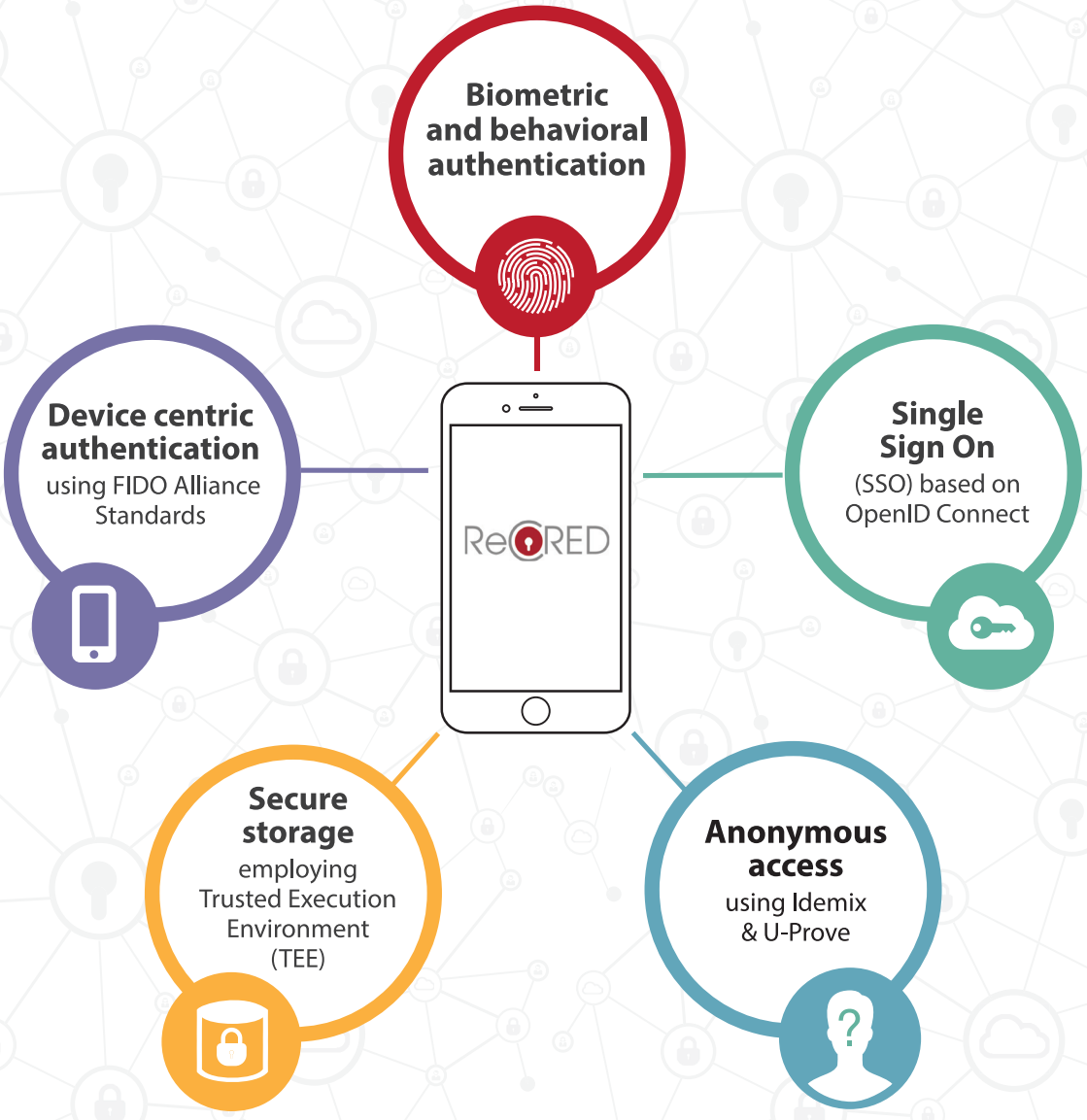
ReCRED

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

Goodbye Passwords. Hello Online Security

Online security today heavily relies on passwords. Each of us has tens of online accounts and it is hard to come up with and remember a strong, unique password for each one of them. As a result, we pick easy to memorize passwords and tend to re-use them across all our accounts[1] , in our personal and business lives. The bad news is that easy to memorize passwords are also easily guessable by bad guys that are set to steal our online identities. Also, using the same password for each account is dangerous because one breach can easily snowball into something far more serious and wide-reaching. Password managers[2] might look as an appealing choice but they come with a high risk that you must be willing to take. They are an obvious target with an astoundingly valuable payout for a successful attacker. The question that rises from the above thoughts is apparent to all of us ReCRED project[3] , addresses many of the above mentioned challenges since one of its goals is to minimize the use of passwords to login and protect online accounts. ReCRED delivers secure yet usable authentication for the web. To this end, ReCRED leverages multi-factor authentication, blending biometric and behavioral authentication so that your online identity is not verified leveraging a secret that you know (i.e., a password) but leveraging "how" you are and behave. Authentication in ReCRED is based on your fingerprint, your face, the way you type on your phone, the way you walk, your whereabouts, or even your browsing behavior on the Internet. Therefore, the good news is that you no longer have to remember a password to enter an online account you own. You simply need to behave as usual and ReCRED will do allthe heavy-lifting to let you access your accounts securely. And there is also a better news. Your biometric features and the way you behave are very difficult for an attacker to mimic. So your accounts are secure and you do not have to worry about remembering passwords. One of the key components of the ReCRED platform is the Behavioral

What should we do to protect our accounts from attackers? Can we find other strong but easy to use modes of authentication?

Authentication Authority (BAA). This web-service provides behavioral-based authentication services and uses smartphones to harvest user behavior data in a way that is non-intrusive for the user and energy-efficient for the device. BAAs are instantiated by telecommunication providers in order to use network information to build the behavioral profile of a user. Incoming and outgoing calls, cell towers that track the device throughout the day, or web browsing habits, are some of the information that a BAA can use to authenticate an individual in a multi-factor authentication framework. Most importantly, such information can be collected by a telecommunication provider acting as a BAA in a manner that is completely transparent to the user. Call logs, cell tower connections and browsing histories are already being collected by telecommunication providers for security and billing purposes. ReCRED leverages such information for authentication purposes. Other behavioral traits that ReCRED leverages, require data collection directly from the smartphone, but are still transparent to the user. In particular, gait and typing behavior are used to verify the identity of the user. Both modalities collect data through the ReCRED app installed on the user device. While the user is walking or typing, the ReCRED app collects data through the sensors available on the smartphone (e.g., accelerometer, gyroscope, etc.) and uploads them to the BAA. Uploaded data is used to build a user profile and, later on, to authenticate the user.

One of the key components of the ReCRED platform is the Behavioral Authentication Authority

BAAs offer authentication services to webservers by extending widely adopted authorization frameworks. In particular, the BAA implements the Application Programmable Interfaces (APIs) of an identity provider as defined by OAuth2[4] and allows webservers (i.e., relying parties) to offload user authentication to the BAA. A key advantage of the BAA compared to other OAuth2 identity providers, is that it can leverage multiple authentication modalities in a single authentication transaction, leveraging two or more authentication factors to serve an authentication request from a relying party.

Authentication at the BAA can happen either proactively or on-demand. The latter is the standard authentication modality of OAuth2 where the identity provider authenticates the user upon receiving a request of a service provider. With proactive authentication, the BAA continuously monitors the behavior or a user to spot deviations from the usual patterns. If suspicious activity is detected, the BAA can either alert the user (e.g., sending an email to her account) or flag the event to the Identity Consolidator, another of the key component of the ReCRED architecture.

Two additional aspects of high importance for ReCRED are authorization and privacy. Through a unified console available at the BAA, users have the power to decide which behavioral data is being collected by a BAA and which data is used towards authentication. A user can decide which relying party can ask for a given authentication modality to the BAA and can browse all authentication requests issued by relying parties. Finally, users can delete their data stored at the BAA. Regarding privacy, ReCRED implements privacy-preserving authentication through anonymous credentials. Anonymous credentials allow the authenticating party to verify the claims on the "attributes" of a prover on a "right to know" basis. For example, purchases of age-restricted goods, require the seller (i.e., the verifier) to check the age of the buyer (i.e., the prover) while any other information (e.g., the buyer's name, last name, etc.) are not required. Traditional authentication mechanisms either disclose a wealth of information to the user or require the authority that certifies the attribute of the user to take active part in the authentication transaction. The anonymous credentials systems implemented by ReCRED allows a user to obtain certified attributes from certification authorities that the user can later utilize in authentication transactions with verifiers. Authentication through an anonymous credential does not disclose the identity of the user, nor can one link two authentication transactions to the same user. From a given credential, a user can decide which attributes to disclose to the verifier and which should be kept hidden. Furthermore, a user can prove predicates of a certified attribute, e.g., showing that her age is between eighteen and thirty without disclosing the actual age.

[1] https://securityintelligence.com/its-time-for-users-to-pony-up-and-quit-reusing-passwords/

[2] http://www.ey.com/Publication/vwLUAssets/Identity_and_access_management_-_Beyond_compliance/$FILE/Identity_and_access_management_Beyond_compliance_AU1638.pdf

[3] http://www.recred.eu/

[4] https://oauth.net/2/


ReCRED


ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS


EXUS


institute
imdea
networks


cnit


Cyprus
University of
Technology


Telefónica
Telefónica I+D


THE
PRODUCTIZERS


certSIGN


wedia


verizon


upcom
Bringing business and IT together


Baker
McKenzie.