FIDO2 als Login-Möglichkeit

Es gibt eine neue Möglichkeit, die wir Ihnen zusätzlich zum Login mit Key-Datei und TOTP anbieten. **Sie heißt FIDO2**.
(Diese Technik wird u.a. auch Passkeys genannt.)

Diese wesentliche Neuerung bezüglich der Sicherheit für den Login bei BOLLE beruht auf der Einführung des Sicherheitsstandards FIDO, dem sich alle großen Webservices angeschlossen haben und diesen auch umsetzen werden und der somit demnächst auch in weiteren Bereichen im Internet immer wichtiger wird.

Doch zunächst zur Relevanz für den Login bei BOLLE:
Für das Personal gab es bisher drei Login-Möglichkeiten: Key-Datei, TOTP oder die Einrichtung eines vertrauenswürdigen Geräts.

Die meisten Ihrer Kolleg:innen benutzen eines der ersten beiden Verfahren (**Key-Datei oder TOTP**), an denen sich auch in Zukunft nichts ändern wird. **Für diese Kolleg:innen besteht also aktuell kein Handlungsbedarf**.

All diese Möglichkeiten haben gemeinsam, dass sie das Sicherheitskriterium einer sogenannten Zwei-Faktor-Authentisierung (2FA) erfüllen. Die bisherigen Login-Verfahren für BOLLE sind alle softwaregestützt.

Das Bundesamt für Sicherheit in der Informationstechnik stellt fest, dass „vor allem hardwaregestützte Verfahren ein hohes Maß an Sicherheit“ bieten (Quelle).

An solch einem hardwaregestützten Verfahren als zweiten Faktor haben wir in den vergangenen Monaten gearbeitet und wollen Ihnen die Möglichkeit geben, dieses Login-Verfahren einzusetzen. **Das neue Verfahren heißt FIDO2 (Fast Identity Online 2.0).**

Der Login mittels FIDO2 erfolgt geräte- und browsergenau. Dabei wird im Browser mittels der vorhandenen Technik des Geräts der zweite Faktor direkt gespeichert. Selbst wenn er ausgelesen werden könnte, funktioniert dieser nur auf dem Gerät und dem Browser, auf dem er eingerichtet wurde.

Die meisten aktuellen Geräte und Browser unterstützen solch eine FIDO2-Einrichtung. Auch die durch die Senatsverwaltung ausgegebenen Diensttablets könnten das theoretisch. Bisher hat die zuständige Stelle die Möglichkeit hierzu aber noch nicht aktiviert.
(NB: Auf den Diensttablets funktioniert für eine mögliche FIDO2-Nutzung nur ein sogenannter YubiKey, eine Art USB-Sicherheitskey. Der Login auf den Diensttablets funktioniert aber auch weiterhin mit Key-Datei oder TOTP.)

Auf diesen Hilfeseiten erklären wir ausführlich,

1. **wie Ihre Admins FIDO2 als Login-Verfahren für Ihre Kolleg:innen aktivieren können** und
2. **wie Sie FIDO2 auf Ihren Geräten einrichten und nutzen**.

Im Zuge dieser Umstellung und der Veränderung der Sicherheitsanforderungen mussten wir die bisherige Möglichkeit der Einrichtung vertrauenswürdiger Geräte mittels TOTP deaktivieren. Diese Form der 2FA konnte bis jetzt auf vertrauenswürdigen Geräten zeitweise übersprungen werden. Dies führt zu einer Verringerung der Sicherheit. Daher kann der Login mittels eines vertrauenswürdigen Gerätes ab sofort nicht mehr erfolgen. **Mit FIDO2 können die Kolleg:innen jedoch ebenfalls „vertrauenswürdige Geräte“ einrichten,** nur handelt es sich hierbei um eine vielfach sicherere Möglichkeit.

> Wichtig: **Für Kolleg:innen, die den Login mittels Key-Datei und TOTP nutzen, ändert sich nichts.** Sie können sich weiterhin normal mit ihrer Key-Datei oder TOTP einloggen. Erst wenn ein persönlicher FIDO2-Key erstellt wurde, geht der Login nur noch über FIDO2 sowie zusätzlich auch weiterhin mit der Key-Datei. Ein Login mittels TOTP ist dann nicht mehr möglich. Weitere Informationen finden Sie auf den oben genannten Hilfeseiten.

Wir hoffen, wir konnten Ihnen die ziemlich technische Seite des neuen sicheren Loginverfahrens gut erläutern und hoffen vor allem, dass Sie unseren Anspruch an höchsten Datenschutz und Datensicherheit nachvollziehen und teilen.

Wie bereits erwähnt: **Die Login-Verfahren mit Key-Datei und TOTP bleiben bestehen.** Wenn Sie möchten, probieren Sie gerne einmal die neue FIDO2-Technik aus. Die Erst-Einrichtung wirkt vermutlich erst etwas abschreckend; wir versuchen den Prozess für Sie und Ihre Kolleg:innen so einfach wie möglich zu gestalten.

> **Wenn Sie das Verfahren ausprobieren möchten, sprechen Sie Ihren Admin an der Schule an.**

Version #5
Erstellt: 16 August 2022 07:07:54 von BOLLE Support
Zuletzt aktualisiert: 16 Dezember 2022 16:30:16 von BOLLE Support