FONDAZIONE BRUNO KESSLER
MAGAZINE

DIGITAL ONBOARDING AND GDPR: DISTRIBUTED CONTROL AND USE OF DATA AND DOCUMENTS

October 11, 2021

The first of a series of in-depth studies by CherryChain, an entrepreneurial reality co-located in the FBK headquarters in Povo that collaborates with the Cybersecurity research center of the Bruno Kessler Foundation, directed by Silvio Ranise

Among the processes that have been most affected by digital transformation is the identification and certification of the identity of those who are about to become a customer: the so called “onboarding” step.

The pandemic has certainly emphasized and accelerated the issue of digital onboarding, although it has not yet resolved the main risks associated with traditional procedures, such as: the acquisition of images of paper documents (photos or photocopies), the transposition of data (e.g. help-desk or back-office activities), the misalignment between paper and digital documentation and so on.

On the one hand, we are faced with the risks associated with the manipulation of data between digitized documents and digital identity attributes stored in different organizations. On the other hand, there is the opportunity for every person as a citizen, worker, retiree or student to be able to make use of different tools and digital identity solutions made available.

This takes place both in the public sphere, with SPID and CIE 3.0 Electronic Identity Card, and in the private one, with the identification tools used for access to Remote Banking (Strong Customer Authentication) or with the digital signatures offered by the many certification authorities.

In fact, all the solutions listed above have **onboarding** in common, through which the acquisition of user data and documents and its recognition is obtained, i.e. the proof that combines the identification of the declarant and the information collected to produce and associate an identity (identity proofing).

The methods between the physical channel and the digital channel can change, but in the end they must be able to comply with the same principles of **due diligence** (Know Your Customer or Due Diligence) to demonstrate the consistency between the person and the attributes (data and documents) referring to the coded (e.g. personal data, contract number, contract, user, etc.) and digitized identity (authentication factors).

Why is it not possible for us to shorten onboarding times to access online PA services or open new utilities using the digital identity provided by our bank, or on the contrary use the CIE 3.0 to join a new payment service? Beyond the technical limits that can be solved as already proven in the case of banks with API platforms (API PSD2 or OpenBanking), the different digital identities, even if corresponding to the same qualified person, do not yet allow to be fully used.

This does not refer to the access credentials (the two or more authentication factors), but to the possibility for the person to have control of data and documents made available for onboarding already performed and to reuse and update them in other processes of activation of new services from different operators.

If that was possible, any inconsistencies due to the risks associated with traditional procedures such as errors, omissions, manipulations or misalignments would be gradually identified and resolved by a sort of “social control” or “**chain of custody**” between the person and the public and private operators where digital contracts are subscribed.

This solution does not require a single centralized entity, because it can make use of a distributed and decentralized architecture due to the concatenation of the identity attributes exchanged in the various onboarding. It may seem a paradox, but the GDPR is certainly not a limit to all this, on the contrary it promotes the usability of the data by the owner of the data (the citizen, worker, retiree or student) once a level of consent for the transfer has been set between one operator and another.

CherryChain was founded in 2018 by Carlo Rizzi and Marco Sittoni and deals with research and development in the field of Distributed Ledger Technology and Smart Contract. It collaborates with FBK Cybersecurity research center directed by Silvio Ranise.

PERMALINK

https://magazine.fbk.eu/en/news/digital-onboarding-and-gdpr-distributed-control-and-use-of-data-and-documents/

RELATED MEDIA

- Cherry Chain : https://www.cherrychain.it/
- FBK Cybersecurity : https://www.fbk.eu/it/cybersecurity/

AUTHORS

- Editorial Staff