



**Technische Berufsschule Zürich TBZ**  
**Höhere Fachschule**  
Sihlquai 101  
8090 Zürich

# Smart User Management

Diplomand: Patrick Seifert  
Klasse: ITSE16b  
Schulexperte: Gerd Gesell  
Firmenexperte: Steven Glogger  
Firma: Swisscom (Schweiz) AG



Patrick Seifert

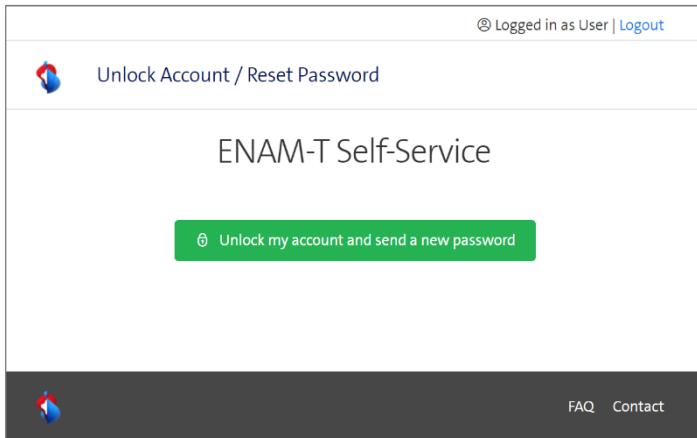


## Ausgangslage

Das Usermanagement auf über 160 Systemen wird zurzeit manuell verwaltet. Diese Systeme bieten keine einheitliche Lösung für eine Benutzerverwaltung und sind nicht mit der Microsoft Active Directory (AD) Lösung kompatibel. Aus diesem Grund wurde das Produkt "Ericsson Network Access Management" (ENAM) im Auftrag von Swisscom erweitert. Da ENAM nicht an das AD angebunden werden kann, wurde eine Microsoft Access Datenbank aufgebaut, in welcher alle Benutzer und Berechtigungen erfasst wurden. Die Datenbank wird für das Auffinden von gelöschten Benutzern und Auslösen von Audits verwendet. Somit ist das Usermanagement zwar zentral,

jedoch nicht automatisiert und die Konsistenz nicht gewährleistet.

Der Zeitaufwand für das Erstellen eines neuen Benutzers beträgt ungefähr 15 Minuten und das zurücksetzen eines Passworts und entsperren des Accounts ungefähr 5 Minuten. Zusätzlich werden noch 3 bis 4 Arbeitstage pro Jahr für die Auditierung und Bereinigung der Berechtigungen beansprucht. Im Schnitt werden in einem Monat 15 neue Berechtigungen vergeben und 5 Passwörter zurückgesetzt oder Accounts entsperrt. Hochgerechnet auf ein Jahr ergibt dies zusammen mit der Auditierung einen Aufwand von ungefähr 81 Mannstunden.



## Ziel

Das Projekt hat sich zum Ziel gesetzt, die Konsistenz der Berechtigungen zu gewährleisten, die Microsoft Access Datenbank abzulösen und möglichst viele manuelle Prozesse im Bereich der Benutzerverwaltung zu automatisieren.

## Umsetzung

Um dieses Ziel zu erreichen, mussten Schnittstellen zu ENAM und dem AD gebaut werden. Aufgrund der grossen Anzahl an Modulen und der Kompatibilität in der iAPC wurde für die Umsetzung die Programmiersprache Python verwendet. Die iAPC ist eine auf dem Open-Source Projekt CloudFoundry basierende Lösung.

Damit die aktiven Berechtigungen bequem und securitykonform in der internen "Identity and Access Management"-Applikation verwaltet werden können, mussten die ENAM-Rollen im AD abgebildet werden. Prozesse wurden im internen Wiki dokumentiert. Zusätzlich wurde ebenfalls im Wiki ein FAQ erstellt, welches Benutzeranfragen auf ein Minimum reduzieren soll.

## Fazit

Mit der neu entwickelten Lösung erfüllt die Benutzerverwaltung auf den verwalteten Systemen die aktuellen Security Anforderungen. Neu werden Accounts, welche im AD deaktiviert wurden, automatisch auch auf ENAM deaktiviert und Accounts, welche nicht mehr im AD vorhanden sind, automatisch gelöscht. Somit wurde das Risiko von Zugriffen, welche nicht mehr sein sollten, eliminiert.

Die Verarbeitung eines Auftrages nimmt nun weniger als eine Minute in Anspruch. Die restlichen Schritte wurden vollständig automatisiert. So können die Benutzer ihr ENAM Passwort selbst zurücksetzen und ihren Account selbstständig entsperren. Dadurch konnte der Verwaltungsaufwand um 97% reduziert werden. Genauso wichtig ist auch, dass sich die betroffenen Mitarbeiter wieder auf ihre Hauptaufgaben fokussieren können und sich nicht mehr mit einer Microsoft Access Datenbank herumschlagen müssen.

