The Egomet ecosystem meets all levels of security and support required by the most complex and secure multi-factor authentication services, including PSD2 and eIDAS standards. This datasheet covers the features of Egomet - FIDO.

The Egosystem consists of 3 modules:

**Onboarding**
Egomet - Onboarding is the perfect system to digitize identity, by scanning electronic documents like passports or identity cards. Ideal in recovering the REAL user’s data in a fast and smart way.

**FIDO**
Egomet - FIDO (Fast IDentity Online) provides a secure and simple solution to today’s password problem. The standard is used by the biggest online services companies.

**Mobile Connect**
Egomet - Mobile Connect is a secure universal authentication system. By matching the user to his phone number, Mobile Connect grants access to digital services without having to type in credentials. It can be integrated with Egomet - FIDO, that through the use of biometrics, can add a further security level and a faster user experience.

About us:

With over 20 years of expertise, Movenda has become leader in the mobile identity market, focusing on development of innovative carrier-grade software platforms dedicated to identity management and remote management.

Movenda works within the major international software standardization committees such as GSMA and FIDO Alliance.
Egomet - FIDO

FIDO is the world's largest ecosystem for standards-based, interoperable authentication. The FIDO standard is the outcome of the FIDO Alliance's members' contribution. In order to make websites and online services easy to use, FIDO takes advantage of the native security features and biometrics built in mobile devices. It provides a multi-factor authentication system reducing the problems associated with the creation and preservation of the many credentials that are crucial in the digital world.

They and many others already use FIDO:

How it works:

Authenticator set up

The mobile device is certified through the detection of the user's biometric data. Simultaneously, a private and a public key are enabled. The private key is always kept exclusively within the device.

Online authorisation

During the authentication procedure on an online service (RP - relying party) the client sends, towards a FIDO server, a request containing the details of the transaction that the user wishes to complete. The server verifies the identity of the device and authorises the client through the challenge process, based on a public key infrastructure (PKI).
Egomet - FIDO contains 2 modules:

**Egomet Client/Authenticator Combo**
Mobile app developed for both Android and iOS platforms. The authenticator detects the authentication systems available on the device, gathers and stores securely the biometric data. The client enables the private key stored in the device, in order to sign the transactions that are sent to the server.

**Egomet FIDO® Server**
The fastest and easiest way to manage multi-factor authentication. It manages public keys and verifies the signed transactions generated by the user’s device. The security of the process is guaranteed by the fact that the server doesn’t hold at no time the client’s private key.

**Egomet is FIDO® certified**
The Egomet FIDO® Server and Egomet Client/Authenticator Combo modules, are FIDO Universal Authentication Framework (UAF) certified.