univention
be open.

IDENTITY- UND ACCESSMANAGEMENT (IAM) MIT UNIVENTION CORPORATE SERVER (UCS)

Impressum:

Veröffentlichungsdatum: 1. Version Mai 2021

Herausgeber:

Univention GmbH, Mary-Somerville-Straße 1, 28359 Bremen, info@univention.de

Autoren:

Ingo Steuwer, Head of Product Management, Univention GmbH, steuwer@univention.de

Inhaltsverzeichnis

1 Univention GmbH

Univention ist führender Anbieter von Open-Source-Produkten für das Identity- und Accessmanagement. Einfach handhabbare IT-Lösungen für Unternehmen und Organisationen der öffentlichen Verwaltung und im Bildungsbereich haben für Univention eine strategische Bedeutung. Zu unseren Kunden zählen öffentliche Verwaltungen wie beispielsweise das Ministerium für Bildung, Wissenschaft und Kultur Schleswig-Holstein, das Ministerium für Bildung, Jugend und Sport des Landes Brandenburg, der Landtag Brandenburg, die Stadt Köln oder das Bundesamt für Strahlenschutz sowie Unternehmen wie die Orange S.A. Frankreich mit mehr als 30 Millionen verwalteten Identitäten.

Ziel von Univention ist es, IT-Lösungen für alle Beteiligten (Administrator*innen und Benutzende) einfach und verlässlich nutzbar zu machen. Die wiederkehrenden Anforderungen an das Identity- und Accessmanagement adressieren wir mit unserem Standardprodukt Univention Corporate Server (UCS) und vereinfachen Wartung und Betrieb der damit realisierten Lösungen nachhaltig, weil der Aufwand für die Pflege und Weiterentwicklung nicht von einem einzelnen Kunden bzw. einer einzelnen Organisation getragen werden muss. Der mit der Softwareentwicklung verbundene Aufwand wird auf viele Schultern verteilt und potenzielle Fehlerquellen können viel systematischer ausgeschlossen werden. Univention übernimmt die Produktgewährleistung und Support mit SLAs bis 24/7. Insgesamt setzen heute weltweit mehr als 15.000 Organisationen unser Produkt „Univention Corporate Server (UCS)“ ein.

Der Quellcode aller Produkte von Univention ist vollständig unter Open-Source-Lizenzen veröffentlicht und ermöglicht Dritten die Möglichkeit zur Mitwirkung an der Weiterentwicklung über Plattformen wie Github. Das Engagement von Univention für Open Source drückt sich auch durch zahlreiche weitere Aktivitäten und Mitgliedschaften aus.

Univention pflegt Partnerschaften mit mehr als 400 Kooperationspartnern, vorrangig mit Systemintegratoren und mit Softwareanbietern.

Die Univention GmbH wurde im Jahr 2002 in Bremen gegründet. Neben unserem Hauptsitz in Bremen verfügen wir über weitere Büros in Berlin, Leipzig und Seattle in den USA.

2 Univention Corporate Server (UCS)

Das Produkt Univention Corporate Server (UCS) ist vollständig Open Source Software und wird in vielen, zum Teil auch sehr großen, Umgebungen eingesetzt, um digitale Identitäten, Rollen und Berechtigungen zu verwalten. Die Basis bilden Standard-Services wie ein erprobter und skalierbarer Verzeichnisdienst mit einem Identity- und Access Management (IAM), ein Webportal und ein SAML basiertes Single-Sign-on (SSO). Diese Services werden mit verschiedenen Produkten in umfangreich getesteter, kontinuierlich gepflegter und hoch skalierbarer Weise ausgeliefert. Mögliche individuelle Anpassungen oder Erweiterungen können damit auf erprobter Basistechnologie aufgebaut und auf den spezifischen Nutzwert fokussiert werden.

2.1 Betriebsumgebung und Skalierbarkeit

UCS wird als Softwarelösung zu Verfügung gestellt, die in eigenen Rechenzentrums-Infrastrukturen (On Premises) oder bei Private- oder Public Cloud Service Providern betrieben werden kann. Die Lösung sieht eine horizontale und vertikale Skalierung vor und kann damit sowohl hohe Zugriffszahlen, hohe Verfügbarkeit und auf mehrere Standorte verteilte Infrastrukturen bedienen.

2.2 Zentrale Module der IAM-Lösung

Die IAM-Lösung von UCS besteht aus mehreren, ineinander verzahnten Modulen, die im Folgenden beschrieben werden.

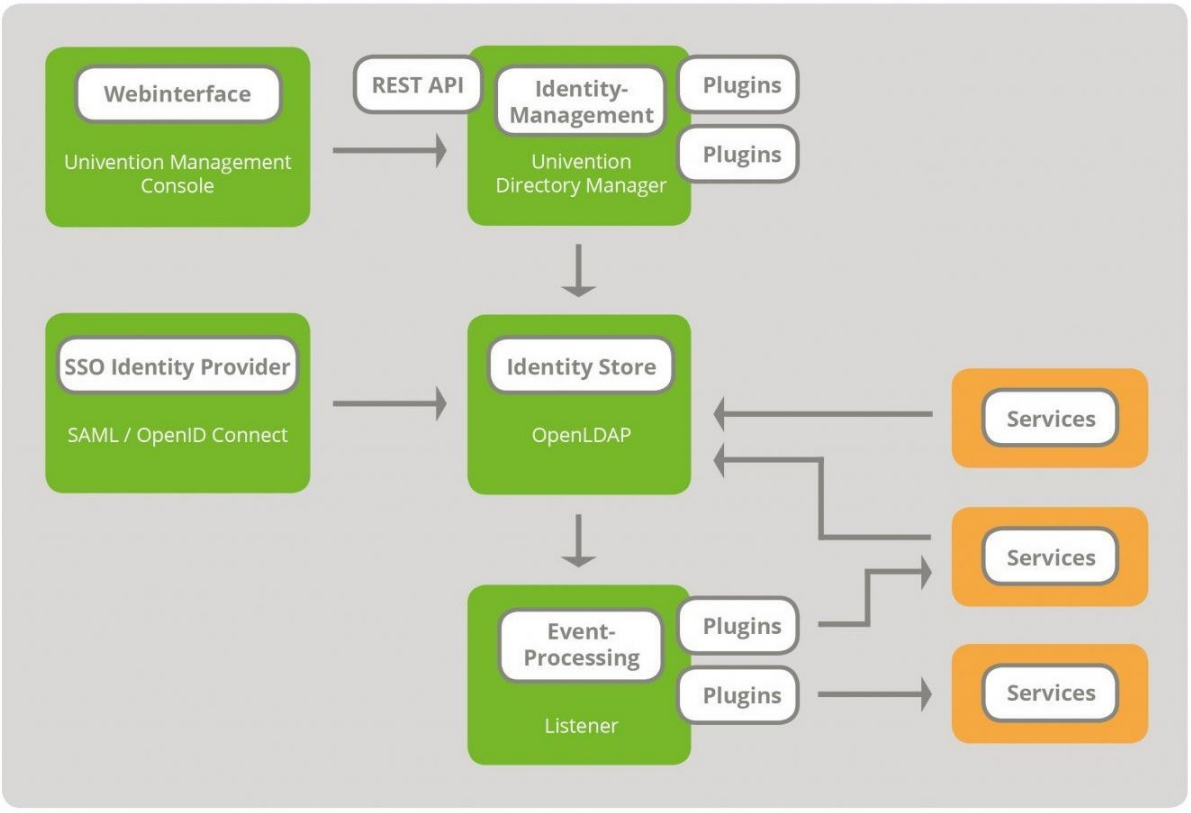

Abb. 1: Grundarchitektur UCS

2.2.1 Identity Store (Verzeichnisdienst)

Die führende Datenhaltung der IAM-Lösung erfolgt in einem Verzeichnisdienst auf Basis von OpenLDAP, welches als „Identity Store" die Identitäten und weitere Informationen speichert und gegenüber authentifizierten Systemen entsprechend den jeweiligen Rechten abrufbar macht. Die im Verzeichnisdienst gespeicherten Informationen werden aus Gründen der Lastverteilung und Ausfallsicherheit automatisch auf mehrere Systeme repliziert.

2.2.2 Identity Management (UI und APIs)

Kernelement des Identity Managementsystems ist das Modul „Univention Directory Manager", das für konsistente und standardkonforme Pflege der Inhalte im Identity Store sorgt. Für die manuelle Verwaltung

durch Benutzer und Administratoren steht die Univention Management Console (UMC) als ID Management UI (User Interface, Benutzeroberfläche) zur Verfügung. Die Funktionen und Inhalte des Webinterface richten sich dabei nach den konfigurierten Berechtigungen.

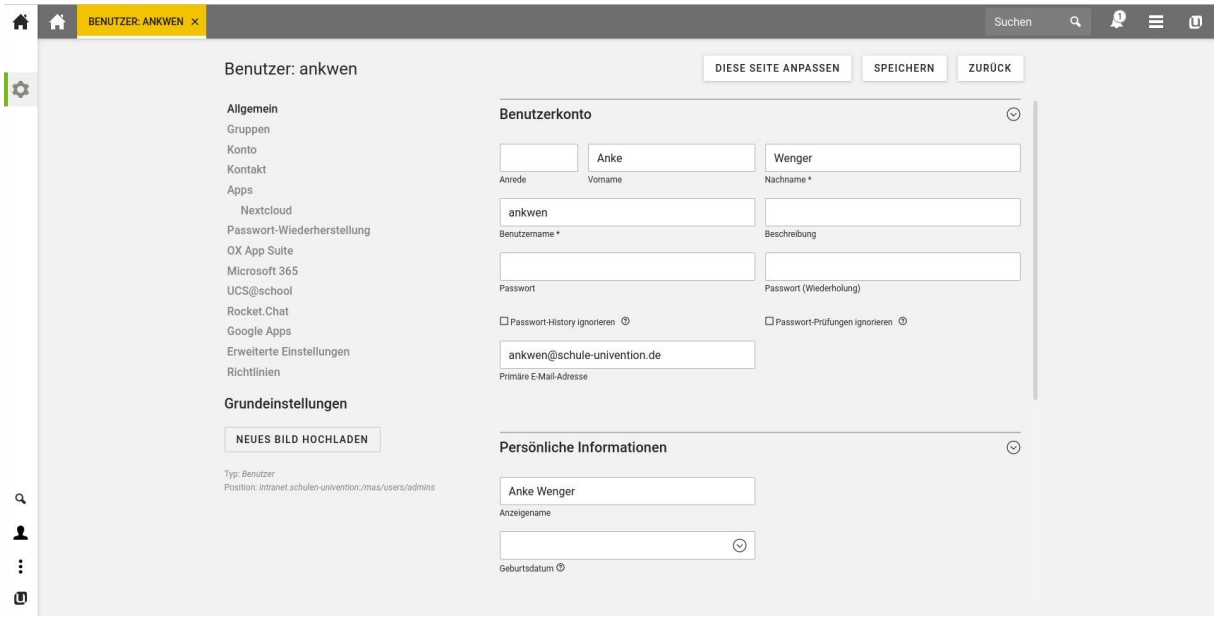

Abb. 2: Univention Management Console (UMC)

Mit der REST API (https://docs.software-univention.de/developer-reference-4.4.html) steht eine Schnittstelle zur Verfügung, die den Zugriff auf alle Inhalte des Verzeichnisdienstes von Univention Corporate Server ermöglicht. Diese kann beispielsweise genutzt werden, um Integrationen mit Quellsystemen (HR Systeme etc.) zu realisieren. Administratoren steht zudem noch der Zugang zum UDM-CLI-Tool offen, das als Kommandozeilentool bestimmte administrative Arbeiten gegenüber dem Webinterface vereinfachen kann.

Das Identity Management verfügt über standardisierte Schnittstellen zur Erweiterung der verarbeiteten Inhalte (z.B. Eigenschaften von Identitäten) und Individualisierung der Prozesse.

2.2.3 ID-Management Notifications

Ein wichtiger technischer Bestandteil des ID-Management ist der "Listener/Notifier-Mechanismus". Über diesen Mechanismus können Event-basierte Aktionen beim Anlegen, Verändern oder Löschen von Verzeichnisdienstobjekten ausgelöst werden.

So führt zum Beispiel das Anlegen eines Benutzerobjekts mit der Univention Management Console dazu, dass der Benutzer in das LDAP-Verzeichnis eingetragen wird. Der Listener/Notifier-Mechanismus stellt dann sicher, dass das Benutzerobjekt beispielsweise auch in einem gewünschten (externen) Zielsystem angelegt wird.

Der Listener/Notifier-Mechanismus kann leicht um Module für weitere – auch kundenspezifische – Vorgänge ergänzt werden und wird zum Beispiel von zahlreichen Technologiepartnern für die Integration ihrer Produkte in den LDAP-Verzeichnisdienst und das ID-Management verwendet.

2.2.4 Identity Provider / Single Sign-on

UCS implementiert die Rolle eines SAML und OpenID Connect Identity Providers und bietet damit Web Single Sign-on, sodass bei integrierten Diensten nur eine einmalige Anmeldung notwendig ist (http://docs.software-univention.de/handbuch-4.4.html#domain:saml bzw. https://docs.software-univention.de/handbuch-4.4.html#domain:oidc).

Die Benutzerdaten müssen nicht redundant vorgehalten und gepflegt werden und die Ausfallsicherheit in verteilten Umgebungen wird erhöht, indem die Konfigurationen direkt im OpenLDAP-Verzeichnisdienst von UCS abgelegt und somit automatisch synchronisiert werden.

2.2.5 Portal

Das UCS Portal ist eine Webanwendung, die als zentraler Anlaufpunkt für Endanwender positioniert wird. Das Portal kann interne wie externe Dienste verlinken und viele so integrieren, dass sie direkt im Portal geöffnet und genutzt werden können.

Zudem können Benutzer sich mit ihren Nutzerdaten am Portal einmalig authentifizieren und erhalten anschließend auf alle per SSO angeschlossenen Dienste direkten Zugriff ohne ihre Zugangskennung erneut eingeben zu müssen (vorausgesetzt der jeweilige Dienst ist für den jeweiligen Benutzer im IAM freigeschaltet). Welche Portal-Kacheln und damit Dienste angemeldeten Benutzer*innen angezeigt werden, kann in Abhängigkeit der jeweiligen Gruppenzugehörigkeiten konfiguriert werden. Zudem kann konfiguriert werden, ob und wenn ja, welche Portal-Kacheln nicht angemeldeten Besuchern des Portals gezeigt werden.

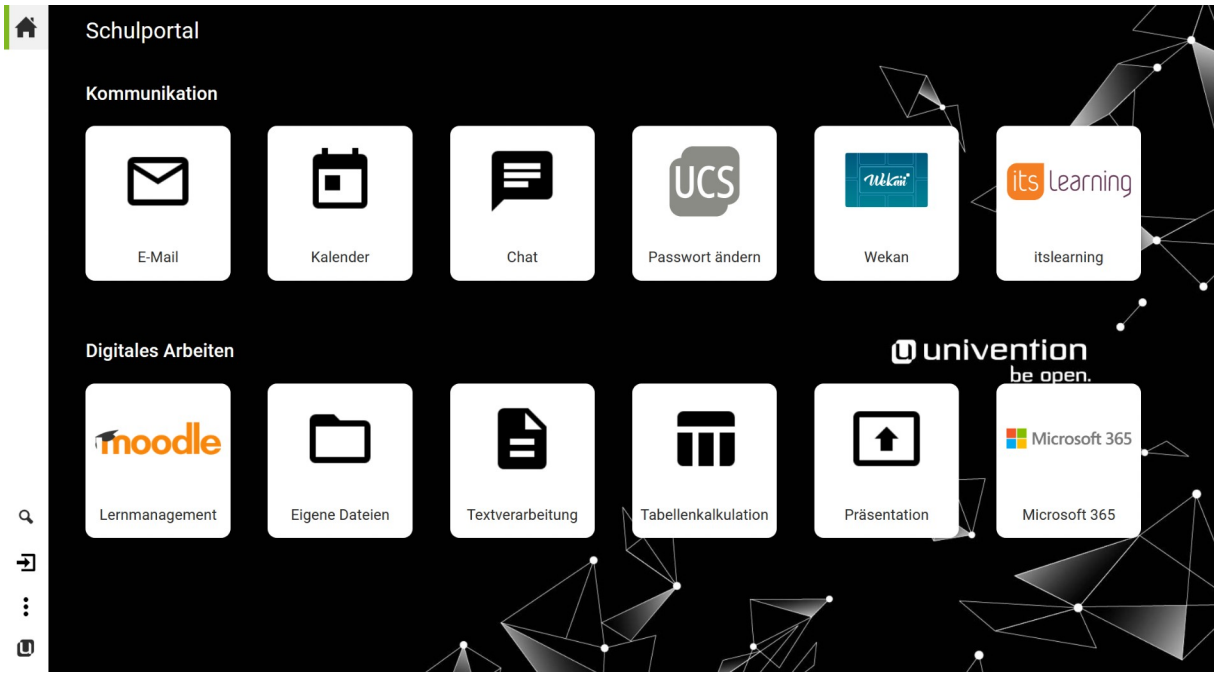

Abb. 3: UCS-Portalansicht

2.2.6 Self-Service

Der UCS Self-Service ist ein Webdienst, der die Endbenutzer in die Lage versetzt, ihr Benutzerkonto selbstständig zu verwalten.

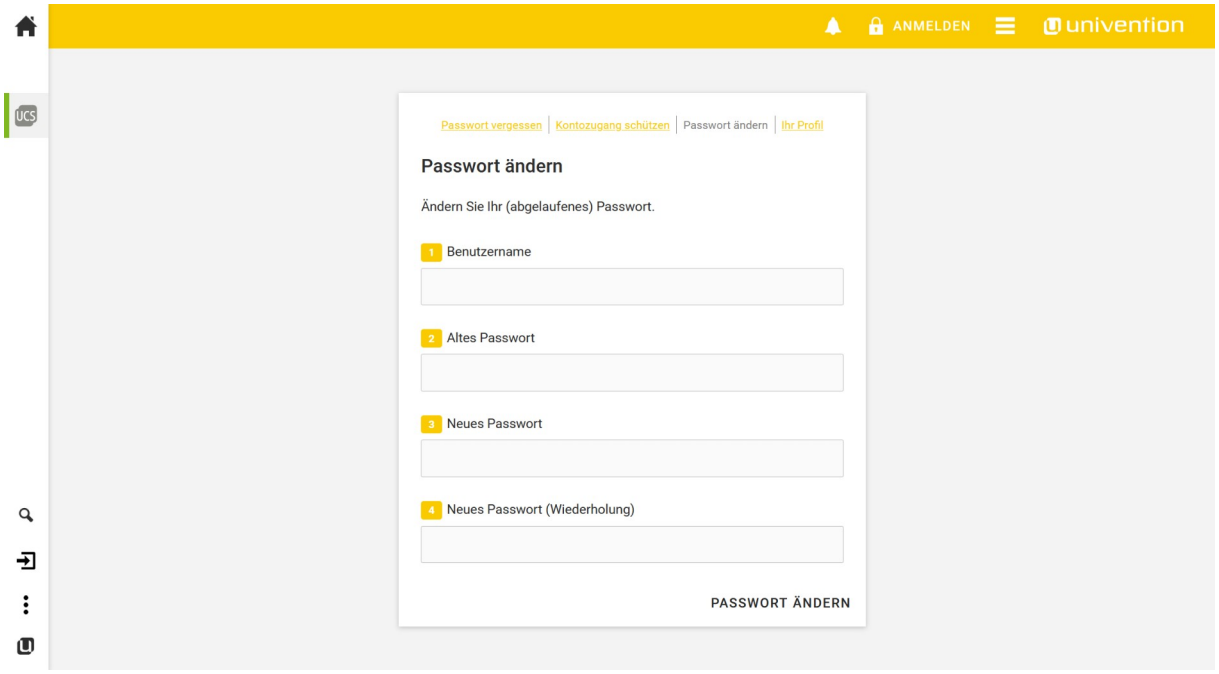

Abb. 4: Login-Ansicht Self-Service

Die primären Funktionen des Self-Service sind das Registrieren bzw. Beantragen neuer Konten, das Ändern von Eigenschaften des eigenen Nutzerkontos (z.B. Passwort oder Kontaktinformationen) und das Generieren eines neuen Passworts bei Verlust. Welche Funktionen zur Verfügung gestellt werden, ist individuell konfigurierbar.

Der Einsatz eines solchen Self-Services entlastet erfahrungsgemäß den Anwendersupport erheblich.

3 Projektergänzungen

Auf Basis zahlreicher Projekte und der laufenden Pflege wird die Architektur und Funktionalität von UCS stetig erweitert. Dazu gehören die Modularisierung und Containerisierung des IAM sowie der Ausbau des Provisionierungs-Backends zur Anbindung und Steuerung anderer Systeme und Dienste. Im IDP Bereich wird die Standardunterstützung von SAML und OpenID Connect durch die Integration eines ID Brokers erweitert, wie er im Projekt Phoenix (Dataport) und im „ID Broker“ genutzt wird. In der Abbildung ist die sich daraus ergebende Gesamtarchitektur dargestellt.

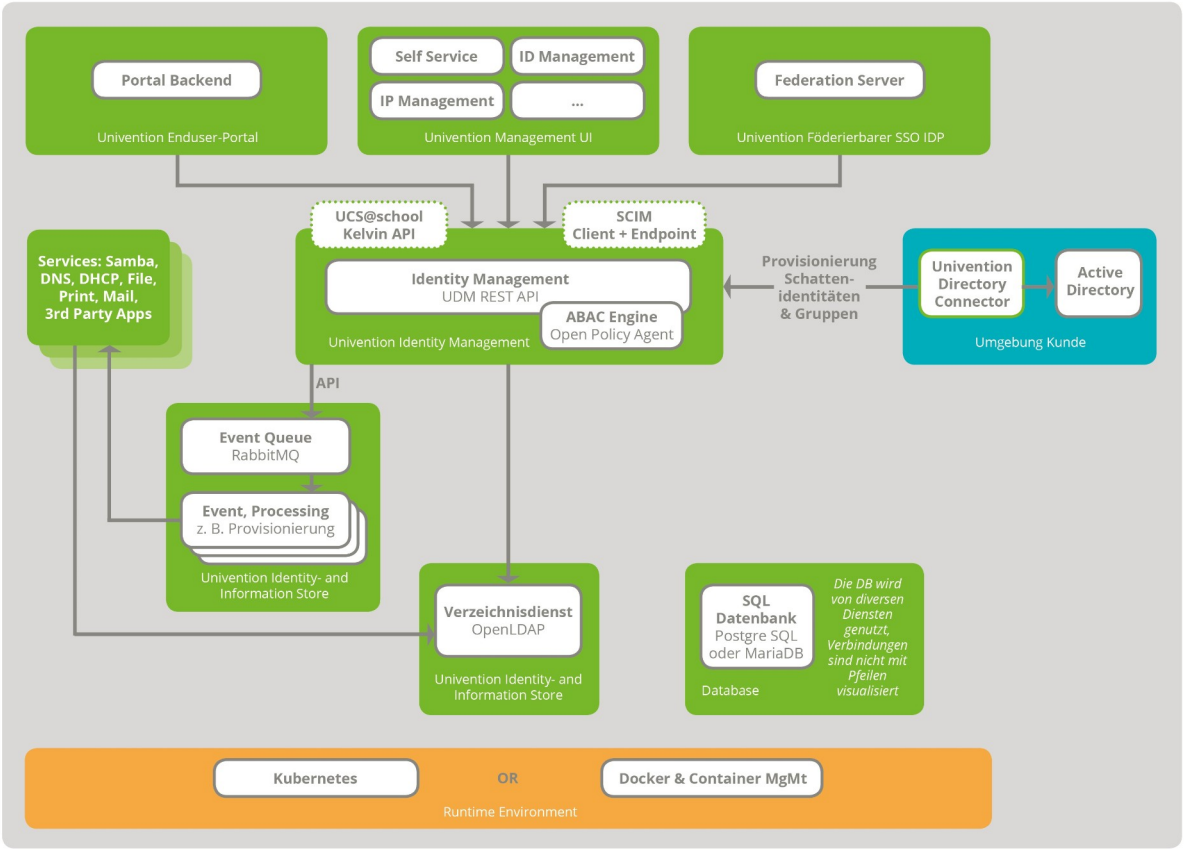

Abb.5 Gesamtarchitektur UCS

4 Auswahl von Projekt-Referenzen

Ministerium für Bildung, Jugend und Sport des Landes Brandenburg

Identity- und Accessmanagement für bis zu 300.000 Benutzer (Lehrkräfte sowie Schüler und Schülerinnen)

SUSE Software Solutions Germany GmbH

Identity- und Accessmanagement sowie Self Service für 200.000 Identitäten im OpenSUSE Build Service und integrierten Diensten

Orange S.A.

Identity- und Accessmanagement für aktuell ca. 31 Millionen Benutzer der Orange Telekom und Integration mit bzw. Provisionierung in ca 15 angebundene Systeme

Ministerium für Bildung, Wissenschaft und Kultur des Landes Schleswig-Holstein

Identity- und Accessmanagement sowie Service-Portal für 25.000 Benutzer (Lehrkräfte) und aktuell ca. 70.000 Schülerinnen und Schüler

Univention GmbH | Mary-Somerville-Straße 1 | 28359 Bremen | Tel +49 (0) 421 22232-0 | info@univention.de | www.univention.de