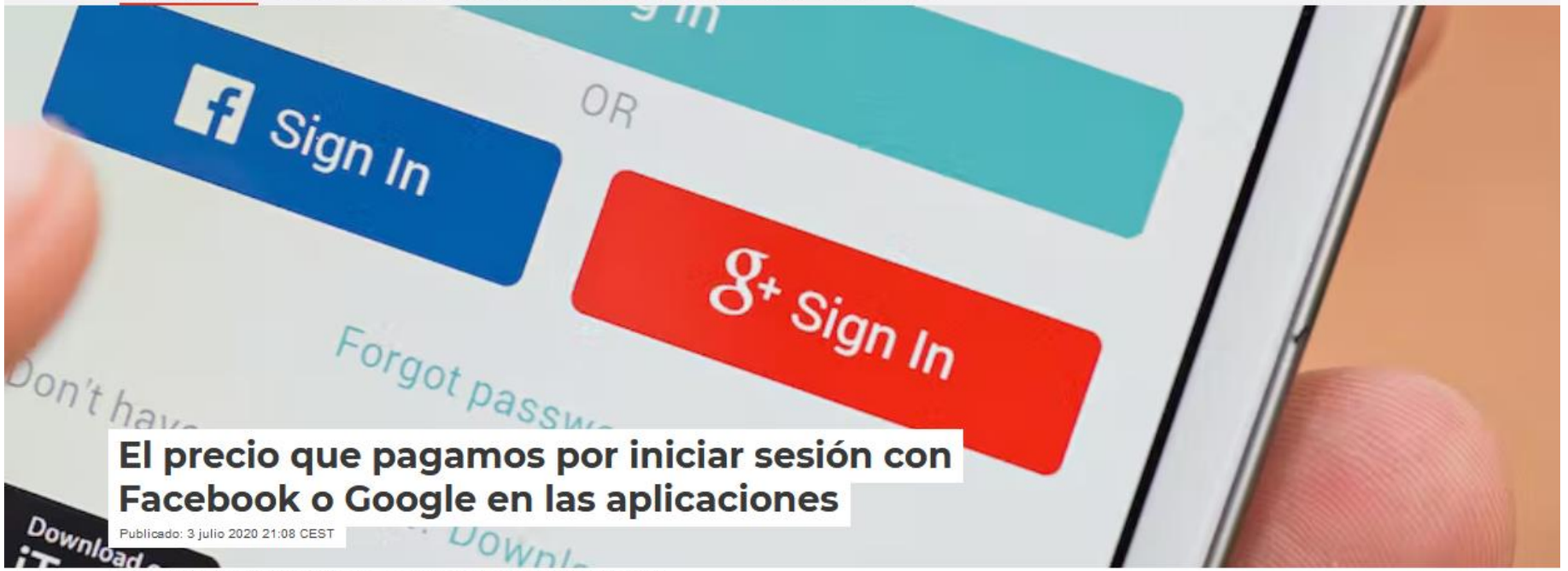
eIDAS y eIDAS2

3

Las amenazas


AMENAZAS PARA LA SEGURIDAD
REPLAY DE TOKENS LEGÍTIMOS/ CREACIÓN DE TOKENS FALSOS
INTERCEPCIÓN DE LOS FLUJOS
COMPROMISO DE LA CUENTA EN EL PROVEEDOR
AMENAZAS PARA LA PRIVACIDAD
FALTA DE CONTROL SOBRE NUESTRA PII
BRECHA DE DATOS
PROFILING Y TRACKING

THE CONVERSATION
Rigor académico, oficio periodístico



El precio que pagamos por iniciar sesión con Facebook o Google en las aplicaciones

Publicado: 3 julio 2020 21:08 CEST

Muchas aplicaciones ofrecen la posibilidad de iniciar sesión con una cuenta de Google o Facebook. Shutterstock/Roman Pyshchyk

Correo
Twitter 33
Facebook 664
LinkedIn
Imprimir

¿Cuántas contraseñas utiliza un usuario medio a lo largo del día? ¿50? ¿100? Y se supone que todas ellas tienen que ser diferentes, largas, suficientemente complejas, no estar relacionadas con su vida, etc. Todo esto para que sean seguras y un atacante no las pueda adivinar o reutilizar si las averigua o roba.

Para ahorrarles trabajo, en los últimos años se está trabajando mucho en ofrecer a los usuarios soluciones que les permitan autenticarse (demostrar que son quienes dicen ser) cuando necesitan utilizar un recurso, aplicación o servicio web, normalmente desde su ordenador o móvil.

Identificación a través de Facebook y Google

Una de estas soluciones son los esquemas federados para la gestión de accesos. Se

Autoría

Marta Beltrán
Profesora y coordinadora del Grado en Ingeniería de la Ciberseguridad, Universidad Rey Juan Carlos

Jorge Navas Diaz
Doctorando en Ciberseguridad, Universidad Rey Juan Carlos

Cláusula de Divulgación

Las personas firmantes no son asalariadas, ni consultoras, ni poseen acciones, ni reciben financiación de ninguna compañía u organización que pueda obtener beneficio de este artículo, y han declarado carecer de vínculos relevantes más allá del cargo académico citado anteriormente.

https://theconversation.com/el-precio-que-pagamos-por-iniciar-sesion-con-facebook-o-google-en-las-aplicaciones-141851

COMPUTERS & SECURITY 84 (2019) 1–16

Available online at www.sciencedirect.com

ScienceDirect

Journal homepage: www.elsevier.com/locate/cose

Computers & Security

Understanding and mitigating OpenID Connect threats

*Jorge Navas, Marta Beltrán**

Department of Computing, ETSII, Universidad Rey Juan Carlos, Móstoles, Madrid 28933, Spain

ARTICLE INFO

Article history:
Received 9 November 2018
Revised 8 February 2019
Accepted 2 March 2019
Available online 11 March 2019

Keywords:
Authentication
Federated Identity Management
Identity providers
OpenID Connect
Threat modelling

ABSTRACT

Federated Identity Management (FIM) specifications have been massively adopted in web, cloud and mobile environments during the last years. Facebook, Google, Twitter, LinkedIn, Amazon, Microsoft or Salesforce, to mention only some significant examples, are actively supporting standards such as OAuth or OpenID Connect, becoming in many cases identity providers. This last specification is able to solve identification, authentication, authorization and accounting (IAAA) with one unified flow and two tokens; making logging easier, safer and more secure when compared with previous solutions. Naturally, experts are predicting a widespread adoption of OpenID Connect in the next years not only in web, cloud or mobile environments but also in Fog Computing, IoT or Smart Places. To better understand the threats that this specification poses, this work presents a thorough threat modelling of OpenID Connect core specification and its current implementations. Threats for security and privacy and up to 16 different attack patterns have been identified, analysed and described. Furthermore, possible mitigations and solutions are proposed for both, specification and implementation aspects.

© 2019 Elsevier Ltd. All rights reserved.

1. Introduction

The nature of identity is changing to the point of considering that identity is the new money. Main technology providers have been trying for years to leverage existing user accounts in order to provide new services regarding identity and access management while users has been looking for effortless solutions allowing them to consume different services from different devices with a Single Sign-On approach (SSO).

Federated Identity Management (FIM) allows end users (EU) to access different resources, applications and services through a single Identity Provider (IdP), avoiding the need of having an account (with its related password and/or authenticators) for each resource, application or service. Resource, application and service providers are clients or Relying Parties (RP) in these schemes, relying on IdPs to support identification, authentication and authorization decisions and to store accounting information. IdPs usually provide RPs different Software Development Kits (SDKs) and Application Programming Interfaces (APIs) to help their development teams in implementing access control functionalities.

Many standards and protocols have been specified in the last few years following this kind of scheme. OpenID (OIDF) is an authentication protocol providing a way to prove that an end user controls a specific identifier. OAuth (IETF) is an authorization protocol typically focused on managing access delegation. OpenID Connect (OIDC) (OIDF) is an authentication and authorization protocol based on building OpenID on top of OAuth, and therefore, extending it to solve authentication besides authorization. For example, if a user needs to check in for a flight, and the airline's website supports OpenID Connect, the user clicks on the Identity Provider logo as log-in option (Facebook or Google, for example) and she begins an

* Corresponding author.
E-mail addresses: jorge.navas@urjc.es (J. Navas), marta.beltran@urjc.es (M. Beltrán).
https://doi.org/10.1016/j.cose.2019.03.003
0167-4048/© 2019 Elsevier Ltd. All rights reserved.

Hace falta mejorar las especificaciones, pero también las implementaciones

Jorge Navas, Marta Beltrán:
Understanding and mitigating OpenID Connect threats.
Computers & Security 84: 1-16 (2019)

4

Los retos

GESTIÓN FLEXIBLE Y EN TIEMPO REAL, SEGURIDAD ADAPTATIVA, RESPETO A LA PRIVACIDAD

¿Podemos tener en cuenta el pasado de un usuario o de otros parecidos a él? ¿Cómo adaptamos la seguridad al contexto? ¿Podemos hacer todo esto sin amenazar a la privacidad?

COMPUTERS & SECURITY 108 (2021) 102356

Available online at www.sciencedirect.com

ScienceDirect

Journal homepage: www.elsevier.com/locate/cose

Computers & Security

An approach to detect user behaviour anomalies within identity federations

Alejandro G. Martín, Marta Beltrán, Alberto Fernández-Isabel, Isaac Martín de Diego*

Rey Juan Carlos University, Department of Computing, ETSII, C/ Tulipán, s/n, Móstoles, 28933, Madrid, Spain

ARTICLE INFO

Article history:
Received 13 January 2021
Revised 22 April 2021
Accepted 31 May 2021
Available online 10 June 2021

Keywords:
Anomaly detection
Behavioural fingerprint
Federated identity management
Machine learning
User and entity behaviour analytics

ABSTRACT

User and Entity Behaviour Analytics (UEBA) mechanisms rely on statistical techniques and Machine Learning to determine when a significant deviation from patterns or trends established as a standard for users and entities is occurring. These mechanisms are beneficial within cybersecurity contexts because they allow managers and administrators to have early alerts warning about potential security incidents. This paper proposes the utilisation of UEBA to improve the security of Federated Identity Management (FIM) solutions. The proposed UEBA workflow allows Relying Parties within identity federations to build a session fingerprint characterising each user's behaviour from available information. Furthermore, it enables anomaly detection based on this fingerprint, integrating raised alerts within current identity management specifications. The proposed workflow is validated and evaluated in a real use case based on a web chat application using OpenID Connect for identity management.

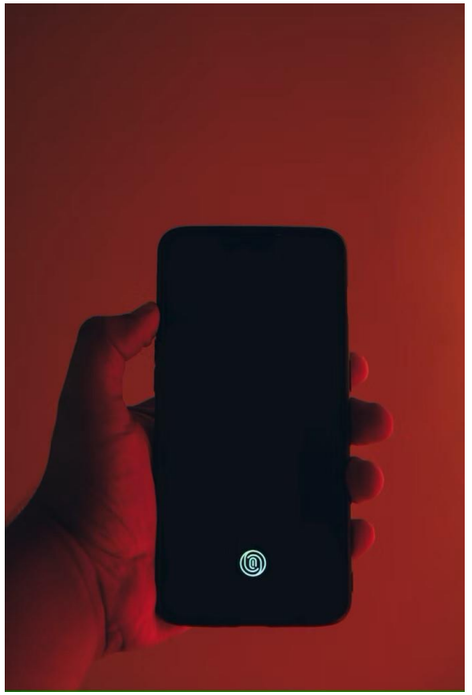
© 2021 The Author(s). Published by Elsevier Ltd.
This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/)

1. Introduction

User and Entity Behaviour Analytics (UEBA) relies on Machine Learning (ML) to model users and entities' behaviour trying to find anomalous behaviour that could be the sign of a cyber-attack. UEBA solutions usually gather information on the average expected behaviour of users and entities from different sources. Once this information is filtered and pre-processed, a baseline of user behaviour can be established through patterns or fingerprints. Then, UEBA solutions perform continuous monitoring of users and entities' behaviour to compare it to baseline behaviour.

This work focuses on proposing a framework to add UEBA techniques to Federated Identity Management (FIM) solutions (Chadwick, 2009) such as OpenID Connect or Mobile Connect OIDF (2021). With these identity management specifications, end-users credentials are stored at an external server or Identity Provider (IdP), responsible for Identification, Authentication, Authorisation and Accounting (IAAA). When an end-user needs to access a resource, application or service (i.e. the Relying Party or RP), the RP trusts the external server or IdP to solve IAAA. Thus, the end-user is authenticated outside the RP (i.e., in the IdP), obtaining a capacity in the form of a token. Finally, the end-user can access the RP using this token. Moving from traditional solutions to identity federations implies that the authentication process goes from local (i.e., the RP stores and checks locally the end-user credentials or authenticators) to outsourced (i.e., the RP trusts the IdP in order to accomplish the IAAA).

* Corresponding author.
E-mail addresses: alejandro.garciam@urjc.es (A.G. Martín), marta.beltran@urjc.es (M. Beltrán), alberto.fernandez.isabel@urjc.es (A. Fernández-Isabel), isaac.martin@urjc.es (I. Martín de Diego).
https://doi.org/10.1016/j.cose.2021.102356
0167-4048/© 2021 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/)



Los mecanismos UEBA (User and Entity Behaviour Analytics) pueden ayudar a detectar suplantaciones y secuestros de sesión

Alejandro G. Martín, Marta Beltrán, Alberto Fernández-Isabel, Isaac Martín de Diego:
An approach to detect user behaviour anomalies within identity federations.
Computers & Security 108: 102356 (2021)

Static and predictable inputs

Noise and variable inputs

MEASUREMENT

Instrumentation

Metrics

Monitoring

Context-awareness

DECISION

Adaptation engine

Rules

Policies

Decision-maker

Policy administrator

ADAPTATION

Interfaces

APIs

Middleware

Control owner

PLUGIN

Security control

Computers & Security 115 (2022) 102612

Contents lists available at ScienceDirect

Computers & Security

Journal homepage: www.elsevier.com/locate/cose

TC 11 Briefing Papers

A Model For risk-Based adaptive security controls

Miguel Calvo, Marta Beltrán*

Department of Computing, ETSII, Universidad Rey Juan Carlos, Móstoles 28933, Madrid, Spain

ARTICLE INFO

ABSTRACT

1. Introduction

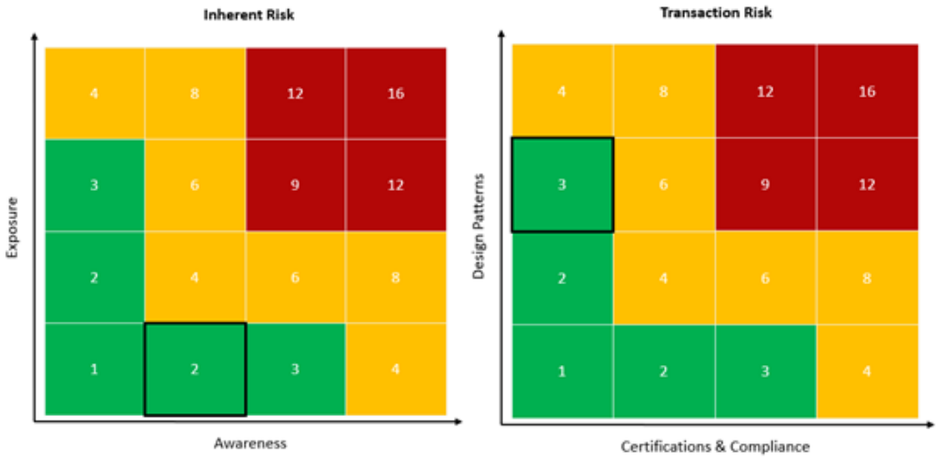
Miguel Calvo, Marta Beltrán:
A Model For risk-Based adaptive security controls.
Computers & Security 115: 102612 (2022)

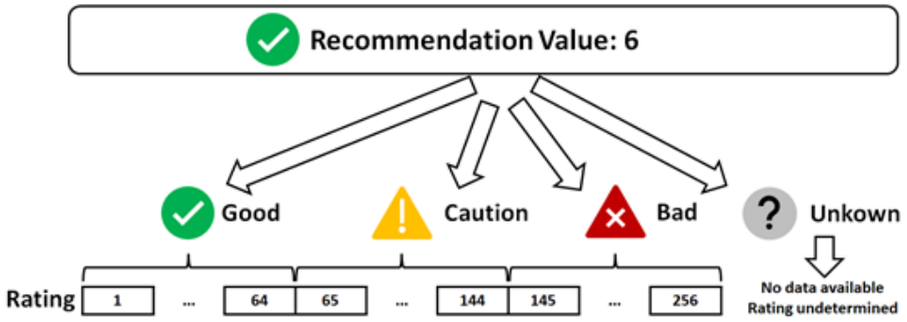
Layer 1

Recommendation: Good

Layer 2

TOTAL RISK: 6/256





Total Risk = Inherent risk X Transaction Risk

Total Risk = 2 X 3 = 6

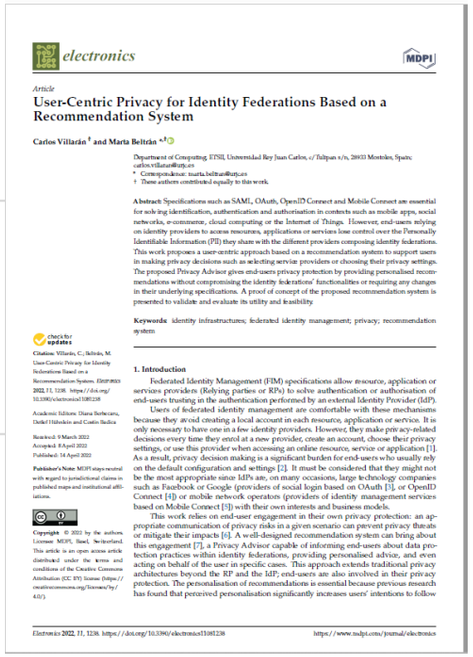
Layer 3

- Reputation
- Privacy Certifications
- Design Patterns
- Compliance

Design Patterns

Misdirection

Privacy Zuckering



electronics

MDPI

Article

User-Centric Privacy for Identity Federations Based on a Recommendation System

Carlos Villarán † and Marta Beltrán *,†

Department of Computing, ETSII, Universidad Rey Juan Carlos, c/ Tulipan s/n, 28933 Mostoles, Spain; carlos.villaran@urjc.es

* Correspondence: marta.beltran@urjc.es

† These authors contributed equally to this work.

Abstract: Specifications such as SAML, OAuth, OpenID Connect and Mobile Connect are essential for solving identification, authentication and authorisation in contexts such as mobile apps, social networks, e-commerce, cloud computing or the Internet of Things. However, end-users relying on identity providers to access resources, applications or services lose control over the Personally Identifiable Information (PII) they share with the different providers composing identity federations. This work proposes a user-centric approach based on a recommendation system to support users in making privacy decisions such as selecting service providers or choosing their privacy settings. The proposed Privacy Advisor gives end-users privacy protection by providing personalised recommendations without compromising the identity federations' functionalities or requiring any changes in their underlying specifications. A proof of concept of the proposed recommendation system is presented to validate and evaluate its utility and feasibility.

Keywords: identity infrastructures; federated identity management; privacy; recommendation system

1. Introduction

Federated Identity Management (FIM) specifications allow resource, application or services providers (Relying parties or RPs) to solve authentication or authorisation of end-users trusting in the authentication performed by an external Identity Provider (IdP).

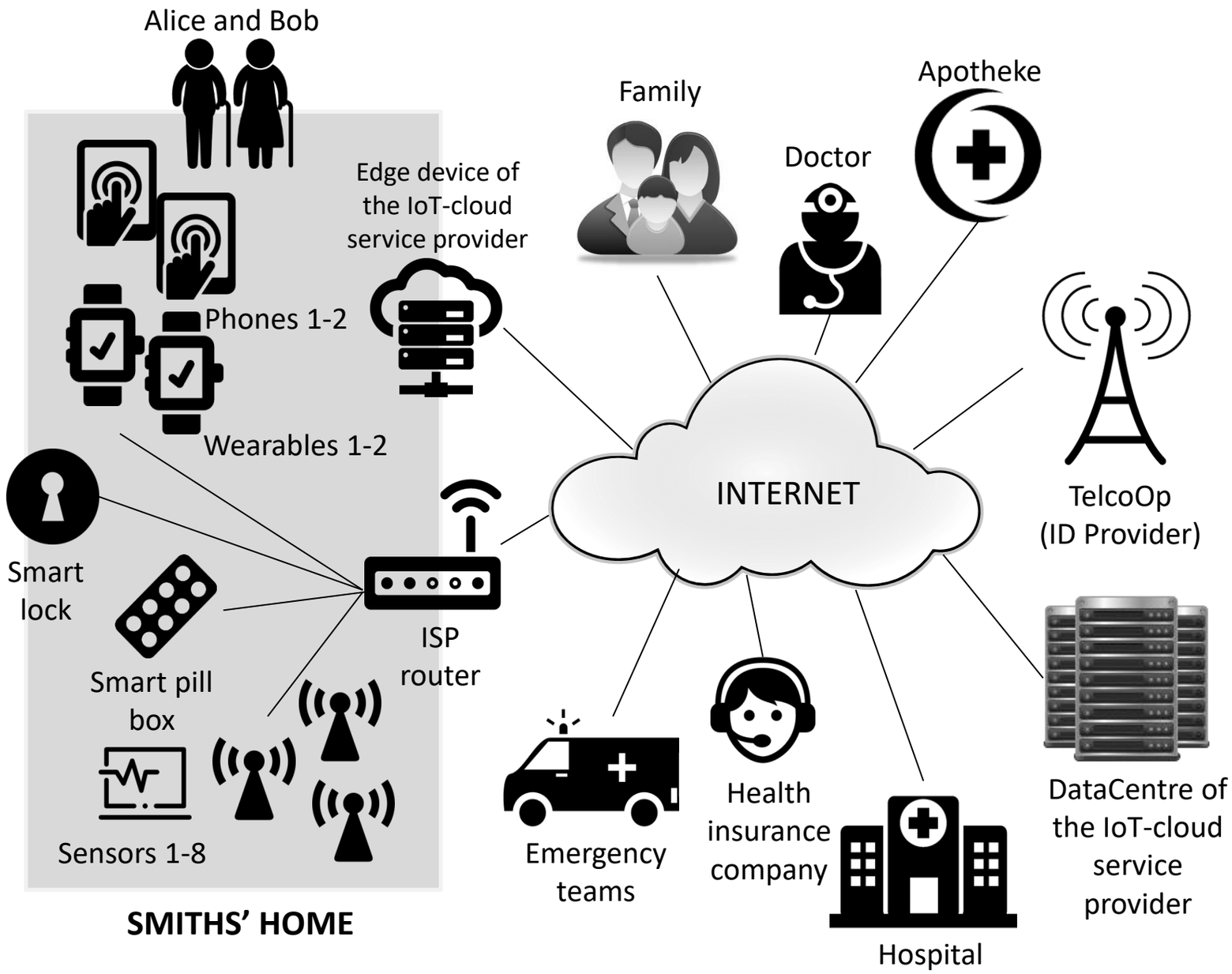
Users of federated identity management are comfortable with these mechanisms because they avoid creating a local account in each resource, application or service. It is only necessary to have one in a few identity providers. However, they make privacy-related decisions every time they enrol at a new provider, create an account, choose their privacy settings, or use this provider when accessing an online resource, service or application [1]. As a result, privacy decision making is a significant burden for end-users who usually rely on the default configuration and settings [2]. It must be considered that they might not be the most appropriate since IdPs are, on many occasions, large technology companies such as Facebook or Google (providers of social login based on OAuth [3], or OpenID Connect [4]) or mobile network operators (providers of identity management services based on Mobile Connect [5]) with their own interests and business models.

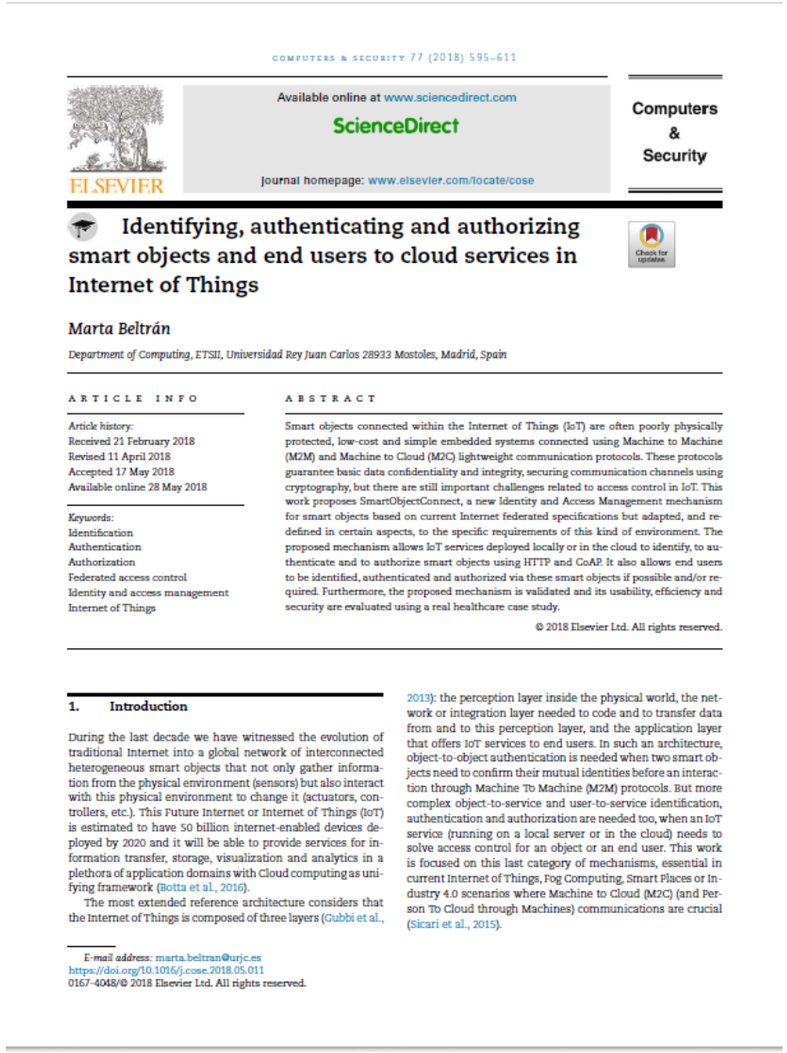
This work relies on end-user engagement in their own privacy protection: an appropriate communication of privacy risks in a given scenario can prevent privacy threats or mitigate their impacts [6]. A well-designed recommendation system can bring about this engagement [7], a Privacy Advisor capable of informing end-users about data protection practices within identity federations, providing personalised advice, and even acting on behalf of the user in specific cases. This approach extends traditional privacy architectures beyond the RP and the IdP; end-users are also involved in their privacy protection. The personalisation of recommendations is essential because previous research has found that perceived personalisation significantly increases users' intentions to follow

Carlos Villarán, Marta Beltrán:
User-Centric Privacy for Identity Federations Based on a Recommendation System.
Electronics 11(8): 1238 (2022)

IAAA en el Internet de las Cosas (IoT)

¿Y si no hay un navegador? ¿Y si el protocolo no es HTTP? ¿Y si no hay una persona detrás? ¿Y si una persona necesita autenticarse a través de un dispositivo con recursos limitados? ¿Y si trabajamos con Edge Computing?





COMPUTERS & SECURITY 77 (2018) 595–611

Available online at www.sciencedirect.com

ScienceDirect

Journal homepage: www.elsevier.com/locate/cose

Computers & Security

Identifying, authenticating and authorizing smart objects and end users to cloud services in Internet of Things

Marta Beltrán

Department of Computing, ETSII, Universidad Rey Juan Carlos 28933 Mostoles, Madrid, Spain

ARTICLE INFO

Article history:
Received 21 February 2018
Revised 11 April 2018
Accepted 17 May 2018
Available online 28 May 2018

Keywords:
Identification
Authentication
Authorization
Federated access control
Identity and access management
Internet of Things

ABSTRACT

Smart objects connected within the Internet of Things (IoT) are often poorly physically protected, low-cost and simple embedded systems connected using Machine to Machine (M2M) and Machine to Cloud (M2C) lightweight communication protocols. These protocols guarantee basic data confidentiality and integrity, securing communication channels using cryptography, but there are still important challenges related to access control in IoT. This work proposes SmartObjectConnect, a new Identity and Access Management mechanism for smart objects based on current Internet federated specifications but adapted, and redefined in certain aspects, to the specific requirements of this kind of environment. The proposed mechanism allows IoT services deployed locally or in the cloud to identify, to authenticate and to authorize smart objects using HTTP and CoAP. It also allows end users to be identified, authenticated and authorized via these smart objects if possible and/or required. Furthermore, the proposed mechanism is validated and its usability, efficiency and security are evaluated using a real healthcare case study.

© 2018 Elsevier Ltd. All rights reserved.

1. Introduction

During the last decade we have witnessed the evolution of traditional Internet into a global network of interconnected heterogeneous smart objects that not only gather information from the physical environment (sensors) but also interact with this physical environment to change it (actuators, controllers, etc.). This Future Internet or Internet of Things (IoT) is estimated to have 50 billion internet-enabled devices deployed by 2020 and it will be able to provide services for information transfer, storage, visualization and analytics in a plethora of application domains with Cloud computing as unifying framework (Botta et al., 2016).

The most extended reference architecture considers that the Internet of Things is composed of three layers (Gubbi et al., 2013): the perception layer inside the physical world, the network or integration layer needed to code and to transfer data from and to this perception layer, and the application layer that offers IoT services to end users. In such an architecture, object-to-object authentication is needed when two smart objects need to confirm their mutual identities before an interaction through Machine To Machine (M2M) protocols. But more complex object-to-service and user-to-service identification, authentication and authorization are needed too, when an IoT service (running on a local server or in the cloud) needs to solve access control for an object or an end user. This work is focused on this last category of mechanisms, essential in current Internet of Things, Fog Computing, Smart Places or Industry 4.0 scenarios where Machine to Cloud (M2C) (and Person To Cloud through Machines) communications are crucial (Sicari et al., 2015).

E-mail address: marta.beltran@urjc.es
https://doi.org/10.1016/j.cose.2018.05.011
0167-4048/© 2018 Elsevier Ltd. All rights reserved.

Marta Beltrán:
Identifying, authenticating and authorizing smart objects and end users to cloud services in Internet of Things.
Computers & Security 77: 595-611 (2018)

Computer Communications 160 (2020) 464–474

Contents lists available at ScienceDirect

Computer Communications

Journal homepage: www.elsevier.com/locate/comcom

Edge-centric delegation of authorization for constrained devices in the Internet of Things

Elías Grande, Marta Beltrán *

Department of Computing, ETSII, Universidad Rey Juan Carlos, 28933 Mostoles, Madrid, Spain

ARTICLE INFO

Keywords:
Access control
Delegation of authorization
CoAP
Identity management
Internet of Things
OAuth

ABSTRACT

Access management poses a significant challenge within the Internet of Things (IoT) given the constrained capabilities in terms of computing, memory, storage, bandwidth and energy available for most of the low-cost devices and things embedded in the physical world. In this scenario, Edge Computing can be considered a powerful opportunity to solve authorization issues, deploying edge devices near IoT constrained things capable of performing as logical intermediaries or brokers between them and cloud resources, services or applications. This work proposes an edge-centric delegation of authorization for constrained devices (without cryptographic capabilities) based on well-known and extensively used specifications and protocols such as OAuth 2.0 and CoAP (Constrained Application Protocol). The proposed solution is based on three different roles allowing constrained devices automated enrolment, authorized access to resources deployed in the cloud and roaming. Furthermore, the proposed solution is validated and assessed using a real smart farming case study.

1. Introduction

Ensuring proper levels of security has become an essential topic for the success and evolution of the Internet of Things (IoT) [1]. In this scenario, the protection of IoT resources, services and applications against unauthorized accesses still represents one of the main challenges to overcome [2]. The traditional trust-based security model relying on identification, authentication and authorization is no longer feasible due to the inherent scalability of IoT projects and to resource limitations. How can we control the access to IoT resources, services and applications from such a large number of heterogeneous and often constrained devices? The security model requires a new approach, preferably based on well-known and widely used technologies and specifications, based on the least privilege and the least attack surface principles but considering the specificities of IoT scenarios [3]. Ideally, taking advantage of them to propose scalable, light, efficient, resilient and robust solutions.

Federated specifications such as OAuth [4] may be an excellent solution to solve authorization in IoT scenarios because they address several significant security issues such as fine-grained and time-limited authorization, access rights revocation, support for offline authorization, protection against collusion attacks, integration of robust cryptographic algorithms when required, etc. But given the limited hardware resources of many of the IoT devices, only lightweight security functions can be deployed on them. This does not include support for OAuth or other similar token-based specifications.

The new Edge (or Fog) Computing paradigm introduces key nodes (such as smart gateways, controllers, etc.) at the edge of the network, near constrained devices and able to communicate with IoT resources, services and applications in the cloud [5]. These new nodes can be used to offload security functions, to prevent attacks from spreading to an entire IoT domain, to control the scope of security threats, etc. In summary, edge devices can be used as logical intermediaries, brokers or proxies between the physical and the Internet/Web layers of IoT raising security levels [6].

The main contributions of this work are:

1. The specification of a new token-based access control mechanism for IoT relying on edge-centric delegation of authorization.
2. A novel approach for handling this authorization in large scale scenarios in the presence of constrained devices (without cryptographic capabilities) leveraging and properly adapting and extending the well-known OAuth 2.0 specification.
3. The definition of three different flows, all of them working over a lightweight communication protocol (CoAP), solving the most important challenges arising in the considered scenario: automated enrolment, access control and roaming.
4. A complete implementation of the proposed specification used in a real scenario (in the smart farming context), validating its functionalities and assessing its levels of efficiency and security.

* Corresponding author.
E-mail addresses: elias.grande@urjc.es (E. Grande), marta.beltran@urjc.es (M. Beltrán).

https://doi.org/10.1016/j.comcom.2020.06.029
Received 22 January 2020; Received in revised form 22 May 2020; Accepted 25 June 2020
Available online 29 June 2020
0140-3664/© 2020 Elsevier B.V. All rights reserved.

Los dispositivos Edge pueden hacer de intermediarios entre los IoT y los servicios en la nube, "cediendo" sus tokens

Elías Grande, Marta Beltrán:
Edge-centric delegation of authorization for constrained devices in the Internet of Things.
Computer Communications 160: 464-474 (2020)

5

Conclusiones

La resolución del IAAA se ha convertido en un modelo de negocio opaco.

Se debe evitar, en la medida de lo posible, que las corporaciones privadas incorporen biometría u otra información sensible a los datos que ya manejan: el potencial impacto de las amenazas es mucho mayor.

Que los datos sean manejados por administraciones públicas no garantiza que se apliquen estrategias de privacidad desde el diseño: minimizar, ocultar, separar, abstraer, informar, controlar, cumplir, demostrar.

¿QUÉ IMPLICA EXACTAMENTE EL CONCEPTO DE IDENTIDAD AUTO-SOBERANA (SSI) Y DE LA CARTERA DIGITAL?

La prioridad debería ser no depender de un tercero, de un proveedor con sus propios intereses y agenda

Hasta el momento se ha asociado mucho con la tecnología blockchain, pero es algo muy preliminar

GRACIAS

POR HABER ATENDIDO HASTA AHORA

¿Tenéis alguna pregunta o comentario para mi?

De todas formas podéis localizarme fácilmente:


marta.beltran@urjc.es


@experiencia_T


https://mbelpar.github.io/

©2023 Marta Beltrán URJC (marta.beltran@urjc.es)
Algunos derechos reservados.
Este documento se distribuye bajo la licencia “Reconocimiento-CompartirIgual 3.0 España” de Creative Commons, disponible en
https://creativecommons.org/licenses/by-sa/3.0/es/

Presentación creada con Visme (https://www.visme.co/es/)
Fotografías: https://unsplash.com
Iconos: https://www.flaticon.es/