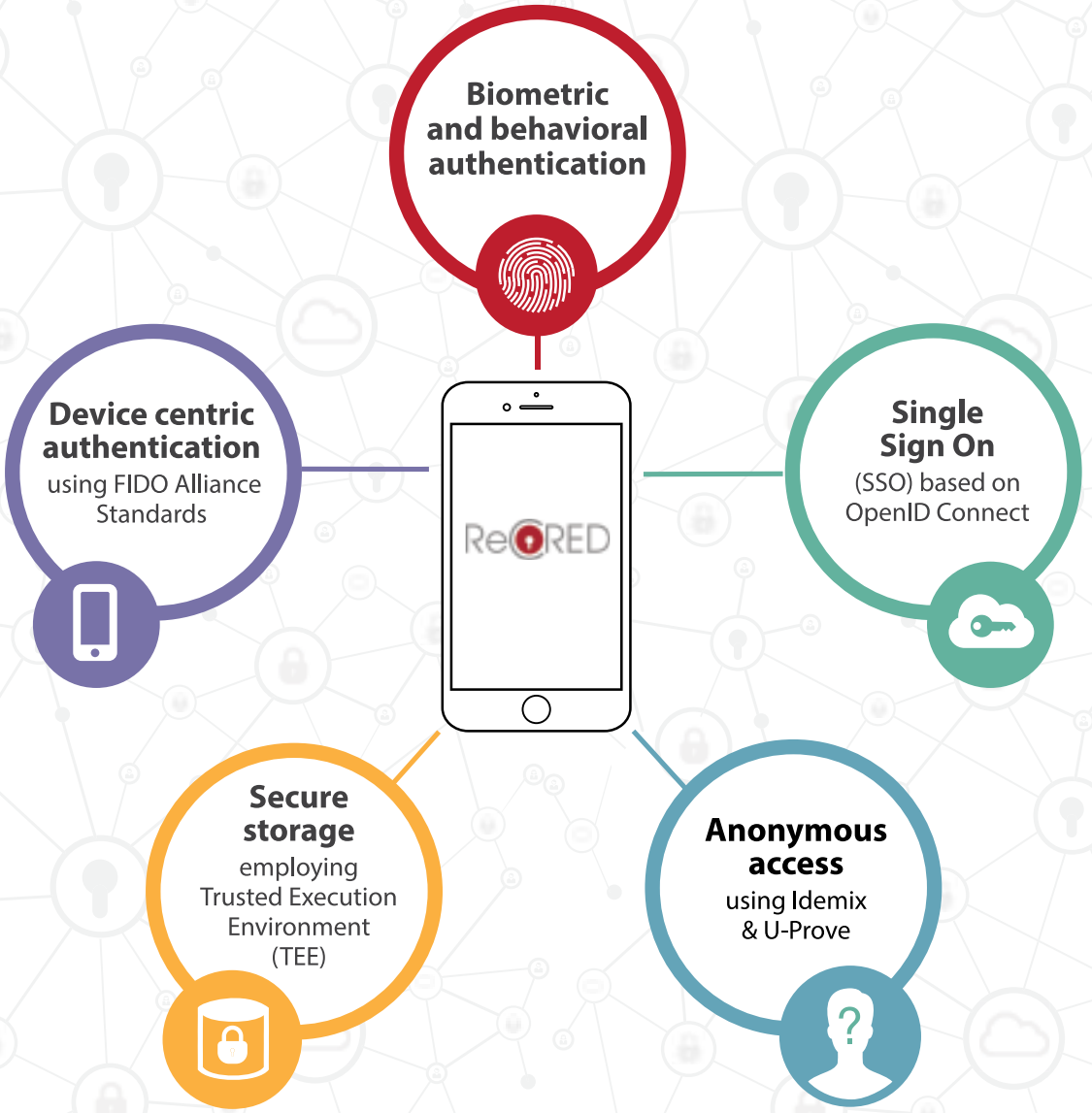
ReCRED

From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control

Makes your digital life **safe** and definitely **easy**!



www.recred.eu

European Commission | Horizon 2020 European Union funding for research & innovation

Privacy minds for your business

The increasing number of Internet connected devices has led to a significant growth in the number and variety of online services. Nowadays individuals are able to receive any kind of information and service over the Internet. However, existing authentication and authorization methods are among the main obstacles for the users that hinder the full enjoyment of such a service. The reason is that, before receiving any online service, the user requires to prove who she/he is. And just after the successful authentication procedure, the online service provider decides which service she/he can access. Usually the authentication is done through providing an Identity number, email address, phone number, etc, by which the online service provider is able to authenticate the user and grant her/him access to the service.

Is there any simpler and privacy-preserving authentication and authorization method?

However, such an authentication and authorization method not only requires the user to carry or remember these personal information (which is not convenient), but also, most importantly, it violates the user's privacy. By contrast, imagine entering a physical store and being asked your personal information before buying anything cash! A store with such policy would probably have a hard time competing against similar stores which do not collect personal details.

Now the important question is: if there is any simpler and privacy-preserving authentication and authorization method. Fortunately, the H2020 ReCRED project gives a "positive" answer to this question through the usage of anonymous credentials. In particular, by adopting "Privacy-Preserving Attribute-Based Access Control (PABAC) ", ReCRED provides a means for the user to access an online service relying on her/his descriptive attributes rather than her/his identity. Owing to the high level of privacy and flexibility provided by ABAC, ReCRED provides a secure, reliable, privacy-preserving and easy-to-use method for online service providers and users to communicate with each other.

PABAC is a logical, fine-grained access control method, which in essence decouples authentication and authorization and protects the user's identity. Authentication is the mechanism which allows an online service provider to acquire who the user is, while authorization is the mechanism through which the online service provider decides which resources the user can access. An online service provider using traditional authentication methods would perform both authentication and authorization. In PABAC, authentication of the users is performed by a trusted authentication authority based on the user's proved attributes, while the authorization of the users is carried out by the online service provider through a defined "access policy" on a set of attributes.
Indeed, upon joining a PABAC system, each user receives a certified private key, from the trusted authentication authority, reflecting her/his descriptive profile attributes. These attributes could reflect different types of personal information: e.g., age, nationality, education level, occupation, etc. and are embedded in the user's private key. On the other hand, the online service provider defines one (or more) access policies on its resources and services, specifying the attributes that a user is required to have to be eligible to access such resources or services. When a user requests to receive a service or a resource, the online service provider does not need to authenticate the user, since due to the usage of PABAC, "only" those users whose attributes encoded in the private key satisfy the attributes in the specified access policy will be authorized to access such a service. Indeed the user employs a pseudonym for each new access request. Moreover, thanks to innovative underlying cryptographic technologies (Idemix, U-Prove and Attribute-Based Encryption), the authentication authority is

not able to track nor recognize the users when these employ their credentials online.

To allow easy integration in existing services, ReCRED's PABAC solution is integrated with the OpenID Connect standard. This integration is based on the use of pseudonyms to protect the user's privacy. A service provider already employing OpenID Connect can thus start deploying PABAC services with minimal effort.

As a use case example of PABAC, consider a scenario of an online course, in which the course lecturer (resource owner) would like to give access to the course material "only" to the students and colleagues of his own department. In such a scenario, traditionally the lecturer requires to lock the resource and either authenticate all the people before accessing the course material (through their identity), or distribute a shared secret between the authorized users (which is not convenient since she/he might need to distribute the share to a large number of users, and any change in the secret should be announced to everybody). In such a scenario, ReCRED provides an efficient solution. The lecturer requires only to define an access policy on the course material in the form of "(student of department X) OR (professor of department X)".

Once the students and professor are joining the department, they receive a credential from the department authority reflecting their descriptive attribute, e.g., student, professor, staff, etc. If and only if a user's attributes associated to her/his credential satisfies the policy specified by the lecture, she/he will be able to access the course material. As it can be seen, the provided solution by PABAC is easy-to-use, privacy-preserving, and efficient from both the lecturer, and the resource user point of view.

As another use case example, consider an online movie repository, or online cinema ticket seller as the resource owner, and a person who is going to download a movie or buy the cinema ticket as the user. Now consider the case that a movie is age-restricted. If the user is willing to download the movie, or buy the ticket for that movie, she/he should prove that her/his age satisfies the restriction policy.

In a traditional authentication scenario, the user requires to provide her/his identity to the resource owner! Again, ReCRED provides a solution for such a scenario which has no equivalent in the physical world: the users can prove in a certified way that their age is above a given threshold without disclosing their actual birth date or any other personal information!

We think that the mechanisms described above allow for scenarios yet to be disclosed. The upcoming General Data Protection Regulation (GDPR) will raise the bar on the level of data protection required from businesses to operate. Moreover, European institutions have expressed their favour to whistleblowing to support accountability in the private and public sector. Finally, it could help digital currencies to become more similar to ordinary cash. All these scenarios could be supported by ReCRED's PABAC.