BioShare available with FIDO2-standard for MFA

Passwordless authentication with biometrics and, at the same time, maximum encryption and security of the biometric features – that´s the combination of FIDO2 and **BioShare**. Multi-factor authentication has never been so secure.

Biometric authentication is extremely secure – of course. More secure than logging in with a password - and a biometric feature such as a fingerprint cannot be forgotten or misplaced. That's why **BioShare**, the biometrics management suite and the digital identity management tool from TWINSOFT biometrics, which can be configured for almost every conceivable application - is a secure and at the same time user-friendly possibility to take authentication in your own company to the next level.

All the advantages of biometrics and a further security upgrade

Reservations regarding the disclosure of biometric features are understandable, no matter how well they are encrypted. And in addition, more secure than a simple biometric authentication is, of course, an authentication that combines biometrics with other factors (MFA). The maximum of security is a multi-factor authentication with the FIDO2 standard, and that is exactly what we can cover with **BioShare** now.

FIDO2 stands for Fast IDentity Online 2 and is an open standard for simple, secure, and passwordless multi-factor authentication, based on public key cryptography, whereby the private key is bound to a piece of hardware and secondary factors such as biometric features, PINs, or gestures are used.

TWINSOFT *biometrics* GmbH & Co. KG
Europaplatz 2 64293 Darmstadt
Tel.: 06151 39756-0 Fax: 06151 39756-50
info@twinsoft-biometrics.de
www.twinsoft-biometrics.de

TWINSOFT *biometrics*

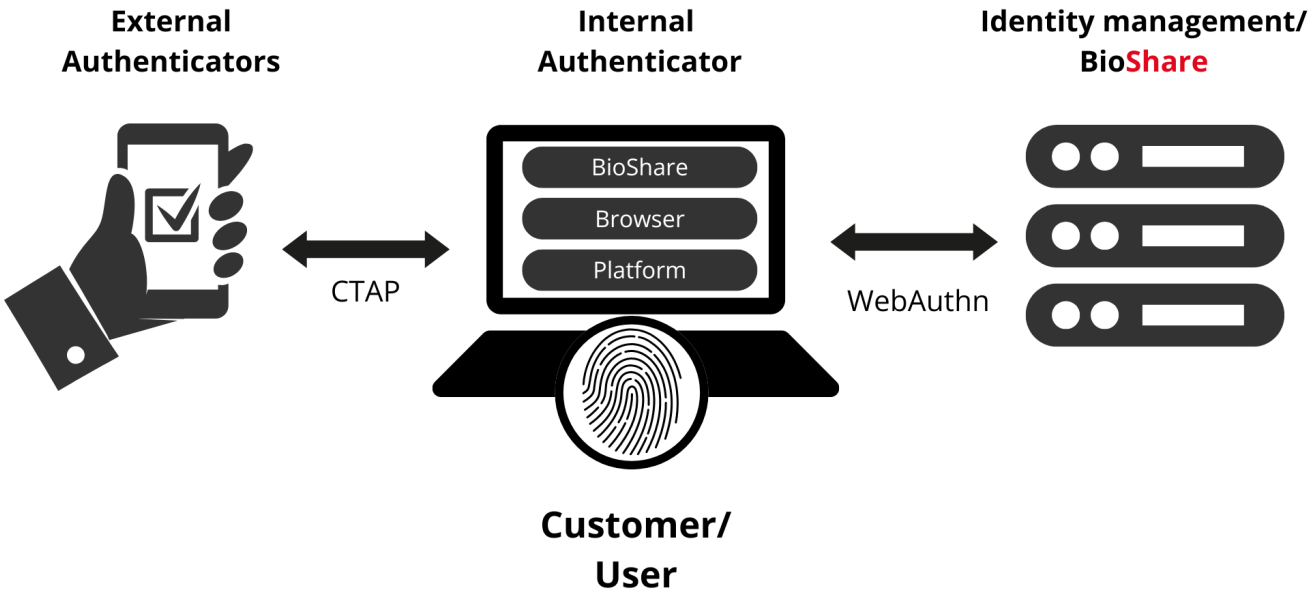
Man-in-the-middle attacks are prevented

FIDO2 provides particularly good protection against “man-in-the-middle” attacks, in which an attacker in the communication between two parties (i.e., between the party who wants to authenticate and the service that verifies the authentication) fakes the identity of one of the parties in order to intercept data. With the FIDO2 standard, this is no longer possible.

To put it simply, a unique digital key pair is created for each registered person. So every unique digital key pair, consisting of a private and public key, is generated for each registered person. The private key remains on the sensor, for example, the smartphone. The public key is sent to the service where the person wants to authenticate themselves.

No transmission of sensitive data

An application example would be: Person X confirms on the **BioShare** sensor, for example, their own smartphone with their fingerprint identity. The fingerprint releases the private key stored on the device, and the response is encrypted with it. Fingerprint and private key always remain on the device.
Confirmation of identity is then carried out using the public key, and the response can only be sent with the corresponding key stored with precisely this service.
The two individual keys are stored at different locations, which can only confirm each other, and the hardly forgeable biometric feature, which, however, is not transmitted anywhere, ensures that no attacker can somehow gain access to the data during communication, to feign a false identity.



TWINSOFT *biometrics* GmbH & Co. KG
Europaplatz 2 64293 Darmstadt
Tel.: 06151 39756-0 Fax: 06151 39756-50
info@twinsoft-biometrics.de
www.twinsoft-biometrics.de

TWINSOFT *biometrics*