

Zwei-Faktor-Authentisierung in BOLLE

Der Zugang zu BOLLE erfolgt für das schulische Personal zwingend über die sogenannte Zwei-Faktor-Authentisierung (2FA). Auf dieser Seite finden Sie Informationen über die technische Organisation des zweiten Faktors.

Inhalt

1. Key für Lehrkräfte
2. Verwaltungskey
3. TOTP
4. BOLLE App
5. FIDO
6. Weitere Verfahren

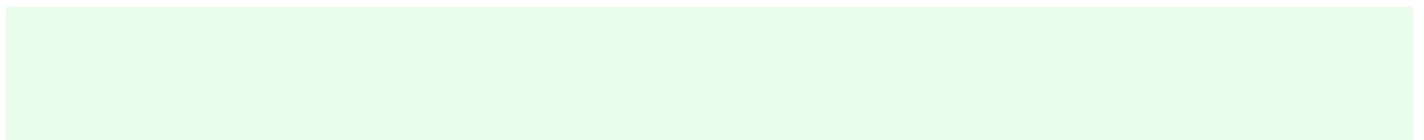
1. Key für Lehrkräfte

Lehrkräfte verwalten besonders sensible Daten in BOLLE. Der Einsatz der 2FA ist obligatorisch und wird bei der Einführung von BOLLE dem Personal erläutert. Jede Lehrkraft erhält eine individuelle Key-Datei, die beim ersten Login generiert wird. Ab diesem Zeitpunkt ist jeder weitere Login nur mit 2FA möglich.

Die Key-Datei ist eine html-Datei, die einen geheimen, persönlichen Schlüssel enthält. Beim Login des Personals wird das gehashte Passwort vom User und dieser geheime Schlüssel zum BOLLE-Server übertragen. Nur wenn beide Faktoren mit den gespeicherten Daten über den User übereinstimmen, wird dieser eingeloggt.

Der geheime Schlüssel ist eine Zeichenkette mit einer Länge von mindestens 50 Zeichen (Zahlen, Groß- und Kleinbuchstaben).

Die html-Datei kann vom Besitzer der Datei nach Belieben vervielfältigt werden. Ein effektiver Schutz dagegen existiert nicht. Es ist ratsam, das Personal regelmäßig darüber zu informieren und auf diesen Sicherheitsaspekt hinzuweisen.



BOLLE unterstützt die Schulen bei der Umsetzung z.B. mit Erinnerungen/Checklisten und Hinweise für Benutzer:innen.

2. Verwaltungskey

Einige Lehrkräfte nehmen besondere Rollen und Verwaltungsaufgaben in BOLLE wahr. Diese besonders sensiblen Bereiche sind durch eine zweite Key-Datei geschützt, dem Verwaltungskey. Dies ermöglicht den Lehrkräften, dass sie ihre Verwaltungsaufgaben von ihren unterrichtlichen Aufgaben trennen können.

Der Aufbau der Verwaltungskey entspricht dem der normalen Key-Dateien.

In der Regel haben solche Lehrkräfte ein eigenes Büro mit stationären Dienstrechnern im Schulgebäude. So kann der Verwaltungskey separat von der *normalen* Key-Datei aufbewahrt werden.

3. TOTP

Anstelle der Key-Datei kann jeder User das TOTP-Verfahren aktivieren. Dabei wird ein offener Standard zur Erzeugung von Einmalkennwörtern genutzt, die zusätzlich zum Benutzernamen und dem Passwort eingegeben werden müssen (siehe Wikipedia TOTP). Die Aktivierung des TOTP steht allen Nutzer:innen offen (Lehrkräften, Schüler:innen und Eltern).

Verwaltungsaufgaben können **nur** durchgeführt werden, wenn eine Authentisierung **mittels Verwaltungskey** erfolgt ist. TOTP genügt hierfür nicht.

4. BOLLE App

Die BOLLE App ermöglicht den Lehrkräften einen schnellen Zugriff auf eine eingeschränkte Funktionsauswahl. Der Login erfolgt nur, wenn man gleichzeitig im Browser bei BOLLE eingeloggt ist. Das Gerät wird dann mittels eines mindestens 200 Zeichen langen Tokens authentisiert, der via QR-Code direkt vom Smartphone eingelesen wird. Ein Login in die App ist somit nur möglich, wenn man korrekt in BOLLE im Browser eingeloggt ist.

Verwaltungsaufgaben können in der App generell nicht durchgeführt werden.

Schüler:innen und Eltern können sich mit den gleichen Logindaten wie im Browser (ggf. mit TOTP) einloggen.

Einmal eingeloggt, bleibt die App authentisiert, bis der User sich ausloggt. Beim Öffnen der App wird ein Entsperrmechanismus vom Telefon verlangt (z.B. Fingerabdruck, Gesichtsscan oder Entsperrcode).

Ist die App über mehrere Wochen inaktiv, wird die Authentisierung automatisch aufgehoben.

5. 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.

Beim Login mit FIDO für Personal mit Verwaltungsaufgaben kann außerdem entschieden werden, ob man sich mit vollen Verwaltungsrechten einloggen möchte. Somit ist auch bei der Nutzung von FIDO eine Unterscheidung ähnlich wie bei den Verwaltungskkeys gegeben (siehe oben).

6. Weitere Verfahren

Neuen Entwicklungen im Bereich der passwortlosen Anmeldung oder weiterer 2FA-Verfahren verfolgen wir interessiert. Neue Verfahren werden von uns dann implementiert, sobald sie sich ausreichend verbreitet und bewährt haben.