Logindaten Personal

In BOLLE haben die Admins die Möglichkeit, die Kolleg:innen bezüglich der Logindaten zu unterstützen. So kann z.B. bei einem Verlust von Sicherheitsmerkmalen entsprechend reagiert werden. Die Einstellung hierzu finden Sie in der Menüleiste bei *Admin* unter der Auswahl von *Logindaten Personal.*

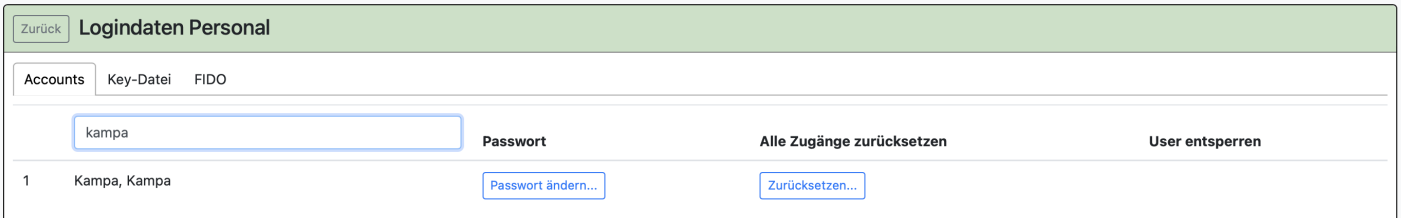
Inhalt

1. Allgemeines
2. Accounts
3. Key-Datei
4. Verwaltungskey
5. TOTP
6. FIDO
7. Häufige Fragen

1. Allgemeines

Auf dieser Seite verwalten Sie die Logindaten des Personals. Sie können

- Passwörter ändern
- Zugänge zurücksetzen
- gesperrte User entsperren
- Key- und Verwaltungskey-Dateien erstellen
- die Initialzugänge für alle Kolleg:innen gleichzeitig herunterladen
- ein eingerichtetes TOTP löschen
- die Key-Erstregistrierung herunterladen
- neue FIDO2-Registrutierungsdaten erstellen
- bereits angelegte FIDO2-Zugänge löschen



Bitte beachten Sie, dass Sie diese Registrierungsdateien für Key-Dateien oder FIDO2-Keys **- NICHT-** per E-Mail versenden. Die Keys sollten ausschließlich direkt vor Ort ausgegeben werden.

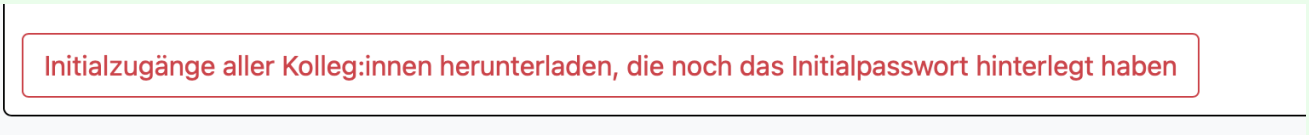
Kolleg:innen, die sich zum ersten Mal bei BOLLE einloggen, können den Key bei der ersten Einrichtung einmalig selbst herunterladen. Dies ist möglich, weil die Kolleg:innen zu diesem Zeitpunkt keinerlei Kursbücher oder andere Systemrechte erworben haben. Bei bereits registriertem und auf BOLLE aktivem Personal müssen mehr Sicherheitsaspekte berücksichtigt werden.

Wenn Sie Personal ein neues Intitialpasswort ausstellen möchten, müssen Sie nicht unbedingt den Account zurücksetzen. Vergeben Sie einfach ein neues Initialpasswort. Die Key-Datei bleibt dann erhalten; so auch alle anderen eingerichteten Zugänge.

Falls Sie einen Personal-Account bereits zurückgesetzt haben, dann laden Sie sich die Key-Datei herunter, übergeben diesen vor Ort (nicht per E-Mail!) an die Kolleg:in und setzen unter dem Reiter Accounts das Passwort zurück auf ein anderes Initialpasswort. Die Kollegin kann das PW dann beim ersten Login ändern.

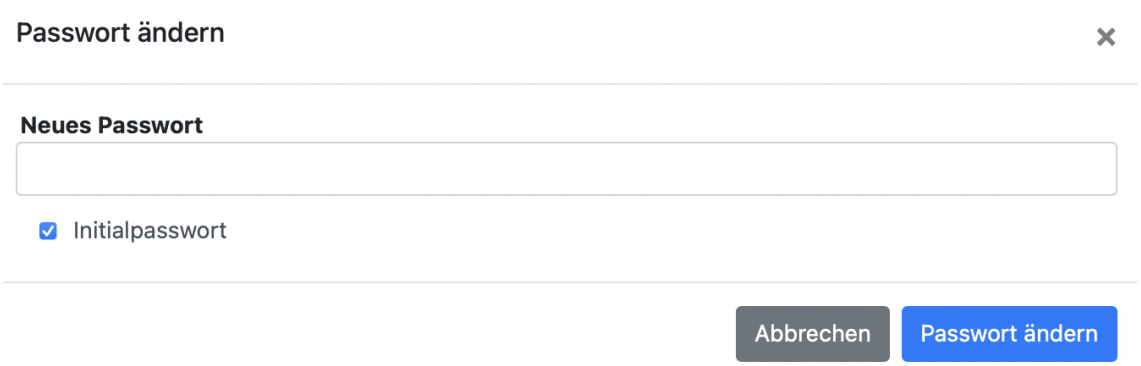
Nach erstmaligem Gebrauch der Initialzugangs-PDF wird keine weitere PDF mehr erstellt. Bitte verfahren Sie so, wie oben beschrieben.

Bei der Ersteinrichtung von BOLLE an Ihrer Schule bietet es sich an, wenn Sie die Initialzugänge aller Kolleg:innen herunterladen können, bei denen noch das Initialpasswort vermerkt ist. Das können Sie über den Reiter *Accounts* machen. Scrollen Sie dann nach ganz unten, wo Sie eine Schaltfläche für den Download finden:

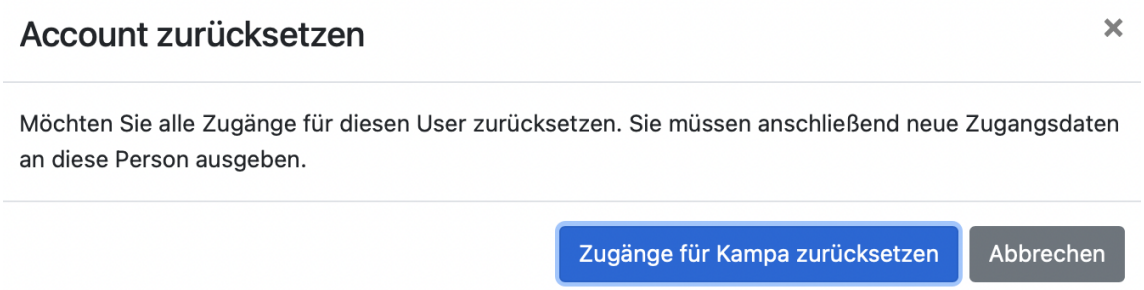


2. Accounts

Unter dem Reiter *Accounts* sehen Sie alle Accounts des Personals. Sie können **Passwörter ändern** und dabei auch entscheiden, ob es sich um ein sogenanntes **Initialpasswort** handelt. Falls ja, dann wird der Nutzer nach erfolgreichem Login um ein neues Passwort gebeten.



Sollte ein kritisches Ereignis eingetreten sein, bei dem unklar ist, ob ein Account weiterhin nur von der befugten Person genutzt werden kann, so können Sie den **Zugang hier direkt zurücksetzen** .

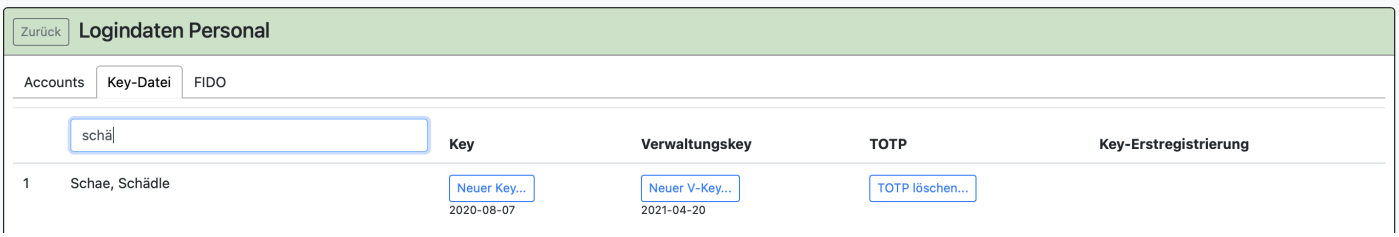


Wenn ein Nutzer wiederholt falsche Passwörter verwendet, kann es sein, dass der Zugang vom System geperrt wird. Sie können über diese Ansicht **User wieder entsperren**.

> **Tipp:** Sie können in das Feld oben das Kürzel oder den Nachnamen des Personals eingeben, um eine Person schneller zu finden.

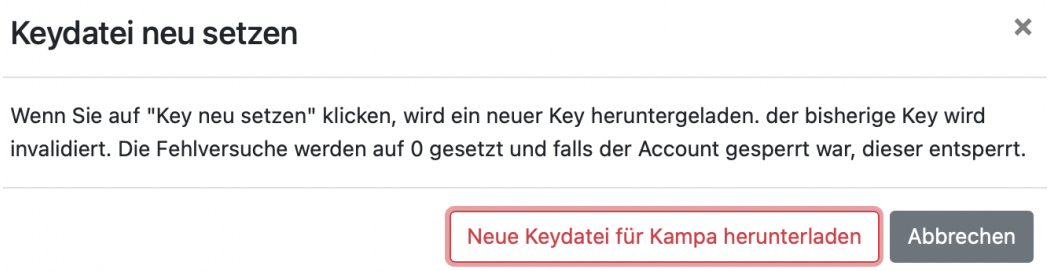
3. Key-Datei

Unter dem Reiter *Key-Datei* finden Sie die allgemeine Key-Datei, den Verwaltungskey, TOTP und die Key-Erstregistrierung (PDF Erstlogin).



Sobald ein Datum unter einem Key-Feld steht, wissen Sie, seit wann der Key gültig ist.

Wenn Sie auf *Neuer Key* klicken, können Sie einen neuen Key oder V-Key erstellen. Dabei wird der alte Key sofort ungültig.



> Wenn Kolleg:innen um einen neuen Key bitten, sollten Sie diesen niemals per E-Mail versenden. Geben Sie die Key-Datei persönlich weiter. Weisen Sie die Kolleg:innen darauf hin, dass die Key-Datei im besten Fall nicht dupliziert wird, sondern sich z.B. auf einem USB-Stick befindet.

> Mit Klick auf das Feld *PDF Erstregistrierung* wird eine PDF erstellt, die Sie neuen Kolleg:innen geben können.

4. Verwaltungskey

Bei einigen Kolleg:innen sehen Sie die Schaltfläche *Verwaltungskey*. Hierbei handelt es sich um einen weiteren Schlüssel, der benötigt wird, wenn weitreichende Nutzerrechte im System vorliegen. Der normale Key ermöglicht unterrichtsalltägliche Eintragungsmöglichkeiten, so wie sie fast alle Lehrkräfte und weiteres pädagogisches Personal brauchen. Die Rechte dieser Personalgruppe sind systemweit deutlich eingeschränkt. Das Verwaltungspersonal, also die Kolleg:innen des Sekretariats, die Verwaltungsleitung, Mittel- und Oberstufenkoordination und die Schulleitung, hat jedoch weitreichende Lese- und Schreibrechte im Programm. Viele, bei einigen Kolleg:innen mit umfangreichen Verwaltungstätigkeiten auch unterrichtliche Aufgaben, bei denen häufige Ortswechsel die Regel sind, werden so in die mobile Unterrichtsarbeit (normaler Key) und die weitreichendere Verwaltungsarbeit (lokaler Verwaltungskey) getrennt.

> Auch nichtpädagogisches Personal muss sich das erste Mal in BOLLE mit dem normalen Key einloggen! Stellen Sie danach den Verwaltungs-Key aus.

Im sichersten Fall wird der Verwaltungskey nur an geschützten, persönlichen Dienstrechnern vor Ort verwendet. Der Zugang zu BOLLE für unterrichtliche Aufgaben kann dabei weiterhin mit dem normalen Key auf einem USB-Stick oder mittels TOTP erfolgen. Auch dabei bleibt die sicherheitsrechtliche Vorgabe der Zwei-Faktor-Authentizierung erfüllt.

Bitte informieren Sie Ihr Verwaltungspersonal regelmäßig über diese Sicherheitsaspekte.

5. TOTP (Time-based One-time Password)

Unter dem Reiter Key-Datei finden Sie auch die Möglichkeit, einen bereits erstellten TOTP-Zugang zurückzusetzen.

Diese Aktion nutzen Sie, wenn

- Ihre Kolleg:innen Probleme mit dem TOTP haben und Sie um Zurücksetzen der Funktion bitten oder
- Ihre Kolleg:innen Ihnen ein gestohlenes Gerät melden.

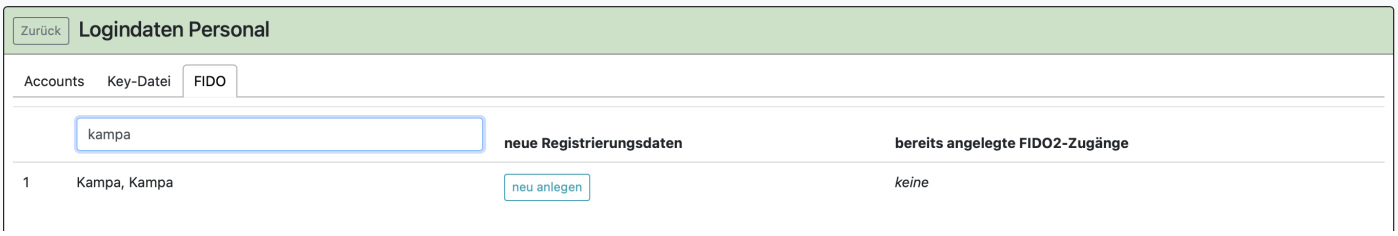
Bei einigen Betriebssystemen kann die Erstellung von TOTP-Zahlencodes integriert stattfinden. Apple ermöglicht dies zum Beispiel. Das kann vor allem für Mac- und iPad-User hilfreich sein. Hier finden Sie mehr Informationen von Apple für das iPad.

6. FIDO

BOLLE unterstützt eine der sichersten Login-Methoden für Webservices: Fast Identity Online 2.0 (FIDO2). Sichere Login-Verfahren nutzen neben Username und Passwort noch einen weiteren Faktor. Diese Zwei-Faktor-Authentisierung (2FA) funktioniert z.B. mittels der oben beschriebenen Key-Datei oder dem TOTP. Diese beiden Varianten sind softwaregestützt. Es gibt aber nun auch die Möglichkeit, eine hardwaregestützte 2FA einzurichten: FIDO2. Hardwaregestützte 2FA gelten als noch sicherer (vgl. Bundesamt für Sicherheit in der Informationstechnik).

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

Diese Art von "Passwörtern" werden auch **Passkeys** genannt.



Klicken Sie auf den Reiter *FIDO* und dort unter *Neue Registrierungsdaten* auf *neu anlegen*. Es wird sofort eine Registrierungdatei erstellt, die Sie herunterladen können.



Geben Sie diese Datei an den berechtigten User weiter. Die Datei wird in etwa so aussehen:

Kampa

Registrierungsdaten BOLLE (FIDO2)

Ihr Kürzel: **Kampa**

Um ein neues Gerät mit FIDO2 zu registrieren, gehen Sie bitte auf die folgende Seite: https://ihreschule.bolle.schule/fido. Sie benötigen den folgenden Registrierungscode:

ABCD :: A2B1 :: ABCD :: 2BC4 :: ABCD :: ABCD

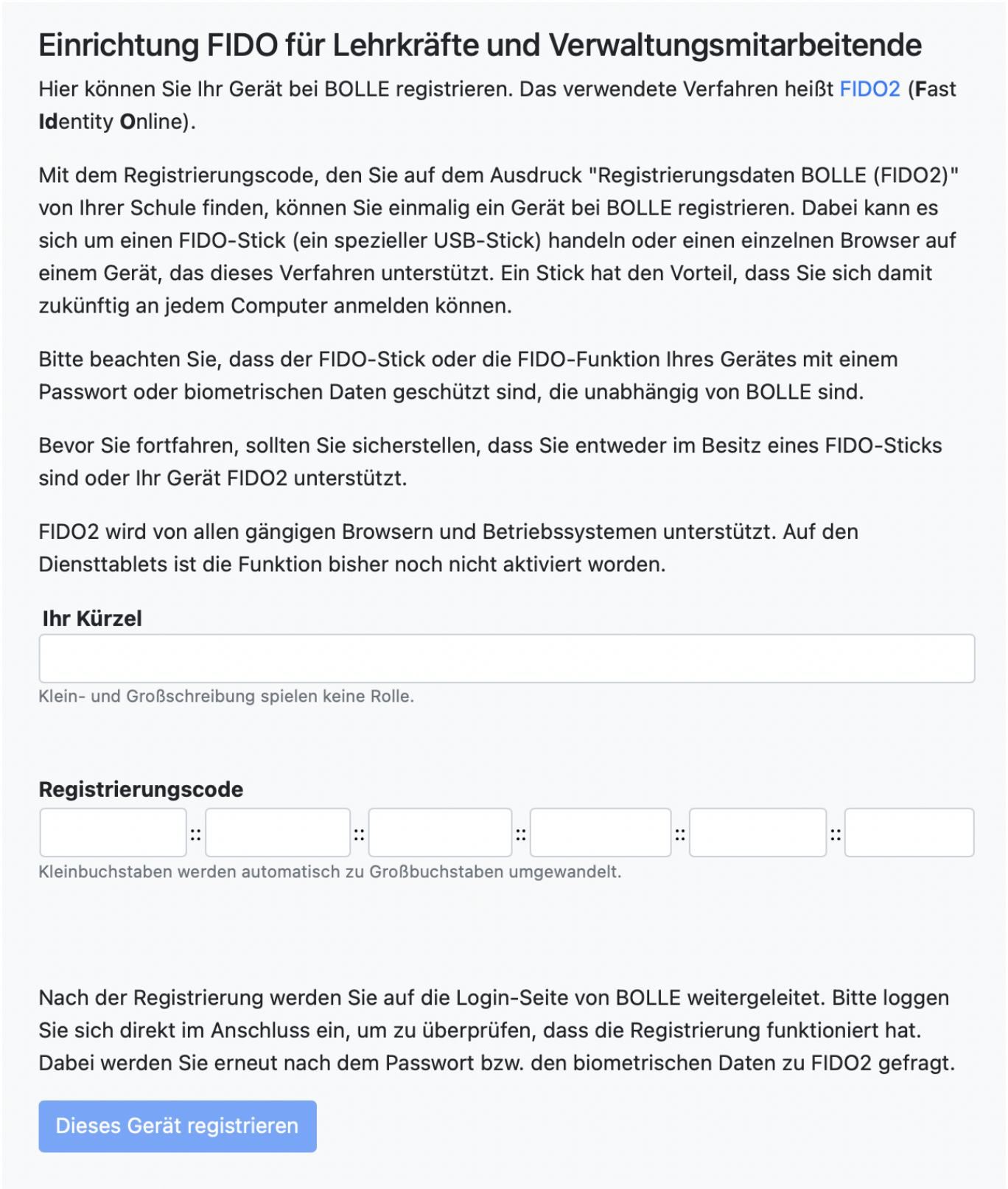
Ihr bisheriges Passwort behält seine Gültigkeit.

Diese Daten sind gültig bis zum 19.08.2022 um 18:00 Uhr.

Wir wünschen Ihnen einen guten Start!

Falls Sie dieses Dokument digital erhalten haben, können Sie hier den Registrierungscode in die Zwischenablage kopieren und in das erste Feld einfügen: ABCDA2B1ABCD2BC4ABCDABCD

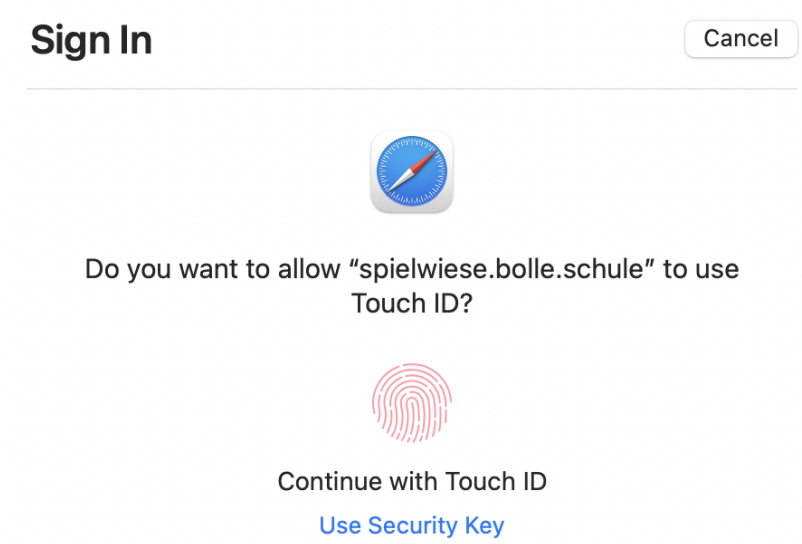
Der hier angegebene Schlüssel (ABCD-A2B1-...) **kann nur einmal** für einen Browser auf einem ganz bestimmten Gerät verwendet werden. Auf dem Gerät, auf dem FIDO2 als hardwaregestützte 2FA eingerichtet werden soll, besucht der User die BOLLE-Webseite der Schule mit der Ergänzung */fido* (wie in der Datei angegeben). Es öffnet sich folgende Seite:



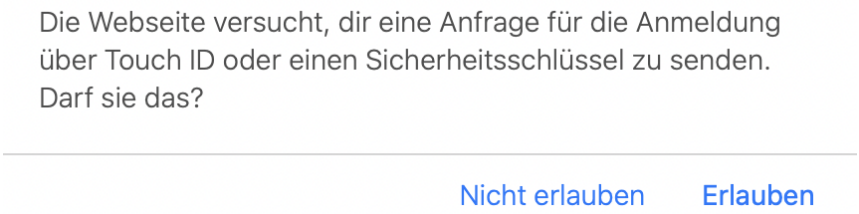
Auf der Seite gibt der User sein Kürzel und den Registrierungscode ein. Danach klickt man auf *Dieses Gerät registrieren*.

Je nach Betriebssystem und Browser wird man dann gefragt, wie man weiter verfahren möchte. Hier ein paar Beispiele:

Safari auf einem Mac mit Touch ID:



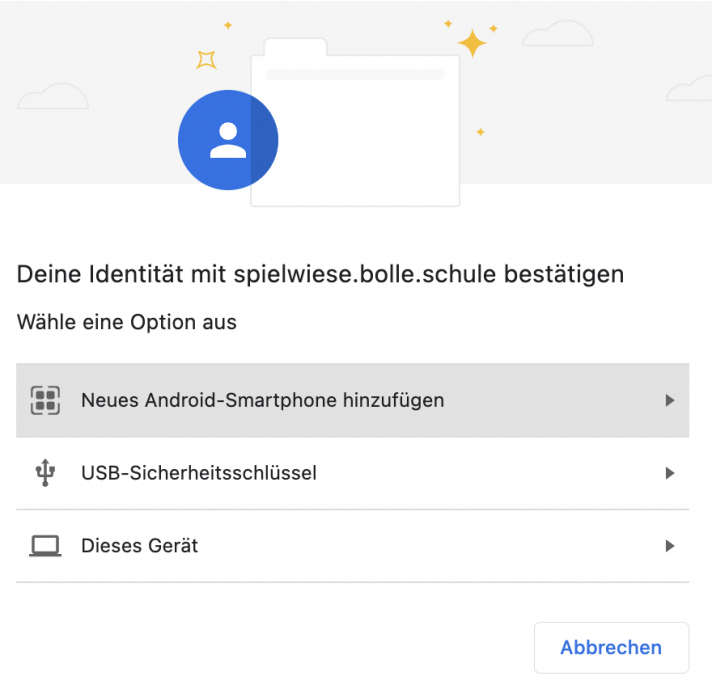
Man nutzt dann z.B. Touch ID zur Bestätigung.



Und klickt auf *Erlauben*.

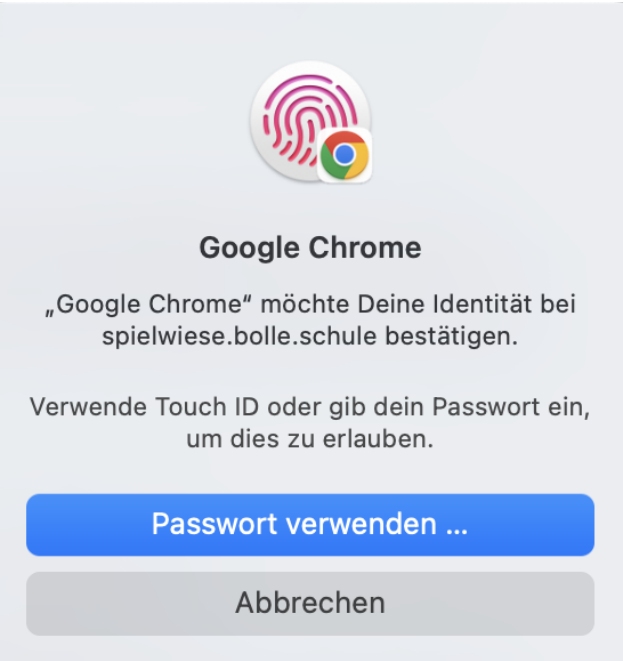
> "Use Security Key" meint hier einen USB-Sicherheitsschlüssel, wie z.B. einen YubiKey. (Was ist ein YubiKey?)

Chrome auf einem Mac mit Touch ID:



Man klickt auf *Dieses Gerät*. (Es sei denn, man will die Methode via USB-Sicherheitsschlüssel / FIDO2-Key / YubiKey verwenden, was auch möglich ist.)

> Auch hier wird z.B., wie im vorherigen Beispiel mit "Security Key" die Einrichtung auf einem USB-Sicherheitsschlüssel als Option vorgeschlagen. Wenn Ihr Gerät FIDO2 unterstützt, klicken Sie besser auf "Dieses Gerät".



> Achtung: Die meisten Geräte und Browser unterstützen FIDO2. Auf dem Diensttablet der Berliner Senatsverwaltung ginge es theoretisch auch, jedoch wurde die Funktion von der zuständigen Stelle noch nicht freigegeben. Der Login auf dem Diensttablet funktioniert deshalb vorerst am besten per Key-Datei oder TOTP. Auch die Verwendung eines

sogenannten FIDO2-Keys / YubiKeys wäre möglich (siehe nächster grüner Kasten).

Der Registrierungscode für den Login mit FIDO2 kann übrigens auch durch externe Hardware erfolgen. Hier eignen sich z.B. sogenannte FIDO2-Keys oder YubiKeys. Diese können dann mithilfe eines USB-Ports für die Authentisierung genutzt werden. Mehr Informationen zu YubiKeys finden Sie hier auf einer externen Webseite.

Wenn User mehrere Geräte mit FIDO2 nutzen möchten, müssen sie die erste FIDO-Registrierung abgeschlossen haben (siehe nächster Absatz), bevor man eine neue starten kann. Danach können die Admins ein weiteres FIDO2-Registrierungsdatenblatt erstellen. Der Login mittels Keydatei funktioniert weiterhin, sofern eine Keydatei ausgestellt wurde.

Nach erfolgreicher Registrierung sieht das Ganze unter dem Reiter *FIDO* so aus:



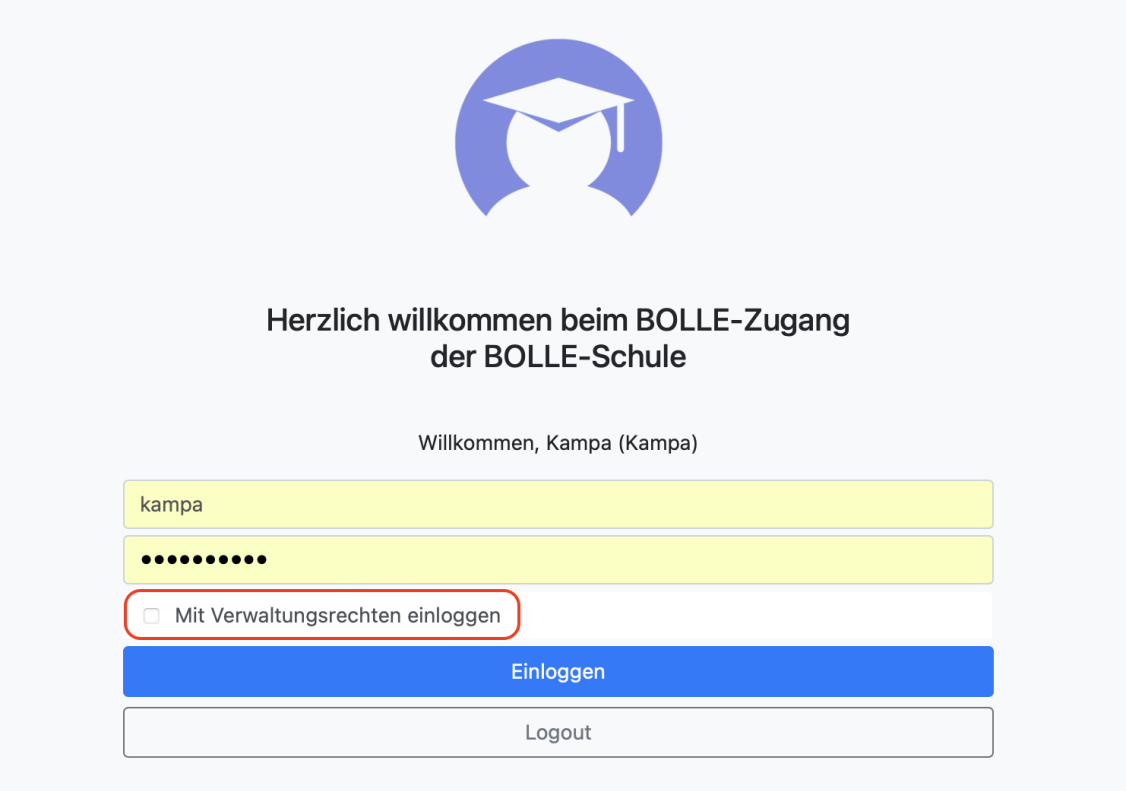
Es können beliebig viele FIDO2-Zugänge erstellt werden. Bevor neue Registrierungsdaten ausgestellt werden können, muss ein bereits erstellter Registrierungscode erfolgreich genutzt worden, gelöscht worden oder abgelaufen sein. Kolleg:innen, die mehrere FIDO2-Zugänge benötigen, müssen die Geräte nacheinander registrieren.

Sobald ein FIDO2-Zugang eingerichtet wurde, ist der Login mit TOTP ruhend gestellt. Er wird erst dann wieder aktiviert, wenn alle FIDO2-Zugänge deaktiviert wurden. Der BOLLE-Login funktioniert also entweder per Key-Datei und TOTP **oder** Key-Datei und FIDO2.
Der Zugang per Key-Datei bleibt also weiterhin möglich, sofern eine Key-Datei ausgestellt wurde.

Löschen Sie bereits eingerichtete FIDO2-Zugänge nur mit großer Sorgfalt. Da es sich hierbei um einen hardwaregestützten zweiten Faktor handelt, kann die Hardware nicht wissen, ob ein Zugang noch existiert. Er verbleibt so erst einmal auf dem Gerät. Löschungen müssen unbedingt direkt mit dem betroffenen User abgesprochen werden.

Orientierungen Sie sich an dem Zeitstempel. Auch die Kennung des FIDO2-Zugangs enthält solch einen Zeitstempel. Sollten Sie aus irgendwelchen Gründen FIDO2-Zugänge einzeln löschen müssen, können Sie so erkennen, welcher Zugang gelöscht werden muss.

Wenn Sie Verwaltungsrechte in BOLLE haben und sich mit FIDO einloggen möchten, dann müssen Sie beim Login direkt entscheiden, ob Sie in dieser Session vollen Zugriff auf Ihre Verwaltungsrechte haben möchten. So ist es möglich, dass Sie bei einem Login mit FIDO eine BOLLE-Umgebung ähnlich wie bei einer normalen Key-Datei haben.



7. Häufige Fragen

1. Ein Kollege hat sich gestern die Keydatei erstellt, diese jedoch nur geöffnet und nicht gespeichert. Ich habe daraufhin einen neuen Key erstellt. Wenn ich das pdf-Dokument zur Erstanmeldung herunterlade, ist jedoch kein Einmalpasswort angegeben. Wie kann der Kollege sich jetzt einloggen?
Nach solch einem Vorfall wird es tatsächlich etwas umständlicher. Das ist eine nötige Sicherheitseinstellung. Beim allerersten Login liegen noch keine persönlichen Daten vor, sodass wir den Erstlogin so gestalten können. Bei Verlust von Sicherheitsmerkmalen kann der "zweite Erstlogin" aus der Distanz so nicht mehr erfolgen. Als Admin gehen Sie in *Logindaten Personal* und laden einen neuen Key für den Kollegen direkt herunter. Sie geben den neuen Key dem Kollegen dann direkt mit; z.B. auf einem USB-Stick. Sie müssen sich also einmal treffen.
Ein Versand von Key-Dateien per E-Mail wird von uns nicht empfohlen, da der Key dann auch im Mailverlauf gespeichert bliebe.
An dieser Stelle können Sie auch z.B. das Passwort zurücksetzen. Sie brauchen für diese Aktionen das Admin-Passwort, das bei Erst-Installation von BOLLE an Ihren damaligen Admin übergeben und von diesem auch geändert wurde. Mehr zum Admin-Passwort erfahrne Sie hier.

2. Eine Kollegin hat Ihre Key-Datei verloren und kann sich nicht mehr einloggen. Was nun?

Als Admin gehen Sie in *Logindaten Personal* und laden einen neuen Key für die Kollegin direkt herunter. Sie geben den neuen Key der Kollegin dann direkt mit; z.B. auf einem USB-Stick. Sie müssen sich also einmal treffen.
Ein Versand von Key-Dateien per E-Mail wird von uns nicht empfohlen, da der Key dann auch im Mailverlauf gespeichert bliebe.
An dieser Stelle können Sie auch z.B. das Passwort zurücksetzen. Sie brauchen für diese Aktionen das Admin-Passwort, das bei Erst-Installation von BOLLE an Ihren damaligen Admin übergeben und von diesem auch geändert wurde. Mehr zum Admin-Passwort erfahrne Sie hier.

Version #27
Erstellt: 10 März 2021 14:55:34 von BOLLE Support
Zuletzt aktualisiert: 12 Mai 2026 19:39:41 von BOLLE Support