OLYMPUS contributions and recommendations for improving cross-border identification in the European Union

The purpose of the project OLYMPUS is to improve traditional delegated IdM solutions, enhancing some of their main drawbacks through novel cryptographic approaches adding security and privacy in identification and authentication processes. More specifically, the project OLYMPUS has developed a distributed and highly resilient password service, at the time it has boosted secure selective disclosure techniques in its two use cases.

The regulatory framework of electronic identification and authentication services across the European Union aims to increase trust in electronic identification across Member States in the realization of the European Union Digital Single Market. The main regulation at the EU level is the eIDAS Regulation. This regulation aims to guarantee cross-border identification and authentication operations by establishing a set of criteria for mutual recognition and determining the technical requirements so that the technology proposed fulfills the level of security (i.e., Levels of Assurance) required for the mandatory admission by the Member States in cross-border identification operations.

Some challenges have risen throughout the development of the project OLYMPUS in terms of application of the existing regulatory framework. These challenges have concerned, in particular, to the evaluation and implementation of disruptive technologies. As a result, the project has supported initiatives for redrafting of the eIDAS Regulation, reinforcing the need of a short-term revision, that has resulted in a proposal for review made public in June 2021. In addition, the eIDAS Regulation has been studied conjointly with other regulations, in particular, with the General Data Protection Regulation, offering relevant results in terms of the necessary consistency within the European Union Regulatory Framework.

CONTRIBUTIONS WITH POLICY IMPACT

1.Challenges to technology neutrality

Description: it should be discussed whether the regulatory framework in the European Union imposes a specific technology for identification and authentication cross-border processes.

The OLYMPUS technology has proved the possibility of achieving a high security level, since it prevents from a wider range of cyberattacks, without the need of including a two-factor authentication mechanism.

Article 7 of the eIDAS Regulation establishes a set of conditions for the mutual recognition of electronic identification means in the European Union between Member States. Among these conditions, pursuing sections b) and c) “the assurance level must be equal or higher than the level required by the relevant public sector body to access the service online”. Security levels are described in Article 8.2, as a number of high-level and somewhat abstract criteria, thus, to determine whether an electronic means fulfills these Levels of Assurance the Annex of the Commission Implementing Regulation (EU) 2015/1502 of the 8th of September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means must be consulted.

Pursuing this legal text, to achieve at least a substantial Level of Assurance during authentication phase, a dynamic authentication method is required. This legal text also contains a definition for a dynamic authentication in Article 1 (3) of the Annex, as “an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and

which changes with each authentication between the subject and the system verifying the subject's identity". In other words, a multi-factor authentication method where one of the factors changes in each authentication process.

Should this definition be interpreted in its strictest terms, the OLYMPUS initial design, as a single factor password-based authentication method, would not be able to fulfill the requirements to achieve a substantial or high level of assurance despite offering a higher security than traditional technologies (even deployed in a multi-factor scheme).

The requirement of a technology by default contravenes the principle of technological neutrality as organizations and individuals would be discouraged from make use of other technologies. Furthermore, it contravenes what stated in the eIDAS Regulation (Recital 16 and Section 3 of the Article 12), claiming that the requirements established should be technology neutral.

Recommendation: to modify sections 1 (3) and 2.2.1. and 2.3.1. of the Annex of the Commission Implementing Regulation (EU) 2015/1502 of 8th September on setting out minimum technical specifications and procedures for assurance levels of electronic identification means, to allow the inclusion of technological infrastructures differing from two-factor authentication methods, but that achieve equal or higher security level in the prevention of attacks.

Other assessment criteria, such as a more detailed specification of the attacks that the electronic identification means should be able to prevent, could be considered in order to guarantee the admission of electronic identification means offering an adequate security level.

These aspects would also have to be considered and reevaluated with regard to the authentication processes taking place within the future European Digital Identity Wallets.

2.Consistency with data protection principles

Description: the need of providing a regulatory framework for identity attributes proofing (e.g., being over a certain age), beyond the traditional identification concept has been subject of study.

Modern cryptographic techniques (i.e., p-ABCs, ZKP among others), have made possible to limit data disclosure by design in identification and authentication processes.

At the present time, this possibility is limited in the EU scope by the eIDAS Regulation. The Annex of the Commission Implementing Regulation (EU) 2015/1501 of 8th September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014, imposes the obligation to use a set of minimum attributes for the identification of natural or legal persons.

This requirement limits the possibilities of deployment of selective disclosure techniques and contravenes the principle of data minimization, as well as the general rule of the eIDAS Regulation to comply with data protection regulations and facilitate privacy by design.

There is an urgent need to provide an adequate regulatory framework in the European Union for these operations to assure compliance with data protection principles, as well as to avoid situations of divergence related to the scope of application of the eIDAS Regulation.

Recommendations: we recommend maintaining, during the legislative process for the adoption of the proposal for review of the eIDAS Regulation, Article 3 point 16 (a) and Section 9 of the Proposal, as an extension of the eIDAS legal framework, that creates a legal rule authorizing the sharing of identity attributes, at the time their validity is assured in the Member States.

3.Privacy by design

Description: it would be interesting to consider the need to provide effective guidelines to assess the level of privacy by design in a technology prior its implementation in real scenarios.

OLYMPUS technology represented an innovative architecture in the sector of Identity Management, and it has required an effective evaluation concerning the level of compliance with data protection principles before its implementation.

The Data Protection Impact Assessment seemed to be the most adequate tool to provide such evaluation. It showed however, some deficiencies at it is designed for context-specific evaluations (e.g. ISO/IEC 29134:2017, as well as national guidelines).

The development of privacy respectful technologies is a complex task. Although technical experts manage some privacy concepts, they tend to omit essential legal requirements that could be decisive in the final evaluation of a technology or that imply in some cases, an inadequate approach to the technology's design.

Some of the privacy and data protection risks detected in a DPIA are linked to the technology deployed. In this sense, performing this study in a prior stage could prevent from discarding technological proposals with big potential, or in the worst cases, implementing technological solutions that imply a high risk but that are too expensive to modify at that phase of development.

Recommendations: we recommend the production of guidelines specifically conceived for performing evaluations in an early stage, over technological proposals, favoring collaboration between technical and legal experts, assuring privacy by design.

It could be considered the development of a multiphase DPIA or a DPIA in layers. By adapting the DPIA methodology, a preliminary assessment, or "first layer" could be performed over technological proposals prior their implementation in order to ease further context-based studies, and above all, assure compliance with privacy by design requirements

Once this first layer has concluded, a second assessment or "layer" consisting in the study of the level of compliance with data protection principles in the specific scope of the data processing could be performed with regard to each specific scenario where the technology aims to be deployed.

4.Allocation of GDPR roles and responsibilities in disruptive scenarios

Description: The GDPR administrative roles of data controller and data processor are envisaged for the allocation of tasks and responsibilities, in particular when more than an entity, natural or legal person are involved in the data processing activity.
The emergence of new technologies is challenging the application of these roles. In distributed technologies an in-depth analysis is required to conclude, in those cases where there is not a clear determination of the purposes of the processing, whether an influence over the essential means of the processing exists.

Recommendation: to clarify the application of data controller and data processor roles to decentralized architectures via an A29 WP Opinion.

OLYMPUS is a distributed technology that can support decentralization, that is to say, it can be deployed by different legal entities in position of equality or where any of them can lead or coordinate the others, but they act conjointly. There is no existing regulation concerning the application of the GDPR to decentralize architectures. Some considerations have been made with regard to blockchain technologies, but they do not offer legal certainty.

On the other hand, OLYMPUS mDL offline scenario is in line with the oblivious use aimed by the proposal for review of the eIDAS

Regulation for the European Digital Identity Wallets. An extension of the number of Issuing Authorities (Credential Providers) will lead to the scenario envisaged in the eIDAS2 Regulation, where there is not a clear entity providing the electronic identification and authentication service.

Such user-centric scenario raises the question of who will hold the role of data controller. Credential providers must be qualified as data controllers for the processing of issuance of the credential, but not for the data processing taking place while stored in the wallet.

Recommendation: the specific scenario of the European Digital Identity Wallets must be studied. It must be assessed whether the role developed by wallet providers is enough and justifies their qualification as data controller for the processing taking place in or via the wallet.

Likewise, the different possibilities for the provision of the wallets envisaged in Article 6.1 of the proposal for review of the eIDAS Regulation must be considered in order to clarify this role.

PROJECT'S INFORMATION

The project OLYMPUS (Oblivious identitY Management for Private and User-friendly Services) is funded under the scheme of H2020-EU 3.7.6. and coordinated by the University of Murcia (Spain) with the participation of the following consortium: IBM Research GMBH (Switzerland), Alexandra Instituttet A/S (Denmark), Multicert- Serviços de Certificação Electrónica SA (Portugal), Logalty Servicios de Tercero de Confianza SL (Spain), Scytales AB (Sweeden).

The project term is envisaged from September 2018 to November 2021 with a budget of 3 147 837,50 euros.

For more information you can contact **mariacristina.timon@um.es** or access the website of the project https://olympus-project.eu/

Publications of interest:

D3.2 Security and Privacy-aware OLYMPUS Framework Impact Assessment- https://olympus-project.eu/wp-content/uploads/2020/02/Olympus_pu_d3_2_v1_0.pdf

D5.3 OLYMPUS support for extended eID models- https://olympus-project.eu/wp-content/uploads/2020/10/Olympus_pu_d5_3_v1_0.pdf

Alamillo Domingo, I. SSI eIDAS Legal Report - How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market. European Commission B-1049 Brussels. April 2020. Available at the following address: https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

Approaching the Data Protection Impact Assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. A special reference to Identity Management systems (Draft version)- https://zenodo.org/record/5647249

D6.3 Final Pilot deployment and evaluation of User Experience and GDPR compliance- https://olympus-project.eu/wp-content/uploads/2021/10/Olympus_pu_d6_3_v1_2.pdf