BioShare jetzt auch mit FIDO2-Standard für MFA

Passwortlose Authentifizierung mit Biometrie und dabei maximale Verschlüsselung und Sicherung der biometrischen Merkmale – das ist die Kombination aus FIDO2 und **BioShare**. Mehrfaktorauthentifizierung war noch nie so sicher.

Biometrische Authentifizierung ist extrem sicher – keine Frage. Sicherer als die Anmeldung mit einem Passwort allemal – und ein biometrisches Merkmal wie der Fingerabdruck kann auch nicht vergessen oder verlegt werden. Deswegen ist **BioShare**, die Biometrie-Management-Suite und das digitale Identitäten-Verwaltungstool der TWINSOFT *biometrics*, welches für nahezu jeden denkbaren Anwendungsfall konfiguriert werden kann, auch eine sichere und gleichzeitig anwenderfreundliche Möglichkeit, Authentifizierungen im eigenen Unternehmen auf die nächste Stufe zu hieven.

Alle Vorteile der Biometrie und ein weiteres Sicherheitsupgrade

Vorbehalte gegenüber der Weitergabe der eigenen biometrischen Merkmale, egal wie gut verschlüsselt sie dabei sind, sind aber verständlich. Und außerdem: Sicherer als eine einfache biometrische Authentifizierung ist natürlich eine Authentifizierung, die die Biometrie mit weiteren Faktoren kombiniert (MFA). Und maximal sicher wird eine solche Multifaktorauthentifizierung mit dem FIDO2-Standard – und genau das ist jetzt auch mit **BioShare** möglich.

FIDO2 steht für Fast IDentity Online 2 und ist ein offener Standard zur einfachen, sicheren und passwortlosen Mehrfaktor-Authentifizierung, auch im World Wide Web, basierend auf der Public-Key-Kryptografie. Wobei der private Schlüssel an eine Hardware gebunden ist und Zweitfaktoren wie biometrische Merkmale, PIN oder Gesten zum Einsatz kommen.

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*

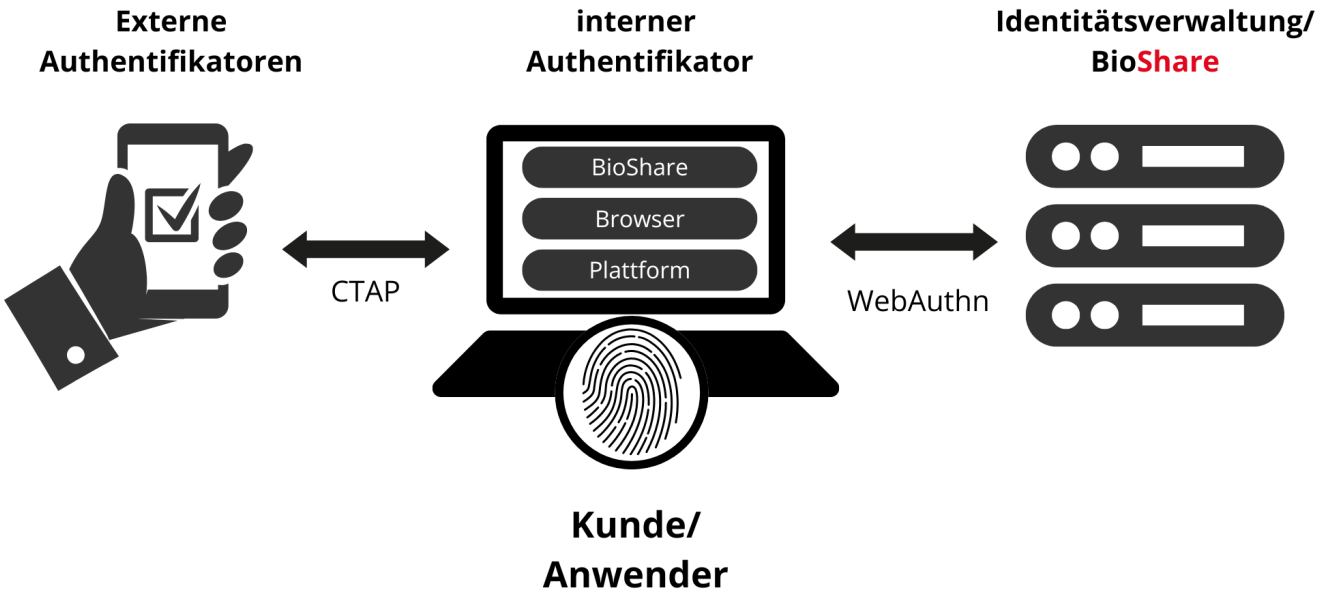
Man-in-the-Middle-Angriffe werden verhindert

FIDO2 schützt besonders gut vor „Man-in-the-Middle“-Angriffen, bei denen ein Angreifer in der Kommunikation zwischen zwei Parteien (also zwischen demjenigen, der sich authentifizieren will, und dem Dienst, der die Authentifizierung überprüft) die Identität einer der Parteien vortäuscht, um Daten abzugreifen. Mit dem FIDO2-Standard ist das nicht mehr möglich.

Vereinfacht ausgedrückt wird für jede registrierte Person ein einzigartiges digitales Schlüsselpaar bestehend aus privatem und öffentlichem Schlüssel generiert. Der private Schlüssel verbleibt auf dem Sensor, zum Beispiel dem Smartphone. Der öffentliche Schlüssel wird an den Dienst gesendet, wo die Person sich authentifizieren will.

Keine Übermittlung sensibler Daten

Ein Anwendungsbeispiel wäre: Person X bestätigt auf dem **BioShare**-Sensor, zum Beispiel dem eigenen Smartphone, mit Ihrem Fingerabdruck ihre Identität. Der Fingerabdruck gibt den auf dem Gerät hinterlegten privaten Schlüssel frei und die Antwort wird damit verschlüsselt. Fingerabdruck und privater Schlüssel verbleiben dabei immer auf dem Gerät. Die Bestätigung der Identität erfolgt dann über den öffentlichen Schlüssel – die Antwort kann nur mit dem entsprechenden, bei genau diesem Dienst hinterlegten passenden Schlüssel bestätigt werden. Die zwei jeweils an verschiedenen Orten hinterlegten individuellen Schlüssel, die nur einander bestätigen können, und das kaum fälschbare biometrische Merkmal, das aber nirgendwohin übertragen wird, sorgen dafür, dass kein Angreifer sich irgendwie während der Kommunikation der Daten bemächtigen kann, um eine falsche Identität vorzutäuschen.



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*