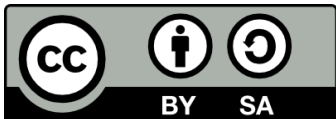




**Mobile Devices  
und 2-Faktor-  
Authentifizierung**



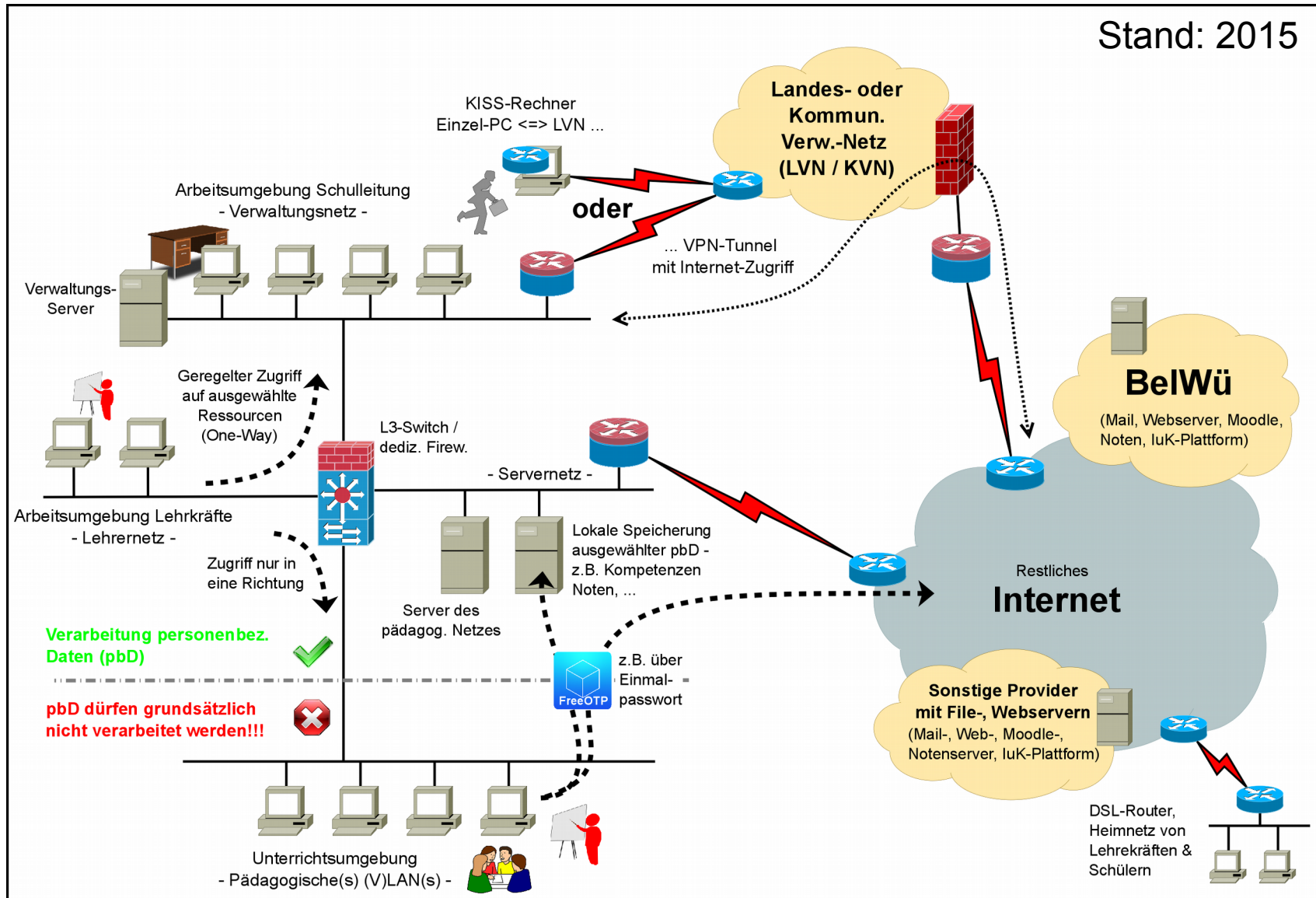
**Andreas Grupp**  
grupp@lehrerfortbildung-bw.de



„Mobile Devices und 2-Faktor-Authentifizierung“ von Andreas Grupp ist lizenziert unter einer Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz. <http://creativecommons.org/licenses/by-sa/4.0/deed.de>



Stand: 2015





*Zeugnisse, Lernstandsberichte, Halbjahresinformationen und vergleichbare Dokumente dürfen in der Unterrichtsumgebung **generell** nicht verarbeitet werden.*

*Ist jedoch beabsichtigt, weitere personenbezogene Daten von Schülern in der Unterrichtsumgebung zu verarbeiten, beispielsweise laufende Leistungsbeurteilungen (Einteilung in Niveaustufen oder der Einsatz von Kompetenzrastern), müssen zwingend die folgenden technischen Datenschutzmaßnahmen getroffen werden.*

- Als Identitätsnachweis ist für jeden Nutzer eine Zwei-Faktoren-Authentifizierung erforderlich, die aus der Kombination von zwei verschiedenen voneinander unabhängigen Komponenten (Faktoren) besteht. Zusätzlich zum üblichen Passwort ist der Besitz eines "elektronischen Schlüssels" erforderlich. Denkbar wäre die Verwendung von Hardwaretokens oder von Einmal-Passwörtern (time-based one-time-Password, nach dem TOTP- bzw. OTP-Verfahren). Bei der Verwendung eines Einmalpassworts muss die Passwörterzeugung zwingend auf einem zweiten Gerät erfolgen. Alternativ könnte auch eine TAN-Liste verwendet werden.*

Zusätzlich ist eigenes Server-Netz (auch als VLAN erlaubt) erforderlich. Die Datenübertragung muss zudem eine Transportverschlüsselung haben.





- **Erster Faktor bei der Authentifizierung**
  - Benutzernamen und zugehöriges Passwort
  - Bei jedem Login gleich!
  - Häufig auch „weiteren Personen“ bekannt
- **Zweiter Faktor bei der Authentifizierung**
  - Zusatz-Hardware – z.B. Smartcard, Hardware-Token
    - Interoperabilität zwischen Anwendungen mäßig
  - Einmal-Passwort – z.B. auf Uhrzeit basierend
    - Time-based One-Time-Password (TOTP)
    - Am weitesten verbreitet → auf Basis des Google-Authenticator-Algorithmus





## Server

Gibt ein „Geheimnis“ vor

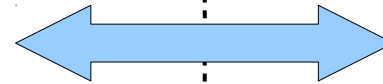
**3EB4G3X5LI7ZKRWS**

## Client

Übernimmt „Geheimnis“

**3EB4G3X5LI7ZKRWS**

Einmaliger Vorgang!  
Server und Client teilen  
sich nun ein „Geheimnis“



Benötigt hierfür keinerlei  
Online-Verbindung auf  
dem 2. Gerät! Weder  
Mobilfunk, noch Internet!  
Code wird von Hand oder  
per QR-Code-Scan  
übertragen



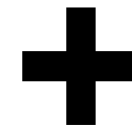
Benötigt hierfür keinerlei Online-Verbindung mehr! Weder Mobilfunk, noch Internet!

## Server

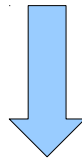
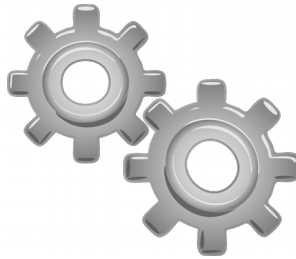
## Client



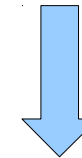
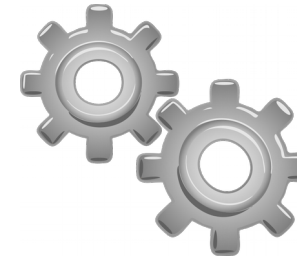
3EB4G3X5  
LI7ZKRWS



3EB4G3X5  
LI7ZKRWS



640118



640118




**Kommt der Client auf das gleiche Ergebnis?**



- Woher wissen „weitere Personen“ eigentlich die Kombination „Benutzernamen / Passwort“?
- Und wo wird der 2. Faktor erzeugt? Netzbrief V3 **schreibt zweites Gerät zwingend vor**
- Zweites Gerät reduziert die Wahrscheinlichkeit, dass Angreifer beide Geräte gleichzeitig unter Kontrolle hat erheblich
- Mögliche Geräte als zweites Gerät:
  - Smartphone – egal welches Betriebssystem
  - Tablets – egal welches Betriebssystem
  - Eher weniger sinnvoll → 2. PC





- Freie, quelloffene Apps für TOTP → verfügbar
  - z.B. für Android, iOS → FreeOTP 
- Serverseitig z.B. für das Kompetenzraster in Moodle → bereits verfügbar
- Zeit auf Server u. Client muss einigermaßen synchron sein → Gewisse Abweichung ok.
- Software- Kosten für eigentliche 2-Faktor-Auth. beläuft sich auf → 0,- €
- Zweites Gerät → Kostenübernahme?  
Unterstützung? Beteiligung?





1.)  Test (Profil)  Abmelden **WebUntis**

Profil Test x

Allgemein Startseite Freigaben **Sicherheit** 2.)

### Google Authenticator

Mit Google Authenticator können Sie Ihren Benutzerzugang zusätzlich schützen.

Authenticator ist ein kleines Programm, das Sie auf Ihrem Smartphone installieren können. Es erzeugt einen Code, der beim Anmelden zusätzlich zum Passwort abgefragt wird.

Sie benötigen dafür ein von Google Authenticator unterstütztes Smartphone.

**Google Authenticator ist hier als mathematisches Verfahren zu verstehen – die Software / App selbst nicht installieren!**

**Google Authenticator aktivieren** 3.)

Speichern Abbrechen





Test (Profil)

Abmelden

WebUntis

Profil Test

Allgemein Startseite Freigaben **Sicherheit**

### Google Authenticator - Aktivierung (1/3)

Bitte installieren Sie die Google Authenticator Anwendung auf Ihrem Smartphone.

Eine Anleitung zur Installation des Authenticators auf Android, iOS oder BlackBerry Geräten finden Sie hier: [Google Authenticator Installation](#).

Im Internet finden Sie auch Apps für Windows Phone.

**4.)**

Zurück **Weiter** Abbrechen

Speichern Abbrechen

**Google Authenticator nicht installieren! Benötigt nicht nachvollziehbar viele Rechte. Empfohlen wie gesagt FreeOTP.**





Benötigt hierfür keinerlei Online-Verbindung auf dem 2. Gerät!  
Weder Mobilfunk, noch Internet!

Test (Profil)

Profil Test

Allgemein Startseite Freigaben **Sicherheit**

### Google Authenticator - Aktivierung (2/3)

Richten Sie Google Authenticator auf Ihrem Smartphone ein, indem Sie entweder den Code auf dieser Seite scannen oder den angezeigten Schlüssel manuell eintragen.

Schlüssel **TP7KIJSNPSLGXHPV**

5.)

6.)

Zurück **Weiter** Abbrechen

Speichern Abbrechen





Profil Test ✕

Allgemein Startseite Freigaben **Sicherheit**

### Google Authenticator - Aktivierung (3/3)

Bitte geben Sie den aktuellen Bestätigungscode ein, den Google Authenticator auf Ihrem Smartphone anzeigt. Klicken Sie dann auf 'Aktivieren'.

7.)

8.)

⚙️ Test (Profil)

🚫 Abmelden

WebUntis

Profil Test ✕

Allgemein Startseite Freigaben **Sicherheit**

**Google Authenticator**

Google Authenticator ist aktiviert.

Google Authenticator deaktivieren Schlüssel anzeigen

9.) **Speichern** Abbrechen



Schulname Benutzer Passwort

HEID TECH Test

.....

**Klick!**

Login WebUntis

**Google Authenticator** x

Bitte geben Sie Ihren Bestätigungscode ein.

136504

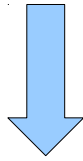
Senden Abbrechen

**Benötigt hierfür keinerlei Online-Verbindung auf dem 2. Gerät!  
Weder Mobilfunk, noch Internet!**



TOTP-Zweifaktorauthentifizierung

TOTP (zeitgesteuertes Einmalpasswort) aktivieren



TOTP-Zweifaktorauthentifizierung

TOTP (zeitgesteuertes Einmalpasswort) aktivieren

Dies ist Ihr neuer TOTP-Schlüssel: PYFRXRY6IURB4GX3

Scannen Sie diesen QR-Code mit Ihrer TOTP-App



Nextcloud login screen showing the username 'mustermann' and a password field with 10 dots. A blue 'Einloggen' button with a right arrow is at the bottom.



Nextcloud TOTP authentication screen. It shows the Nextcloud logo and the text 'TOTP (Authenticator app)'. Below is a text input field containing '08154711' and a right arrow. At the bottom, it says 'Erhalten Sie den Authentifizierungscode von der Zweifaktorauthentifizierung-App auf Ihrem Gerät.'




Da App's auf mobilen Geräten die 2FA ggf. (im allgemeinen) nicht können → App-spezifisches Passwort aktivierbar, das dann keine 2FA benötigt.

Samsung-Note-Tablet	vor 37 Minuten
Thunderbird Dell-Laptop	vor 2 Tagen
iPad Air 2	vor 4 Tagen
VirtWin7PC	vor 18 Tagen

Nutzen Sie die unten angegebenen Anmeldeinformationen, um ihre App oder ihr Gerät zu konfigurieren. Aus Sicherheitsgründen wird das Passwort nur einmal angezeigt.

Benutzername

Passwort  

Bei Geräte-Verlust, oder Verdacht auf Kompromittierung, können App-Zugänge einzeln gelöscht / neu gesetzt werden!





- Unbedingt den Shared Key, der Basis für den TOTP-Algorithmus ist, redundant sichern
  - z.B. im Passwort-Save „KeePass“
- Apropos „KeePass“: Über das Plugin „KeeOTP“ kann auch via KeePass das zeitbasierende One-Time-Passwort generiert werden
  - Beachten: Unter Beachtung des Netzbriefs ist zwingend ein zweites Gerät erforderlich!





**... haben Sie noch Fragen?**

