# Borderless Authentic -Authentication in the Upper-Rhine Area with AI

Abdelhafid Abouaissa, Wilfrid Azan, Yannick Boehmann, Michael Böttger, Ugo Devoille, Marc Gilg, Christian Zirpins, Roxana Hess, Bastian Leferink, Pascal Lorenz, et al.

# Borderless Authentic – Authentication in the Upper-Rhine Area with AI

Abdelhafid Abouaissa[1], Wilfrid Azan[2], Yannick Boehmann[3], Michael Böttger[4], Ugo Devoille[3], Marc Gilg[1], Martin Gwerder[5], Roxana Hess[6], Bastian Leferink[4], Pascal Lorenz[1], David Monschein[7], Zoltan Nochta[7], José Antonio Peregrina Pérez[7], Tim Piotrowski[7], Ioan Szilagyi[3], Oliver Waldhorst[7], Jochen Wendel[6], Oliver Wolf [4], Christian Zirpins[7,*]

[1] Université de Haute Alsace (UHA), 2 rue des Frères Lumière, 68093 Mulhouse Cedex, France
**[firstname.lastname]@uha.fr**
[2] Université Lumière Lyon 2: Lyon, Auvergne-Rhône-Alpes, France
**Wilfrid.Azan@univ-lyon2.fr**
[3] Neomia.ai, 3 Rue Pau-Henri Spaak, 68390 Sausheim, France
**[y.Boehmann|u.Devoille|i.Szilagyi]@neomia.ai**
[4] raumobil GmbH, Auer Straße 19, 76227 Karlsruhe
**[m.boettger|b.leferink|o.wolf]@raumobil.com**
[5] Fachhochschule Nordwestschweiz (FHNW), Bahnhofstrasse 5, 5210 Windisch, Switzerland
**[firstname.lastname]@fhnw.ch**
[6] INIT GmbH, Käppelestraße 4-10, 76131 Karlsruhe, Germany
**[Rhess|Jwendel]@initse.com**
[7] Karlsruhe University of Applied Sciences (HKA), Institute of Applied Research (IAF), Data-Centric Software Systems (DSS) Research Group, Moltkestr. 30, 76133 Karlsruhe, Germany
**[firstname.lastname]@h-ka.de**

**Abstract.** Efficient identity management is not only a concern of the virtual world but also paramount for modern open societies like the European Union. Non-intrusive, AI-based techniques of continuous authentication have recently been proposed to increase the security, efficiency and user friendliness of online systems and services. We introduce the research project aura.ai that will investigate how to transfer and apply these novel means of AI-based authentication in the public transportation area of the Upper-Rhine region.

**Keywords:** Continuous Authentication; Federated ML, Public Transport and Mobility

## 1 Introduction

Identity is a crucial feature of anything valuable. It is even more critical for human beings and their various roles, such as being a European citizen. Their identity is key to the property they own and the rights/obligations they have. Identity is intricately linked with the ability to prove it and the ability to validate such proofs, which is known as authentication. There are various means of authenticating humans, including physical means like ID, passport, driving license, or banking cards, and virtual means like passwords, certificates, credentials, and others. All of these hold the risk of getting lost or even being misused. Depending on the case, this might be trivial or disastrous. Such risks lead to additional security measures like multi-factor authentication, combining two or more means [1]. On the one hand, this safeguards authentication, but on the other hand, it increases complexity and effort [2], which opens room for various trade-offs.

In the digital domain (including the digitalized, cyber-physical world), progress has been made to seamlessly authenticate people in a cost-efficient way. This builds on early ideas to

* Corresponding Author

recognize behavioral patterns that are typical or outright unique to human individuals, like their keystrokes [3]. Today, artificial intelligence (AI) offers novel ways to realize recognition of behavioral patterns and apply it to strengthen other means of authentication [4] (for enhanced security) or even to substitute them (for convenience). In the following, we introduce one such technology, namely FML-CA, and its application for public transport in the Upper-Rhine region.

## 2 FML-CA: Federated ML for Continuous Authentication

Ongoing automated authentication based on contextual information is known as continuous authentication (CA) [5]. A novel way of realizing CA uses machine learning (ML) of behavior [6], such as spatial location, movements or swiping on a touch device. The network is another valuable source of behavioral data [7], where, for example, communication patterns, access location, low-level authentication features, and technical fingerprints may be collected. In any case, learning behavior requires training based on behavioral data of individuals or generalizable data of groups. The latter case benefits from public or shared data of people and organizations.

Handling behavioral data and patterns always raises privacy concerns. Regarding behavioral data, federated machine learning (FML) [8] allows the distributed training of partial patterns at the place where they originated and without the need for sharing them. In the end, the partial patterns are aggregated into a single AI model that represents the knowledge of all federation partners (people or organizations). Only the aggregated model is shared, and security technologies ensure the preservation of individual privacy [9], adequate contributions of all participants [10], and the absence of fraudulent manipulation.

The application of AI models for authentication is possible without revealing the models or their input data to the party that requests the authentication by means of homomorphic encryption (HE) [11]. Also, the real-time behavioral data of individuals being authenticated may be gathered by third parties without exposing their identities by means of pseudonymization. Altogether, FML-based CA (FML-CA) can be achieved while respecting privacy.

## 3 FML-CA for Public Transport in the Upper-Rhine Region

An interesting application area of FML-CA is public transportation, especially for such cases that include international operations crossing borders. To this end, we are focusing on the Upper-Rhine region that spans 350 kilometers along the river Rhine at the borders between France Germany and Switzerland. This tri-national region is involved in the European Territorial Cooperation program (also known as Interreg[†]). Therefore, it offers optimum conditions to implement innovative trans-national applications of FML-CA.

The research project aura.ai aims to tap the potential of FML-CA in the public transport area of the Upper-Rhine region. The goals of aura.ai are to make Upper-Rhine mobility more secure, less expensive, and more comfortable by using FML-CA. More concretely, the project will capitalize on experiences in the context of the regiomove project[‡]. regiomove is a mobility platform in the Karlsruhe area involving multiple federated providers of mobility services. Currently, a similar platform is being built for the Ortenau region and it is planned to connect the two platforms enabling interregional booking. Furthermore, the goal is to enable cross-border connectivity to Strasbourg. Therefore, regiomove is an excellent example of interregional and cross-

[†] https://interreg.eu/

[‡] https://www.regiomove.de/

border mobility. It will provide the application context for utilizing FML-CA, leading to technologies and lessons learned that can be also transferred to other regions in the Upper Rhine area, such as the Basel region.

Today, regiomove builds on close legal relationships of partners on the core platform to provide integrated IT-support for multimodal mobility (route planning, ticketing, bike/e-scooter/car sharing, etc.) in Karlsruhe. Currently, travelers are centrally authenticated to enable seamless use of all services, which is paramount for the required user experience. While reliable permanent login is already challenging in the centralized case, the integration of mobility services of other regions and beyond the core platform federation cannot be done centrally anymore. This hampers the extension of the mobility solution to cover the whole tri-national region and forces travelers to self-organize multiple accounts of regional providers, re-authenticate, and experience media breaks, thereby also reducing the acceptance and usage of public transport as such.

Aura.ai aims to demonstrate that FML-CA can help to solve authentication-related hurdles of interregional multimodal mobility solutions. As a Proof-of-Concept (PoC), we want to apply FML-CA to enable permanent login for services without traveler distraction by automated re-authentication and demonstrate this for the mobile app of the regiomove platform. Building on this core, aura.ai is going to study how to enable automated switches between regional mobility providers based on FML-CA instead of manual logins for services of the Karlsruhe, Ortenau and Strasbourg areas. Overall, this will open the perspective of a seamless network of mobility services across the tri-national region.

## 4 Aura.ai Technical Building Blocks

Concerning the methods and technologies to be applied in aura.ai, fundamental methods for FML-CA have been studied in the research project KIWI[§] at Karlsruhe University of Applied Sciences [12]. These approaches will be augmented, extended, and complemented in two directions, to make them applicable in the case of aura.ai.

First, network modeling and monitoring mechanisms in the domain of multi-provider/cross-border public transport, that are developed at the Université de Haute Alsace (UHA), enable the continuous gathering of real-time data, such as low-level login features, as a basis for CA.

Second, a proxy (PrivID) for a common authentication protocol, that is being developed at Fachhochschule Nordwestschweiz (FHNW), bridges the FML-CA approaches to already established technologies on the Web. PrivID extends the standard functionality of a basic authentication protocol (e.g., Oauth2/SAML2 [13]) to allow CA with privacy-preserving pseudonymization between various providers. This pseudonymization is necessary to connect authentication providers who want to share a joint account but are unwilling or unable (e.g., due to jurisdictional restrictions) to provide customer information. PrivID will introduce consumer-specific pseudonyms while the data functionality (e.g., a pseudonymized email address or a name in a front-end) remains maintained without breaking pseudonymity. Such features are exceptionally important in a transnational mobility context, as jurisdictional rules even may forbid sharing such data.

Together, aura.ai aligns these technical building blocks to augment FML-based CA with vital features for innovative cross-border public transport services.

---

[§]Artificial intelligence in secure web infrastructures with digital identity management (Künstliche Intelligenz in sicheren Web-Infrastrukturen mit digitalem Identitätsmanagement - KIWI) funded by the German Federal Ministry of Education and Research (BMBF, 16KIS1142K, https://www.h-ka.de/iaf/kiwi)

## 5 Conclusion

The upcoming research project aura.ai is targeting various innovation areas like digitalization, cybersecurity, and sustainable mobility. It will make existing scientific results, namely FML-based CA with pseudonymized network data, usable for the economic sector of public transportation. Measures of the project will include the development of demonstrators and the conduction of pilot applications in cross-border public transportation. The tri-national Upper-Rhine region will significantly benefit from the project as it will help to a) bring together transport service and IT providers from multiple countries, b) foster the free movement of people within the region, and c) make public transport even more attractive to citizens. Furthermore, aura.ai includes an approach to AI governance that will ensure the absence of bias and equal treatment of people regardless of gender, race, or disabilities. Overall, aura.ai will make a difference for the holistic benefit of the Upper-Rhine region in line with the goals of the European Union.

## 6 References


[1] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," *Cryptography*, vol. 2, no. 1, p. 1, Jan. 2018, doi: 10.3390/cryptography2010001.

[2] S. Das, B. Wang, Z. Tingle, and L. J. Camp, "Evaluating User Perception of Multi-Factor Authentication: A Systematic Review," 2019, doi: 10.48550/ARXIV.1908.05901.

[3] R. Joyce and G. Gupta, "Identity authentication based on keystroke latencies," *Commun. ACM*, vol. 33, no. 2, pp. 168–176, Feb. 1990, doi: 10.1145/75577.75582.

[4] D. Garabato, C. Dafonte, R. Santoveña, A. Silvelo, F. J. Nóvoa, and M. Manteiga, "AI-based user authentication reinforcement by continuous extraction of behavioral interaction features," *Neural Comput & Applic*, vol. 34, no. 14, pp. 11691–11705, Jul. 2022, doi: 10.1007/s00521-022-07061-3.

[5] F. H. Al-Naji and R. Zagrouba, "A survey on continuous authentication methods in Internet of Things environment," *Computer Communications*, vol. 163, pp. 109–133, Nov. 2020, doi: 10.1016/j.comcom.2020.09.006.

[6] Y. Liang, S. Samtani, B. Guo, and Z. Yu, "Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 9128–9143, Sep. 2020, doi: 10.1109/JIOT.2020.3004077.

[7] D. Monschein and O. P. Waldhorst, "Privacy-Preserving and Scalable Authentication based on Network Connection Traces," in *Proc. GI/ITG Conf. on Networked Systems (NetSys)*, Virt. Conf., Sep. 2021. [Online]. Available: https://journal.ub.tu-berlin.de/eceasst/article/download/1175/1109

[8] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Concept and Applications." arXiv, Feb. 13, 2019. Accessed: Mar. 14, 2023. [Online]. Available: http://arxiv.org/abs/1902.04885

[9] T. Piotrowski and Z. Nochta, "Towards a Secure Peer-to-Peer Federated Learning Framework," in *Advances in Service-Oriented and Cloud Computing*, C. Zirpins, G. Ortiz, Z. Nochta, O. Waldhorst, J. Soldani, M. Villari, and D. Tamburri, Eds., Cham: Springer Nature Switzerland, 2023, pp. 19–31. [Online]. Available: http://dx.doi.org/10.1007/978-3-031-23298-5_2

[10] J. A. Peregrina, G. Ortiz, and C. Zirpins, "Towards Data Governance for Federated Machine Learning," in *Advances in Service-Oriented and Cloud Computing*, C. Zirpins, G. Ortiz, Z. Nochta, O. Waldhorst, J. Soldani, M. Villari, and D. Tamburri, Eds., in Comm. in Computer and Information Science, vol. 1617. Cham: Springer Nature Switzerland, 2023, pp. 59–71. doi: 10.1007/978-3-031-23298-5_5.

[11] D. Monschein and O. P. Waldhorst, "mPSAuth: Privacy-Preserving and Scalable Authentication for Mobile Web Applications." 2022. [Online]. Available: https://arxiv.org/abs/2210.04777

[12] D. Monschein, J. A. Peregrina, T. Piotrowski, Z. Nochta, O. P. Waldhorst, and C. Zirpins, "Towards a Peer-to-Peer Federated Machine Learning Environment for Continuous Authentication," in *Proc. 1st IEEE Int. Workshop on Distributed and Intelligent Systems (DistInSys), co-located with 26th IEEE Symp. on Computers and Communications (ISCC)*, Athens, Greece, Sep. 2021. [Online]. Available: http://dx.doi.org/10.1007/978-3-031-23298-5_2

[13] D. Hardt, "The OAuth 2.0 authorization framework," no. 6749. in Request for comments. RFC Editor, Oct. 2012. doi: 10.17487/RFC6749.