



**Kanton Zürich
Bildungsdirektion
VSA**

Digitale Identitäten

**FN-Zmittag
01. Dezember 2025**

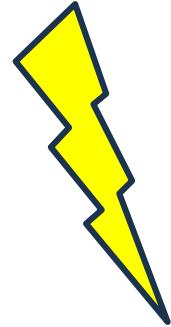
**Fachstelle Bildung und ICT
Simone Büchi und Daniel Jud**

Inhalt

1. Digitale Identitäten – Spannungsfeld
2. Digitale Identitäten im Ökosystem Schulfeld
3. Digitale Identität und Sichtbarkeit
4. Digitale Identitäten und Digitale Souveränität
5. Digitale Identität und Informationssicherheit
6. Digitale Identität und Handlungsbedarf
7. Ausblick

Digitale Identität

- Sichtbarkeit
(Socialmedia)
- Zurechenbarkeit in
der Bearbeitung
- Rollen- und
Berechtigungskonzept



- Digitale
Souveränität
- Recht auf
Löschen von
Spuren
- Anonymität



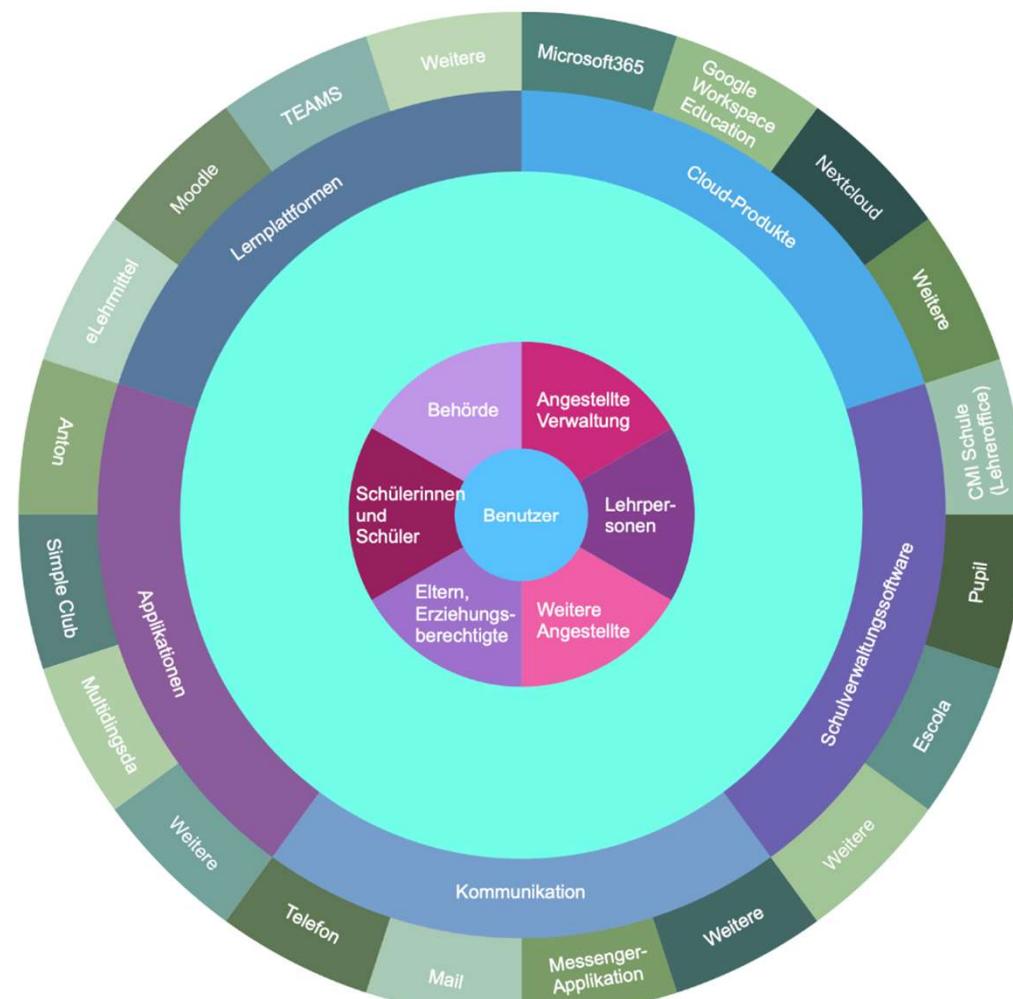
Ziele von heute

- FN-PICTS: Workshop mit Felix Stoppany und Patrick Buff
- CLICKA oder ICT-Coach

Digitale Identitäten im Ökosystem Schule

Gesamtbild von...

- Benutzerinnen und Benutzern
 - Lehrplan 21
 - Unterrichtsentwicklung
 - Personalentwicklung
 - Anforderungen (technisch und organisatorisch)
 - Sensibilisierung und Befähigung



ICT-Coach – Kanton ZH

Willkommen beim ICT-Coach

Wir unterstützen Sie und Ihre Schule mit der Website «ICT-Coach» auf dem Weg des digitalen Wandels.

Dieser wird die Art des Lernens und Lehrens verändern. Ebenso wird er die Kultur der Zusammenarbeit sowie Prozessabläufe innerhalb der Schule beeinflussen. Alle in der Schule - vom Lehrerteam bis zu den Behördenmitgliedern - sind eingeladen, den digitalen Wandel aktiv mitzugestalten.

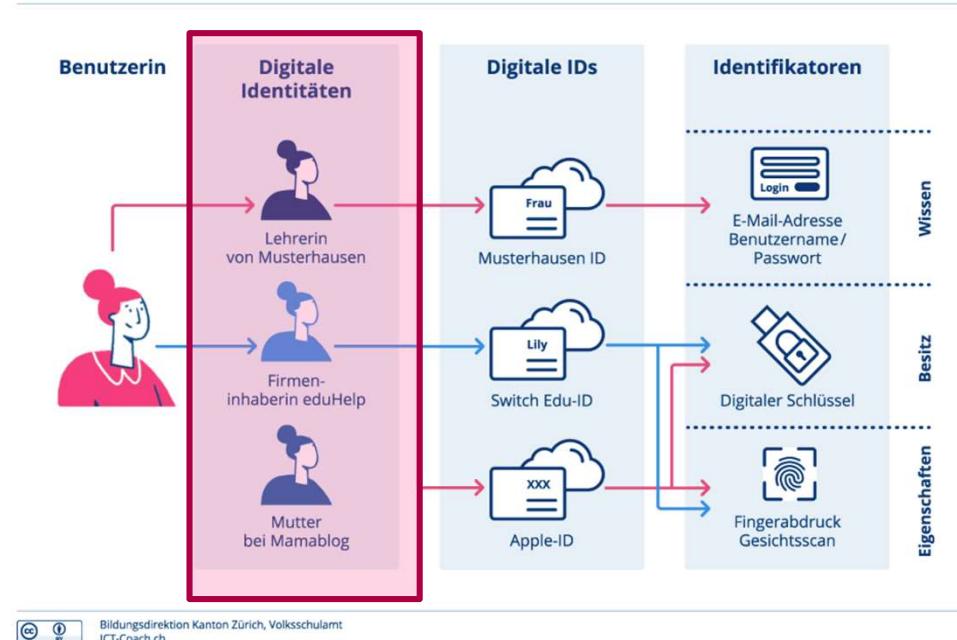
Der «ICT-Coach» baut auf dem lokalen Medien- und ICT-Konzept Ihrer Schule auf und ermöglicht auf wesentliche Fragen vertieft einzugehen.



Digitale IDs

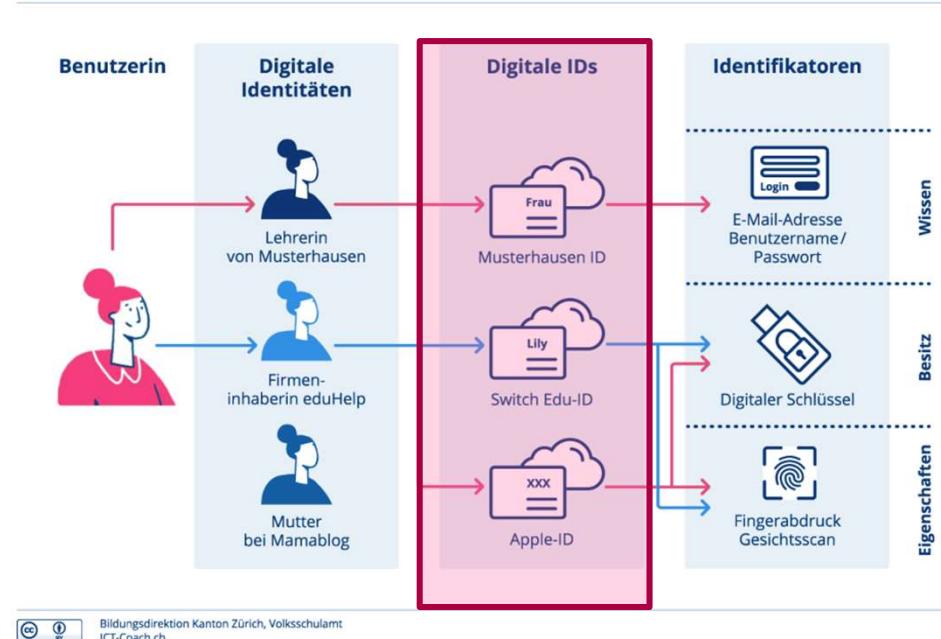
So offen Netzwerke und die Cloud auch sind – **nicht alle sollen auf alles Zugriff haben**. Um diesen zu regeln, brauchen Benutzerinnen und Benutzer eine sogenannte **digitale Identität**. Diese muss je nach Kontext unterschiedliche Kriterien erfüllen und vom System verwaltet werden. Je nach Technologie gibt es auch unterschiedliche Anmeldeprozesse, deren Schritte in diesem Kapitel beschrieben werden.

Digitale Identität



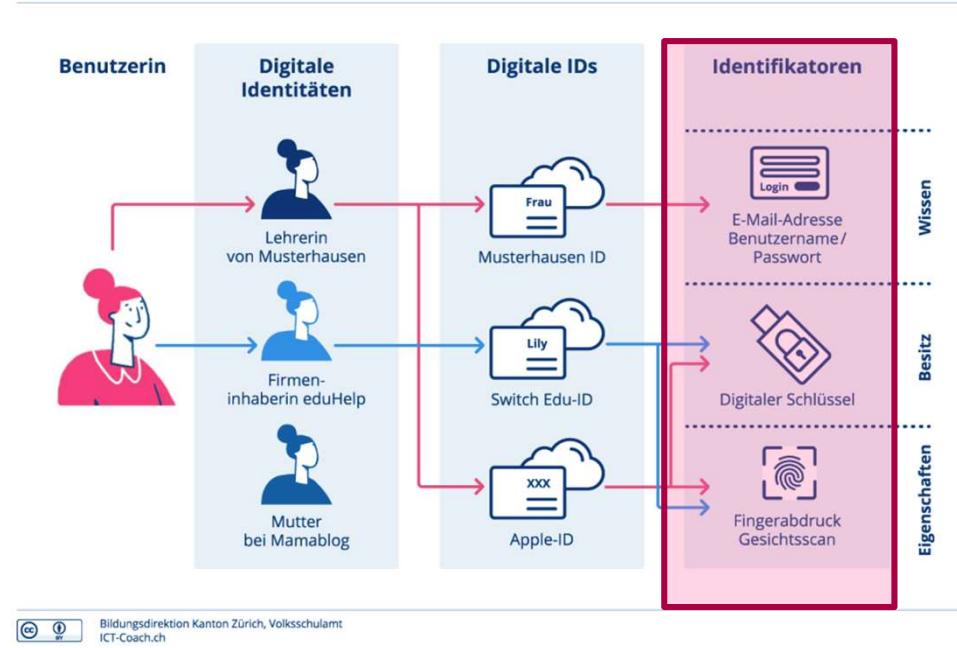
Daten und/oder Merkmale, die eine Person, Organisation oder ein System im digitalen Raum eindeutig beschreiben und wiedererkennbar machen.

Digitale ID (Identifikationsmittel)



Technisches Mittel oder Werkzeug, das dich eindeutig authentifiziert, also deine digitale Identität nachweist und zugänglich macht.

Identity Access Management



Authentisierung

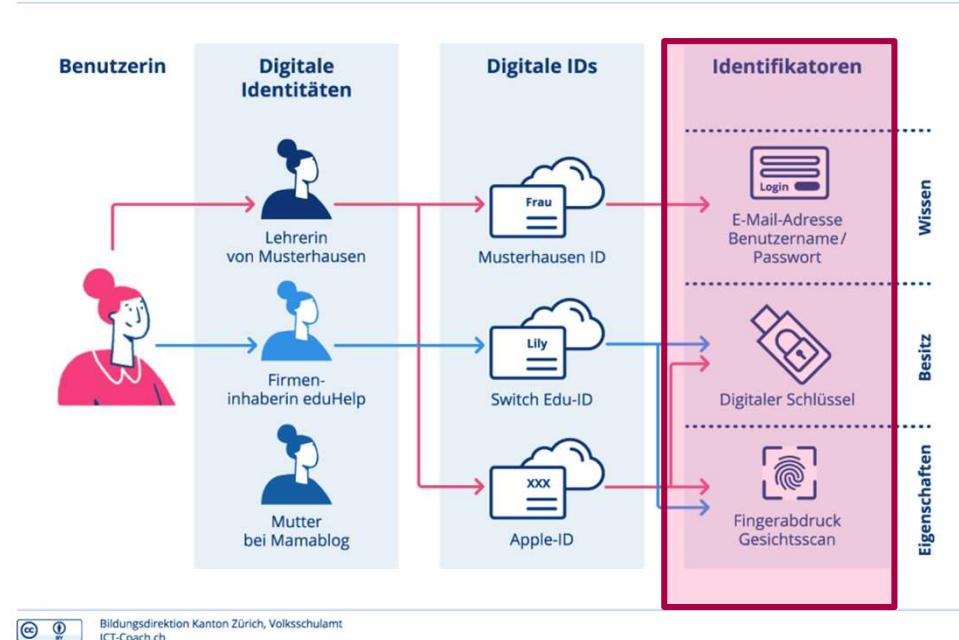
- Jemand oder etwas weist nach, dass er oder es wirklich derjenige ist, der er vorgibt zu sein.

Authentifizierung

- Überprüfung, ob die Authentisierung stimmt.



Identity Access Management



- Email-Adresse und Passwort
- Benutzername und Passwort
- Fingerabdruck
- Gesichtserkennung
- etc.

Arbeitsauftrag

Grundsatz: Ihr wählt selber aus, in welcher der drei identischen Grafiken ihr arbeitet.

1. Verschafft euch einen Überblick über die Grafik
2. Haltet im türkisen Kreis **mit gelbe Notizzetteln** fest, wo **digitale Identitäten im Schulalltag** gebraucht werden. Doppelnennungen per Notizzettel oder «Daumen hoch».
3. Erfasst mögliche **Risiken** und **offene Fragen** in den Schnittstellen **mit roten Notizzetteln**.

Miro

[https://miro.com/app/board/uXjVJoFmKs4=/?](https://miro.com/app/board/uXjVJoFmKs4=/?share_link_id=733284116097)
share link id=733284116097



Digitale Identität und Sichtbarkeit

Privat vs. Beruf

- Ermöglicht Partizipation und Zugehörigkeit in Netzwerken
- Wann ist ein MA einer Schule als MA und wann als Privatperson unterwegs?
- Social Media Guidelines sind in Arbeit

Digitale Identitäten und Digitale Souveränität

- Kompetent digital unterwegs sein
 - Unabhängigkeit wahren bei den genutzten Diensten: Lock-in vermeiden
 - Daten löschen lassen



Digitale Identität und Informationssicherheit

Informationssicherheit

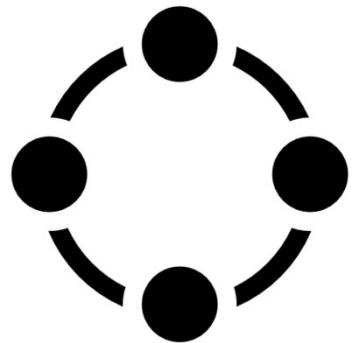
- Bearbeitung einer Information muss einer Person zurechenbar sein

Datenschutz

- Es sollen nur Daten über Personen gesammelt werden, für die es eine gesetzliche Grundlage gibt und die für die Ausübung der Aufgaben nötig sind



angemessenes Sicherheitsniveau erreichen



- Risiken erkennen
- Risiken bewerten
- Risiken priorisieren
- Massnahmen ergreifen
- Umsetzung sicherstellen und reflektieren



Risikobereiche: TOBP

- **Technische Risiken:** Ist das Login sicher
- **Organisatorische Risiken:** Sind die Berechtigungen richtig verteilt
- **Bauliche Risiken:** Unbefugter Zugang zum Serverraum
- **Pädagogische Risiken:** Sind MA, SuS & Eltern genügend sensibilisiert



Massnahmen zu den Risikobereichen: TOBP

- **Technische Risiken:** 2- oder mehrfach Authentifizierung
- **Organisatorische Risiken:** Berechtigungskonzept, Rollen und Aufgaben klären
- **Bauliche Risiken:** Zugangskonzept Serverraum inkl. externe Supporter
- **Pädagogische Risiken:** Sensibilisierung und Weiterbildungen, technisches Grundrüstzeug

Digitale Identitäten im Ökosystem Schule

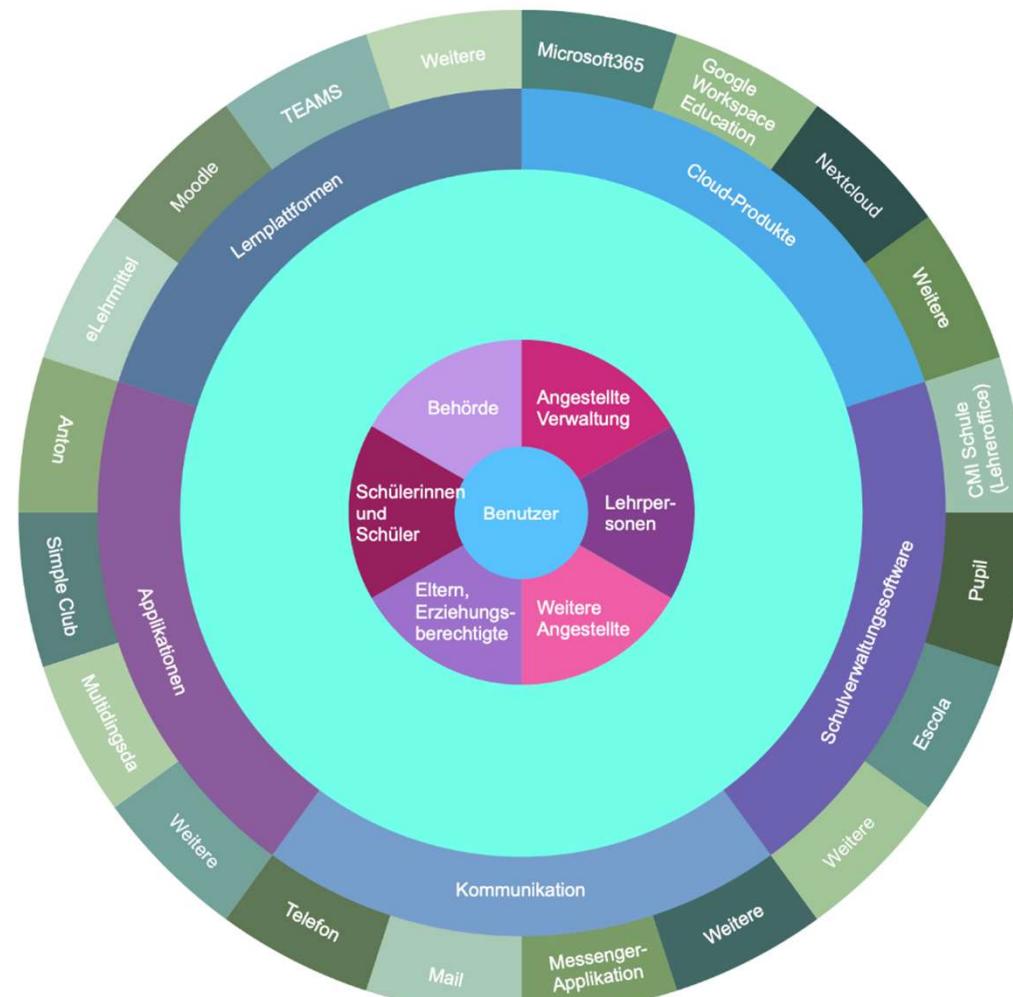
Folie 19

Gesamtbild von...

- Benutzerinnen und Benutzern
- Lehrplan 21
- Unterrichtsentwicklung
- Personalentwicklung
- Anforderungen (technisch und organisatorisch)
- Sensibilisierung und Befähigung
- ...

Blick ins Miro

Klassifizierung: öffentlich



Ausblick

17. Januar 2026

FBI mit HfH: Mit Bildungstechnologien Lernumgebungen für alle schaffen

24. Januar 2026

FN-PICTS Vernetzungstreffen, Zentrum Liebfrauen

09. Mai 2026

FN-DigiWa Vernetzungstreffen am Institut Unterstrass

06. Juni 2026

FN-PICTS Vernetzungstreffen am Institut Unterstrass

