SAP PRESS

SAP® Business Technology Platform – Sicherheit und Berechtigungen

- Anwendungen, Schnittstellen und die Cloud-Plattform absichern
- Administration der Neo- und Cloud-Foundry-Umgebung
- Mit vielen konkreten Beispielen und Checklisten

Martin Koch
Siegfried Zeilinger

Rheinwerk Publishing

Kapitel 2

Sicherheit auf der SAP Business Technology Platform im Überblick

Sicherheit beginnt mit der Wahl sicherer Übertragungstechnologien für Daten und geht weiter mit der Identifikation von Benutzern bis hin zur Vergabe von Rechten. Die Wartung und Konfiguration der Benutzerverwaltung sollte dabei nicht unabhängig von der eigenen Infrastruktur sein. Benutzer sollten sich auch in der Cloud mit den gewohnten Berechtigungen anmelden können, und wenn ein Benutzer nicht mehr gültig ist, sollten das auch die Cloud-Anwendungen und -Services mitbekommen. Integration auf technischer Ebene ist also Voraussetzung, um die Anwendungen auch fachlich nahtlos zu integrieren.

Dieses Kapitel führt in die Sicherheitsmechanismen der SAP Business Technology Platform (SAP BTP) ein, beginnend in Abschnitt 2.1 mit der sicheren Kommunikation. Anschließend gehen wir in Abschnitt 2.2 und Abschnitt 2.3 auf die verschiedenen Authentifizierungs- und Autorisierungsmöglichkeiten ein. Dabei erläutern wir die Unterschiede zwischen der Neo- und der Cloud-Foundry-Umgebung. In Abschnitt 2.4 erläutern wir Ihnen, wie Sie Benutzer mit den SAP Cloud Identity Services als Identitäten verwalten und sicherstellen, dass diese die richtigen Berechtigungen haben. Wir gehen auch auf das SCIM-Protokoll ein, das beim Verwalten von Benutzern bzw. Identitäten in verteilten Architekturen verwendet wird. Schließlich stellen wir in Abschnitt 2.5 die Governance-Funktionen vor, die beim Erkennen und Migrieren kritischer Berechtigungen helfen können. In Abschnitt 2.6 finden Sie eine Checkliste, mit der Sie die grundlegende Absicherung der SAP BTP prüfen können.

2.1 Sichere Kommunikation

Sicherheit ist fundamental bei der Kommunikation zwischen Cloud-Systemen und zwischen Cloud- und On-Premise-Systemen. Einerseits muss auf Anwenderseite Vertrauen in die Sicherheit bestehen, andererseits muss sichergestellt werden, dass Daten auf dem Kommunikationsweg nicht von Dritten mitgelesen oder manipuliert werden können.

Consumer-Bereich

Sichere Kommunikation stand in der Vergangenheit, vor allem im Consumer-Bereich, häufig nicht im Fokus. Das lag vor allem daran, dass sichere Kommunikation aufseiten der Anbieter mit zusätzlichen Kosten verbunden ist und entsprechendes Wissen erfordert. Seit einiger Zeit behandelt Google in den Suchergebnissen sichere Webseiten bevorzugt. Seitdem hat diesbezüglich bei vielen Serviceanbietern ein Umdenken stattgefunden.

Geschäftsanwendungen

In Geschäftsanwendungen ist eine sichere Kommunikation unerlässlich und seit Jahrzehnten nicht diskutierbar. Wenn es um die Absicherung der Kommunikation geht, werden häufig die Abkürzungen SSL, TLS und HTTPS genannt. Häufig werden diese Protokolle verwechselt oder falsch interpretiert. Als Grundlage dienen ihnen symmetrische und asymmetrische Verschlüsselungsverfahren, die wir im Folgenden erklären. Außerdem geben wir einen Überblick über das ISO/OSI-Schichtenmodell, auf dem das TCP/IP-Protokoll basiert, das für Cloud-Anwendungen von essenzieller Bedeutung ist. Nachdem wir Sie in die technischen Grundlagen eingeführt haben, erläutern wir, wie mit den verschiedenen Protokollen und Zertifikaten auf der SAP BTP umgegangen wird.

2.1.1 Grundlagen der sicheren Kommunikation

Um die Wichtigkeit sicherer Kommunikation zu veranschaulichen, führen wir ein triviales Beispiel an, das in der Literatur sehr häufig verwendet wird. Stellen Sie sich folgendes Szenario vor: Sie möchten eine Nachricht auf dem Postweg an einen bestimmten Empfänger oder eine Empfängerin senden. In diesem Szenario würde eine unsichere Kommunikation dem Versand Ihrer Nachricht per Postkarte entsprechen. Diese kann von jeder beteiligten Person auf dem Transportweg, wie beispielsweise dem Briefträger oder der Postbotin, mitgelesen werden. Wenn Sie die Nachricht in einem Briefkuvert an den Empfänger senden, entspricht das dagegen einer sicheren Kommunikation. Nur der oder die Empfänger*in kann die Nachricht lesen, vorausgesetzt das Briefkuvert wird auf dem Transportweg nicht geöffnet.

HTTP vs. HTTPs

In der digitalen Welt entspricht der unverschlüsselte Nachrichtenaustausch dem *HTTP-Protokoll* (Hypertext Transfer Protocol). Jeder Netzwerkknoten kann eine Nachricht auf diesem Weg im Klartext mitlesen. Der verschlüsselte Nachrichtenaustausch entspricht dem *HTTPS-Protokoll* (Hypertext Transfer Protocol Secure). Damit kann zwar auch jeder Netzwerkknoten die Nachricht lesen, jedoch ist diese verschlüsselt und nach aktuellem Stand der Technik ohne Besitz des privaten Schlüssels nur mit immenser Rechenleistung zu knacken.

Verschlüsselung

Basis für die verschlüsselte Kommunikation nach dem *Open-Systems-Interconnection-Modell* der *International Organization for Standardization* (ISO/OSI-Schichtenmodell) sind die symmetrische und asymmetrische Verschlüsselung:

- **Symmetrische Verschlüsselung**
  Bei symmetrischer Verschlüsselung kommt ein einziger Schlüssel zum Einsatz, der sowohl dem Sender- als auch dem Empfängersystem einer Nachricht bekannt sein muss. Der Sender verschlüsselt die Nachricht mit dem Schlüssel, und der Empfänger entschlüsselt die Nachricht mit demselben Schlüssel.

  Die älteste und wohl auch bekannteste Verschlüsselung, die *Caesar-Verschlüsselung*, geht auf das Jahr 100 v. Chr. zurück. Sie wurde nach Gaius Julius Caesar benannt, der diese Art der Verschlüsselung für die militärische Korrespondenz verwendete. Bei der Caesar-Verschlüsselung wird eine einfache Ersetzung (*Substitution*) verwendet.

  Natürlich haben sich die Anforderungen an die Verschlüsselung in der Zwischenzeit geändert. Heutzutage zählen *Data Encryption Standard* (DES), *Triple DES*, *Advanced Encryption Standard* (AES), Blowfish und *International Data Encryption Algorithm* (IDEA) zu den bekanntesten symmetrischen Verschlüsselungsalgorithmen. Für die Qualität der Verschlüsselung ist vor allem die Schlüssellänge von entscheidender Bedeutung. Eine größere Schlüssellänge erfordert aber auch eine höhere Rechenleistung zur Ver- und Entschlüsselung. Die größte Herausforderung der symmetrischen Verschlüsselung ist der Austausch der Schlüssel zwischen Sender und Empfänger. Jeder Netzwerkknoten, der zwischen Sender und Empfänger angesiedelt ist, könnte die Nachricht entschlüsseln, sofern der Schlüssel bekannt ist.
- **Asymmetrische Verschlüsselung**
  Bei asymmetrischer Verschlüsselung besitzen sowohl der Sender als auch der Empfänger ein Schlüsselpaar, das aus einem geheimen (private) und einem öffentlichen (public) Schlüssel besteht. Der Sender kann den Inhalt der Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsseln. Nur der Besitzer des geheimen Schlüssels, in unserem Fall der Empfänger, kann die Nachricht mit dem geheimen Schlüssel entschlüsseln. Asymmetrische Verschlüsselung bietet Sicherheit, hat aber den Nachteil, dass sie signifikant langsamer ist als die symmetrische Verschlüsselung.

Eine Kombination aus symmetrischen und asymmetrischen Verschlüsselungsverfahren bildet die Grundlagen der modernen und sicheren Netzwerkkommunikation.

SSL/TLS

Secure Socket Layer (SSL) wurde in der Version 1.0 von Netscape im November 1994 veröffentlicht und ist im ISO/OSI-Schichtenmodell zwischen der Applikations- und Transportschicht angesiedelt. Nur neun Monate später wurde SSL in der Version 2.0 vorgestellt. Im Laufe der Zeit wurden einige Sicherheitslücken bekannt. Die Version 3.0 des Protokolls sorgte bereits 1996 dafür, dass diese Lücken behoben wurden und neue sicherere Cipher-Suites (Sammlungen von Algorithmen und Protokollen) mit längeren Schlüssellängen und neuen Algorithmen bereitstanden.

Inzwischen wurde SSL zu Transport Layer Security (TLS) weiterentwickelt. Es handelt sich dabei im Wesentlichen um ein symmetrisches Verfahren zur sicheren Datenübertragung. Der Einsatz von SSL/TLS wird im Umfeld von SAP-Cloud-Anwendungen vorausgesetzt und ist standardmäßig ohne weitere Aktivierung in der Konfiguration der SAP BTP nutzbar.

2.1.2 SAP Destination Service

Die SAP BTP bietet sowohl in der Neo- als auch in der Cloud-Foundry-Umgebung den *SAP Destination Service* an. Er wird verwendet, um Dienste über Standardprotokolle anzusprechen.

Folgende Protokolle werden unterstützt:

- HTTP/HTTPS
- RFC
- Mail
- LDAP

Die angesprochenen Dienste können entweder über ein öffentliches Netzwerk direkt erreichbar sein oder sich in der On-Premise-Landschaft des Kunden befinden und über den Cloud Connector angesprochen werden.

Destinationen

Die Funktionsweise des SAP Destination Service kann man grundsätzlich mit der der RFC-Destinationen (Remote Function Call) in ABAP-Systemen vergleichen, die über die Transaktion SM59 gepflegt werden. Die Destinationen sorgen dafür, dass die Konfiguration der Verbindungen nicht hart codiert in der Anwendung durchgeführt werden muss. Stattdessen kann die Konfiguration in der Applikation über den Namen der Destination ausgelesen und dynamisch vorgenommen werden.

Abhängig von der Umgebung können Destinationen auf der SAP BTP auf unterschiedlichen Ebenen angelegt und gepflegt werden. Wir zeigen Ihnen im Folgenden die Anlage und Verwaltung in der Neo- und der Cloud-Foundry-Umgebung.

Destinationen in der Neo-Umgebung

In der Neo-Umgebung können Destinationen gleichzeitig auf drei Ebenen konfiguriert werden:

- auf Ebene des Subaccounts
- auf Anwendungsebene
- auf Ebene der Subskription eines Service (Java oder HTML5)

Das bedeutet, dass es möglich ist, auf mehr als einer Konfigurationsebene ein und dasselbe Ziel einer Kommunikation zu definieren.

Ebene des Consumer-Subaccounts

Soll das Ziel für einen bestimmten Subaccount zugänglich sein (und nur dort), wird die Destination im SAP BTP Cockpit im Bereich **Connectivity • Destinations** angelegt (siehe Abbildung 2.1).

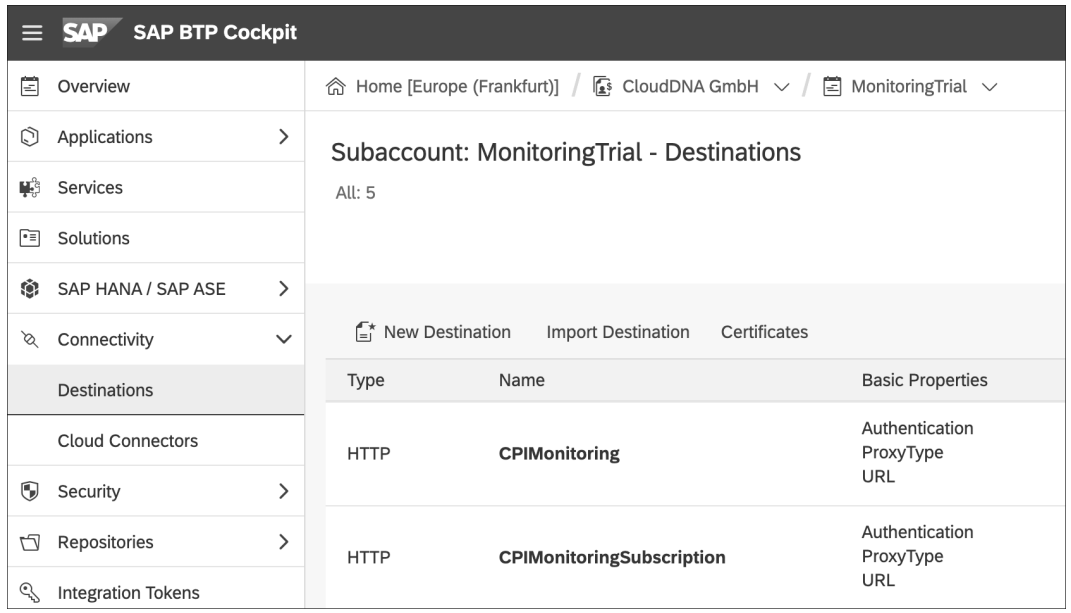

Abbildung 2.1 Anlage einer Destination auf Ebene des Subaccounts in der Neo-Umgebung

Wie Sie Destinationen konfigurieren, erfahren Sie in Abschnitt 5.5, »Einrichtung des SAP Destination Service«.

Anwendungsebene

Bezieht sich das Ziel auf eine Anwendung und den Subaccount des jeweiligen Anbieters (*Anbieter-Subaccount*), wird sie im Rahmen der Konfiguration des jeweiligen Service angelegt. In diesem Fall ist die Destination unabhängig von dem Consumer-Subaccount, in dem die Anwendung läuft. Abbildung 2.2 zeigt exemplarisch die Destinationsübersicht einer mobilen

Anwendung in den *SAP Mobile Services*. Eine neue Destination legen Sie hier über den Button **New Destination** an.

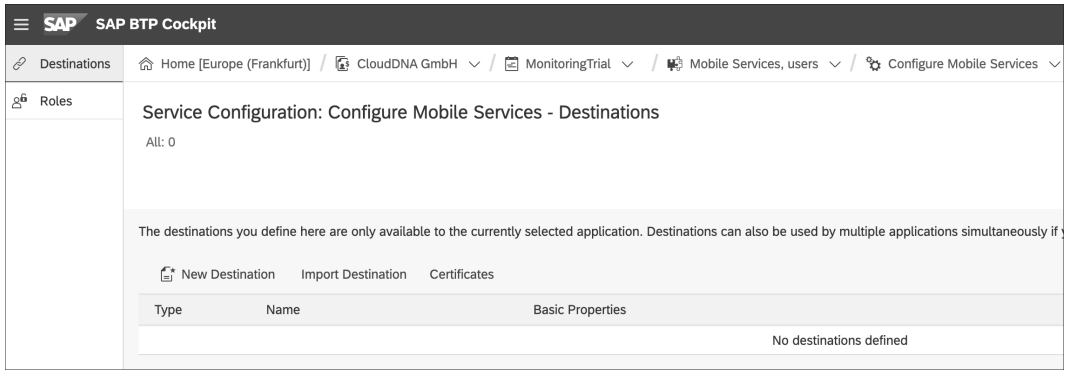

Abbildung 2.2 Destinationen auf Ebene einer Anwendung in der Neo-Umgebung

Ebene der Subskription

Bezieht sich das Ziel sowohl auf die Anwendung als auch auf den Anbieter-Subaccount und den Subaccount des Kunden (*Consumer-Subbaccount*), wird sie auf Ebene der Subskription angelegt. Dieser Fall stellt eine Besonderheit dar, da die Applikation in einem dedizierten Subaccount bereitgestellt und von diesem abonniert wird. Die Applikation wird nicht im Subaccount des Kunden installiert. Die Konfiguration einer solchen Destination erfolgt auf Ebene der abonnierten Anwendung, in Abbildung 2.3 beispielsweise SAP Cloud Portal Service. Auch hier finden Sie unter **Destinations** eine Übersicht der Destinationen und können über den Button **New Destination** eine neue Verbindung anlegen.

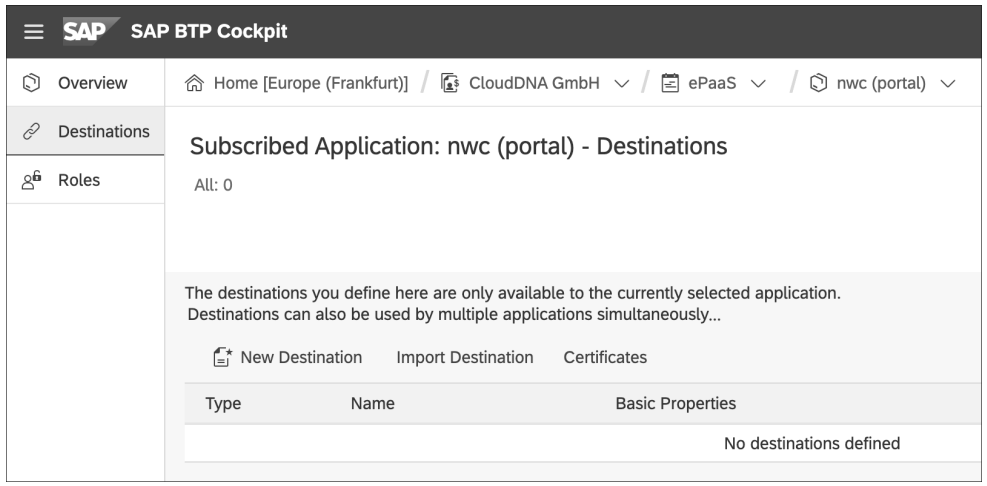

Abbildung 2.3 Destinationen auf Ebene der Subskription in der Neo-Umgebung

Die Laufzeitumgebung versucht, die Destinationen in folgender Reihenfolge zu finden: Subskription, Consumer-Subaccount, Anwendungsebene.

Typen von Destinationen

In der Neo-Umgebung können folgende Arten von Destinationen verwendet werden:

- **HTTP**
  Eine HTTP-Destination ermöglicht die Datenkommunikation über das HTTP-Protokoll sowohl für Internet- als auch für On-Premise-Verbindungen.
- **RFC**
  Eine RFC-Destination ermöglicht Verbindungen zu ABAP-on-Premise-Systemen über das RFC-Protokoll unter Verwendung des Java Connectors (JCo) und des Cloud Connectors.
- **LDAP**
  Eine LDAP-Destination ermöglicht es, eine LDAP-basierte (Lightweight Directory Access Protocol) Benutzerverwaltung zu aktivieren, sofern ein LDAP-Server im On-Premise-Netzwerk betrieben wird.
- **Mail**
  Eine Destination dieses Typs ermöglicht es, einen E-Mail-Provider für das Senden und Empfangen von E-Mails über die Protokolle Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP) oder Post Office Protocol (POP3) anzubinden.

Destinationen in der Cloud-Foundry-Umgebung

In der Cloud-Foundry-Umgebung können Destinationen auf der Ebene des Subaccounts definiert werden. Die Destination wird dabei für den gesamten Subaccount angelegt. Das verwendete Kommunikationsprotokoll und weitere Eigenschaften wie die Authentifizierungsmethode, der Proxy-Typ und eine URL werden dabei angegeben.

Ebene des Consumer-Subaccounts

Bezieht sich das Ziel auf einen bestimmten Subaccount, wird die Destination im SAP BTP Cockpit im Bereich **Connectivity • Destinations** angelegt (siehe Abbildung 2.4). Vergleichen Sie diese Umgebung mit der Neo-Umgebung in Abbildung 2.1, erkennen Sie, dass SAP versucht hat, eine einheitliches Benutzererlebnis in beiden Umgebungen zu schaffen. Die Anlage erfolgt hier demnach auf die gleiche Weise, wie in Abschnitt 5.5, »Einrichtung des SAP Destination Service«, weiter beschrieben.

Typen von Destinationen

In der Cloud-Foundry-Umgebung können ausschließlich HTTP-, RFC- oder Mail-Destinationen angelegt werden. LDAP-Destinationen werden in dieser Umgebung nicht unterstützt.

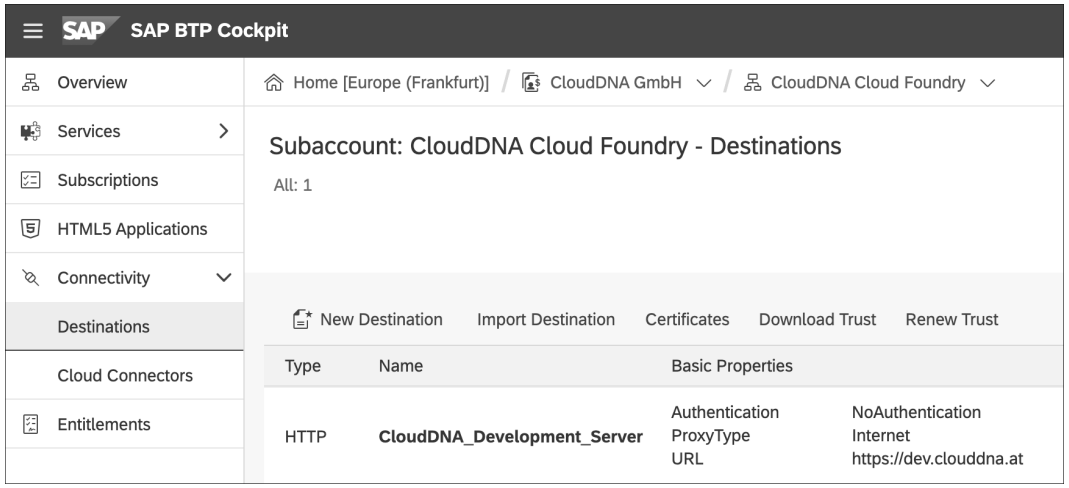

Abbildung 2.4 Destinationen auf Ebene des Subaccounts in der Cloud-Foundry-Umgebung

Neben der Anlage über das SAP BTP Cockpit besteht sowohl in der Neo- als auch in der Cloud-Foundry-Umgebung die Möglichkeit, Destinationen unter Verwendung der Kommandozeile anzulegen. Darüber hinaus lassen sich Destinationen über eine OData-API anlegen.

2.1.3 Zertifikatsbehandlung in Destinationen

Verwendung von Nicht-Standard-Zertifikaten

In der SAP BTP sind bereits Stammzertifikate der renommierten Zertifizierungsstellen vorhanden. Sie werden im *Standard-Truststore* vorgehalten. Hier ist SAP den gleichen Weg gegangen wie die renommierten Browserhersteller, die ebenfalls ein Set an Zertifikaten mit den Browsern ausliefern, denen vertraut wird. Möchten Sie wie im Beispiel von Abbildung 2.5 eine Destination zu einem HTTPS-Endpunkt verwenden, dessen Zertifikate nicht im Standard-Truststore liegen, ist das eine potenzielle Fehlerquelle, die jedoch bei der Anlage der Destination nicht direkt erkennbar ist. Bei restriktiver Auslegung in Ihrem Unternehmen wäre es umgekehrt nötig, Root-Zertifikate, denen nicht vertraut wird, zu entfernen.

Verbindungstest ausführen

Klicken Sie in diesem Fall auf den Button **Check Connection**, um einen Verbindungstest auszuführen. Nun wird Ihnen eine Fehlermeldung vom Typ SSL-Handshake angezeigt (siehe Abbildung 2.6). Das bedeutet, dass die Aushandlung von Schlüsselinformationen nicht funktioniert hat, weil die Vertrauensbeziehung fehlt.

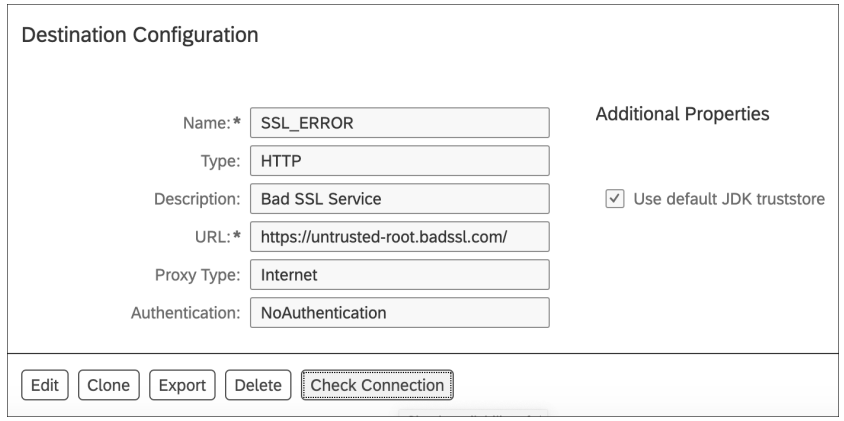

Abbildung 2.5 Destination mit nicht vertrauenswürdigem Endpunkt

Abbildung 2.6 Fehlermeldung bei Auftreten eines SSL-Handshakes

Kundeneigener Truststore

Das Problem lässt sich einfach lösen, indem Sie einen kundeneigenen Truststore verwenden. Entfernen Sie dazu in der Destinationskonfiguration das Häkchen bei der Option **Use default JDK truststore**. Nun haben Sie die Möglichkeit, eine eigene **Trust Store Location** auszuwählen und das zugehörige Passwort einzugeben (siehe Abbildung 2.7).

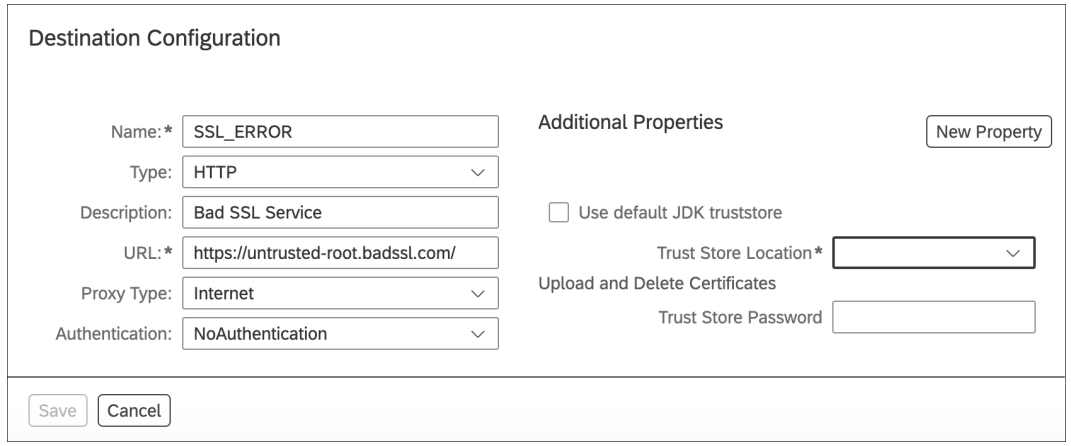

Abbildung 2.7 Verwendung eines kundeneigenen Truststores

Der Truststore kann beispielsweise über Standard-Java-Befehle angelegt werden. Sie können dazu aber auch Werkzeuge mit einer grafischen Benutzeroberfläche verwenden. Ein frei verfügbares Werkzeug zur Administration von Truststores ist beispielsweise *KeyStore Explorer*, erhältlich unter *https://keystore-explorer.org*.

Truststore hochladen

Nachdem Sie einen Truststore angelegt haben, klicken Sie auf den Link **Upload and Delete Certificates**, um den neuen Truststore hochzuladen. In Abbildung 2.8 sehen Sie, wie ein Truststore hochgeladen wird.

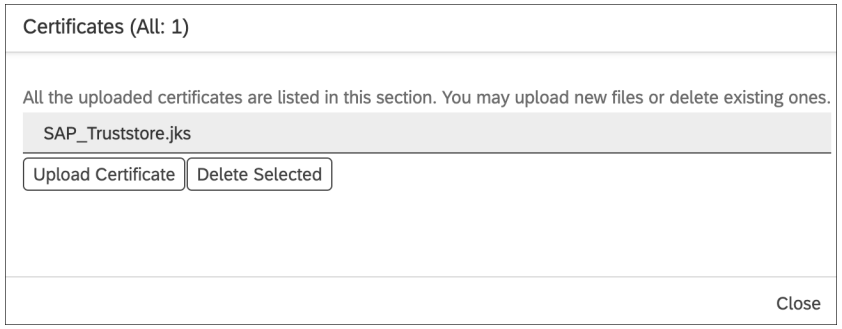

Abbildung 2.8 Hochladen eines kundeneigenen Truststores

In Abbildung 2.9 wird gezeigt, wie der kundeneigene Truststore in einer Destination zu hinterlegen ist.

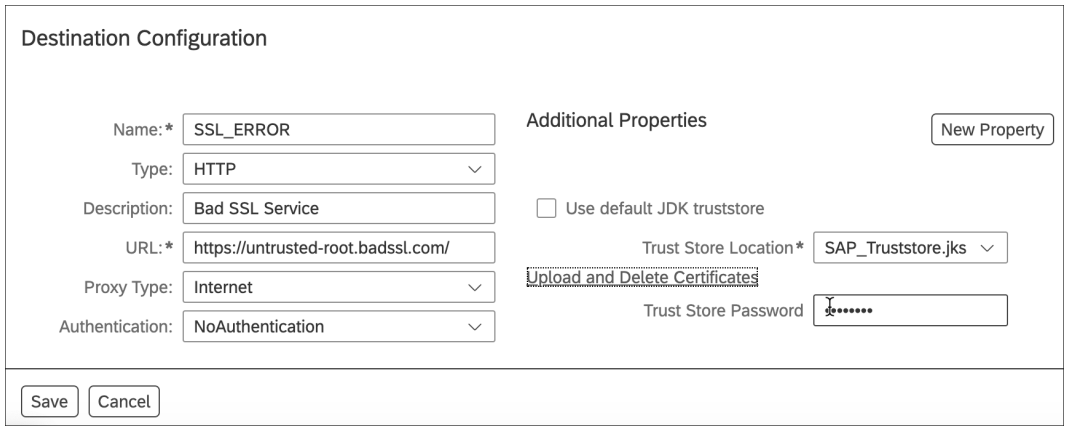

Abbildung 2.9 Konfiguration mit kundeneigenem Truststore

In Abbildung 2.10 sehen Sie das Ergebnis des Verbindungstests bei Verwendung eines kundeneigenen Truststores.

Abbildung 2.10 Verbindungstest mit kundeneigenem Truststore

2.2 Authentifizierung

Benutzername und Passwort

Authentifizierung ist der Prozess der Validierung und Bestätigung, ob ein Benutzer tatsächlich derjenige ist, für den er sich ausgibt. Passwörter sind die am häufigsten genutzte Authentifizierungsmethode. Wenn ein Anwender oder eine Anwenderin für sein oder ihr Benutzerkonto bzw. den Benutzernamen das richtige Passwort eingibt, geht das System davon aus, dass die Identität gültig ist, und gewährt den Zugang.

Dieses einfache Authentifizierungsverfahren ist jedoch anfällig für sogenannte *Brute-Force-Angriffe*. Dabei versucht ein Angreifer so lange, sich mit unterschiedlichen Passwörtern anzumelden, bis das richtige Passwort gefunden wird. Häufig werden die Passwörter bei solchen Angriffen nicht zufällig gewählt, sondern aus einer Liste mit häufig verwendeten Passwörtern gelesen. Brute-Force-Angriffe können dadurch erschwert werden, dass Benutzerkonten nach einer bestimmten Anzahl an fehlerhaften Anmeldeversuchen gesperrt werden.

Passwortrichtlinien

Eine weitere Maßnahme ist es, starke Passwörter mittels Passwortrichtlinien zu erzwingen. Passwörter für den Zugriff auf SAP-Anwendungen sollten sich stets aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen zusammensetzen. Zusätzlich sollten die Passwörter in regelmäßigen Abständen geändert werden. Sie sollten zusätzlich zu den Passwortrichtlinien auch eine Liste mit Wörtern und Begriffen pflegen, die in Passwörtern nicht verwendet werden dürfen.

Andere Technologien wie Client-Zertifikate, Biometrie, One-Time-Tokens oder eigene Authentifizierungsanwendungen können ebenfalls zur Authentifizierung herangezogen werden. Die SAP BTP bietet Ihnen an dieser Stelle sehr viel Flexibilität. Als Standardtechnologie werden Client-Zertifikate auf Basis von X.509 eingesetzt.

Client-Zertifikate

Bei Verwendung von *Client-Zertifikaten* wird die Identität der Benutzer durch den Austausch eines digitalen Zertifikats überprüft. Das Zertifikat wird von einer vertrauenswürdigen Stelle ausgestellt und eindeutig einem Benutzerkonto zugeordnet. SAP bietet Ihnen mit dem *SAP Passport* beispielsweise die Möglichkeit, ein digitales Client-Zertifikat für Ihren S-User

zu erstellen. Damit können Sie sich in der Folge an diversen SAP-Webseiten, dem SAP Support Portal und auch an der SAP BTP anmelden. Detaillierte Informationen dazu finden Sie im SAP Support Portal auf der Seite *http://s-prs.de/v809802*.

Multi-Faktor-Authentifizierung

In bestimmten Fällen erfordern Systeme die erfolgreiche Überprüfung von mehr als einem Faktor bzw. Merkmal, bevor der Zugriff gewährt wird. In diesen Fällen spricht man von einer *Multi-Faktor-Authentifizierung* (MFA). Sie wird häufig eingesetzt, um die Sicherheit im Vergleich zu einer klassischen Passwortauthentifizierung zu erhöhen. Bei der Anmeldung wird ein zusätzlicher Identitätsnachweis verlangt. Dabei werden typischerweise folgende Faktoren verwendet:

- SMS-Token
- Hardware-Token
- Software-Token
- Authentifizierungs-Apps
- Telefonanruf
- FIDO2-Sicherheitsschlüssel

Diese zusätzlichen Authentifizierungen und Verifizierungen werden in der Regel durch den Identity Provider vorgenommen, bei dem dazu entsprechende Komponenten zu aktivieren sind. Die verschiedenen Möglichkeiten bei den Identity Providern erklären wir im Anschluss.

2.2.1 Identity Provider für die SAP Business Technology Platform

Im Kontext der SAP BTP stellt ein *Identity Provider* den Benutzerspeicher bereit. Darin werden sowohl die Benutzer für den Zugriff auf die Subaccounts, etwa zur Administration oder Entwicklung, als auch für den Zugriff auf die Geschäftsapplikationen gespeichert. Bei der Wahl des Identity Providers bietet Ihnen die SAP BTP große Flexibilität. Abbildung 2.11 zeigt die verschiedenen Möglichkeiten.

Es wird zwischen dem Plattform-Identity-Provider und einem Anwendungs-Identity-Provider unterschieden.

Plattform-Identity-Provider

Als Plattform-Identity-Provider für die SAP BTP wird standardmäßig der SAP ID Service verwendet, es kann aber auch der *Identity Authentication Service* verwendet werden (siehe Abbildung 2.12). Im Identity Authentication Service werden die Benutzer über den kundeneigenen Benutzerspeicher (*Corporate User Store*) authentifiziert, ohne separat angelegt werden zu müssen. Ein kundeneigener Identity Provider ist bei dieser Variante nicht zulässig.

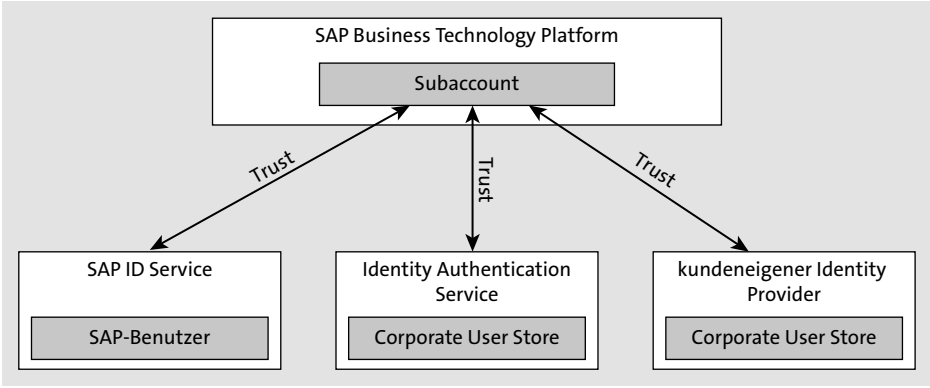

Abbildung 2.11 Identity Provider für die SAP BTP

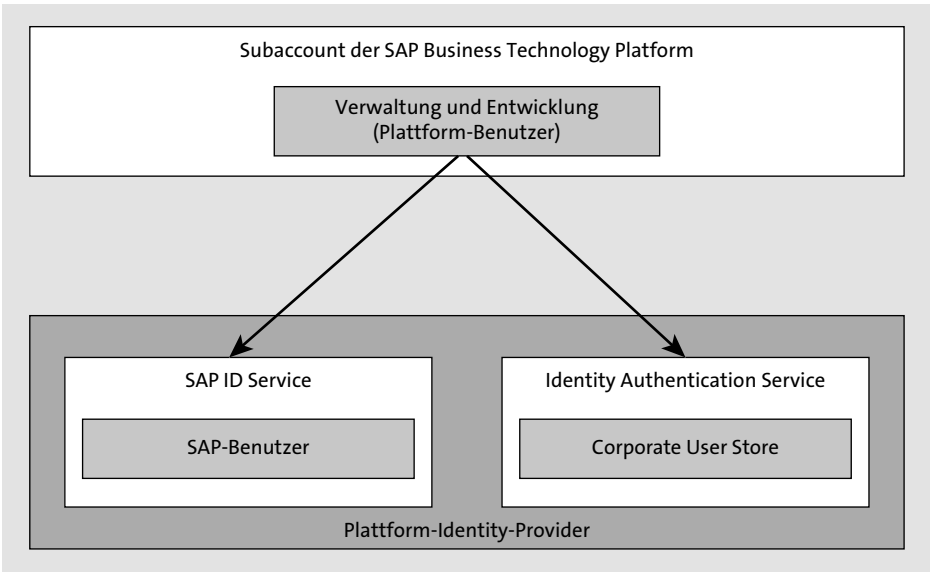

Abbildung 2.12 Plattform-Identity-Provider für die Benutzer eines Subaccounts

Der Plattform-Identity-Provider zeichnet sich durch folgende Eigenschaften aus:

- Er stellt die Benutzerbasis für den Zugriff auf den Subaccount bereit.
- Er wird im SAP BTP Cockpit, in verschiedenen Entwicklungswerkzeugen und in der Kommandozeile verwendet.
- Standardmäßig wird der SAP ID Service verwendet.
- Optional kann der Identity Authentication Tenant und damit der Identity Authentication Service verwendet werden.

- Benutzer, die im Plattform-Identity-Provider verwaltet werden, sind typischerweise Administrations- und Entwicklungsbenutzer.

Anwendungs-Identity-Provider

Der Anwendungs-Identity-Provider dient der Authentifizierung der Anwender*innen bzw. der Konsument*innen einer Anwendung, die auf der SAP BTP läuft. Als Anwendungs-Identity-Provider kann neben dem SAP ID Service und dem Identity Authentication Service auch ein kundeneigener Identity Provider (*Custom Identity Provider*) verwendet werden (siehe Abbildung 2.13). Der kundeneigene Identity Provider muss zwingend ein SAML-basierter Identity Provider sein, wie beispielsweise *Microsoft Azure Active Directory*.

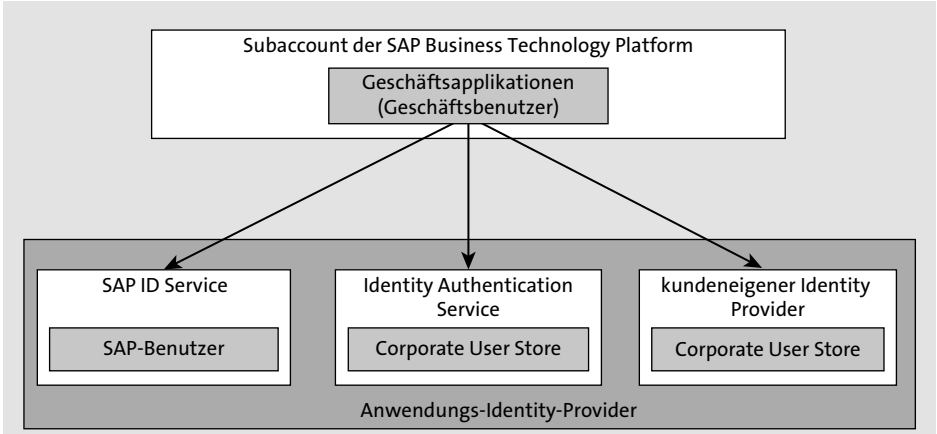

Abbildung 2.13 Anwendungs-Identity-Provider für die Nutzung in einem Subaccount

Der Anwendungs-Identity-Provider zeichnet sich durch folgende Eigenschaften aus:

- Er stellt die Benutzerbasis für den Zugriff auf Applikationen in einem Subaccount der SAP BTP bereit.
- Er wird für den Zugriff von Anwender*innen auf Benutzeroberflächen, Anwenderwerkzeugen und für die App-zu-App-Kommunikation verwendet.
- Standardmäßig wird der SAP ID Service verwendet.
- Optional können der Identity Authentication Tenant oder ein Corporate Identity Provider eines Drittanbieters verwendet werden.
- Benutzer, die mit dem Anwendungs-Identity-Provider verwaltet werden, sind typischerweise Benutzer von Endanwender*innen.

SAP ID Service

Standardmäßig ist die SAP BTP mit einer Vertrauensbeziehung zum SAP ID Service vorkonfiguriert. Das heißt, der SAP ID Service wird sowohl als Plattform-Identity-Provider als auch als Anwendungs-Identity-Provider verwendet. Von Ihrer Seite sind dazu mit Ausnahme der Zuordnung der Benutzer zum Subaccount keine weiteren Konfigurationen erforderlich. Für die Verwendung des SAP ID Service fallen keine zusätzlichen Kosten an.

Der SAP ID Service verwaltet die Benutzer der offiziellen SAP-Seiten, einschließlich der SAP-Entwickler- und Partner-Community. Die Benutzer können entweder über einen Self-Service oder über das SAP Support Portal durch einen berechtigten Benutzer innerhalb der eigenen Organisation angelegt werden.

Der SAP ID Service besteht aus folgenden Komponenten:

- zentraler Benutzerspeicher für alle Identitäten, die Zugriff auf geschützte Ressourcen der Anwendung erfordern
- standardbasierter Single-Sign-on-Service (SSO), mit dem sich Benutzer nur einmal anmelden müssen und einen nahtlosen Zugriff auf alle Anwendungen erhalten, die über die SAP BTP bereitgestellt werden

Kundeneigene Identity Provider

Optional kann sowohl in der Neo- als auch in der Cloud-Foundry-Umgebung ein kundeneigener Identity Provider verwendet werden. Für die Verwendung eines solchen Identity Providers fallen abgesehen von der Lizenz keine Kosten im Zusammenhang mit den Services der SAP BTP an.

Identity Authentication Service

Eine weitere Option ist die Verwendung des Identity Authentication Service als Plattform-Identity-Provider. Dieser Service kann in der Rolle des Plattform-Identity-Providers als Proxy für unternehmensinterne Benutzerspeicher, wie beispielsweise ein LDAP-Verzeichnis, verwendet werden. Er kann aber auch als Proxy für Identity Provider von Drittanbietern wie Microsoft Azure Active Directory verwendet werden. Der Identity Authentication Service wird in Abschnitt 2.4.1 ausführlicher behandelt. Für die Verwendung dieses Service muss eine entsprechende Lizenz erworben werden. Die für die Verrechnung verwendete Metrik ist die Anzahl der Anmeldungen.

Unterstützte Authentifizierungsszenarien

Folgende Szenarien werden von der SAP BTP zur Authentifizierung der Benutzer über den Identity Provider unterstützt:

- Standardidentitätsverbund durch den SAP ID Service
- Identitätsverbund durch den Identity Authentication Tenant
- Identitätsverbund durch einen Corporate Identity Provider

Standard-identitätsverbund

Sie können den SAP ID Service auch als Identity Provider für Ihr Identitätsverbundszenario verwenden. Die Vertrauensbeziehung zum SAP ID Service ist auf der SAP BTP, wie bereits erwähnt, standardmäßig vorkonfiguriert, sodass Sie ihn ohne weitere Konfiguration verwenden können. Optional können Sie auf der SAP BTP zusätzliche Vertrauenseinstellungen konfigurieren, wie z. B. die Registrierung des Service-Providers, Rollenzuordnungen zu Benutzern und Gruppen usw.

Die Verwendung des SAP ID Service für einen Standardidentitätsverbund wird in Abbildung 2.14 dargestellt. Möchte ein Benutzer Zugriff auf die SAP BTP bekommen, erfolgt die Authentifizierung aber über den SAP ID Service und wird mittels Trust von der SAP BTP als vertrauenswürdig eingestuft. Ein Zugriff ist also möglich, wenn der SAP ID Service eine positive Authentifizierung bestätigt hat.

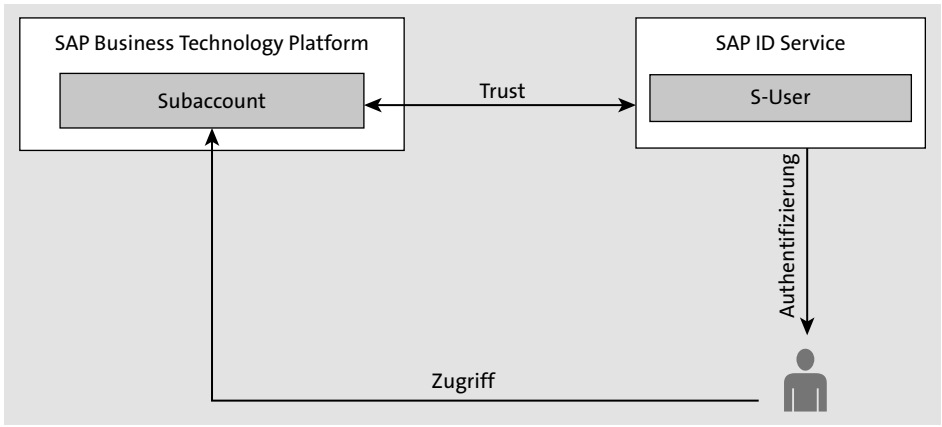

Abbildung 2.14 Ablauf der Authentifizierung mit SAP ID Service als Identity Provider

Identity Authentication Tenant

Wenn Sie Subaccount-Benutzer (Mitglieder) aus Ihrer unternehmenseigenen Benutzerbasis verwenden möchten, anstatt S-User für diese Benutzer anzulegen, können Sie den Identity Authentication Tenant als Identity Provider für Ihre Anwendungen verwenden. Identity Authentication ist ein Cloud-Service für das Lebenszyklusmanagement der von Ihnen verwalteten Identitäten. Damit haben Sie die Möglichkeit, Ihre eigene Benutzerbasis in die SAP BTP zu integrieren. Außerdem können Sie ein Corporate Branding (z. B. die Integration des Unternehmenslogos auf der Authentifizierungsseite) nutzen und Identity Provider sozialer Medien wie Facebook, Twitter, Google oder LinkedIn verwenden. Damit schaffen Sie die Basis für die Bereitstellung der Benutzer in verschiedenen Cloud- und On-Premise-Applikationen.

Der Identity Authentication Tenant (d. h. Ihre Instanz des Identity Authentication Service) steht innerhalb Ihres Global Accounts allen Subaccounts zur Verfügung (siehe Abbildung 2.15).

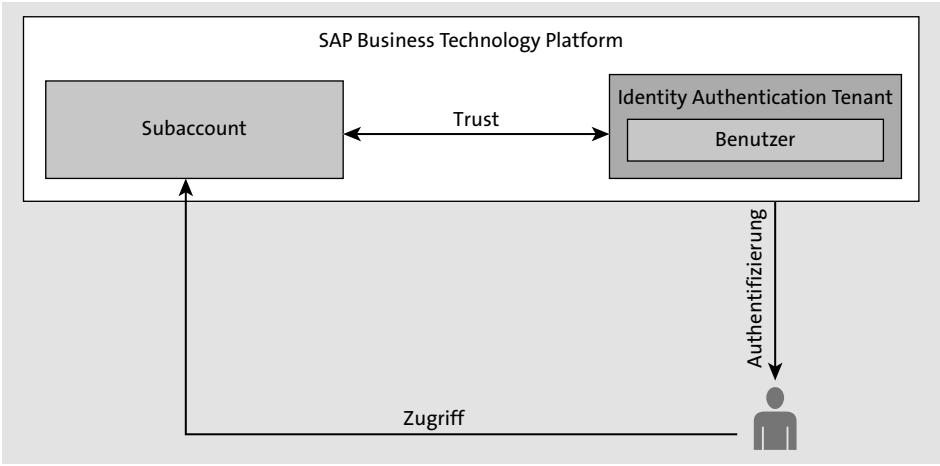

Abbildung 2.15 Verwendung des Identity Authentication Tenants zur Authentifizierung im Identitätsverbund

Identity Provider des Unternehmens

Neben der Verwendung des SAP ID Service und des Identity Authentication Service besteht die Möglichkeit, dass die Anwendungen der SAP BTP die Authentifizierung und die Identitätsverwaltung an einen bestehenden Identity Provider innerhalb Ihres Unternehmens (einen *Corporate Identity Provider*) delegieren. Dieser kann die Mitarbeitenden Ihres Unternehmens beispielsweise gegen einen unternehmensweiten Verzeichnisdienst authentifizieren. Ihre Mitarbeitenden und gegebenenfalls Kunden und Partner haben so die Möglichkeit, sich mit ihren gewohnten Benutzerinformationen an der Cloud-Anwendung anzumelden. Alle von der SAP BTP benötigten Informationen über einen Benutzer können mit dem Anmeldevorgang auf der Grundlage eines bewährten und standardisierten Sicherheitsprotokolls sicher weitergegeben werden.

In diesem Szenario besteht keine Notwendigkeit, zusätzliche Systeme zu verwalten, die sich um die Synchronisierung oder Provisionierung von Benutzerkonten zwischen dem Unternehmensnetzwerk und der SAP BTP kümmern. Es ist lediglich eine Vertrauensbeziehung, ein sogenannter *Trust*, zwischen dem Subaccount der SAP BTP, auf dem die Anwendung läuft, und Ihrem Corporate Identity Provider herzustellen. Dieses Szenario wird in Abbildung 2.16 dargestellt.

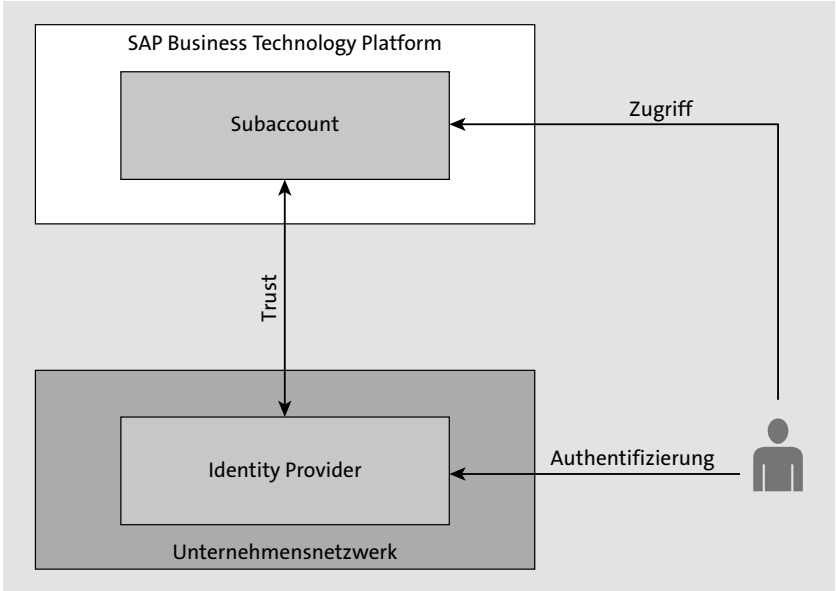

Abbildung 2.16 Corporate Identity Provider im Identitätsverbund

Konfiguration des Identity Providers in der Neo-Umgebung

Die Konfiguration des Plattform-Identity-Providers erfolgt ebenso wie die des Anwendungs-Identity-Providers im SAP BTP Cockpit auf Ebene des Subaccounts. In der Neo-Umgebung wechseln Sie hierzu in den Bereich **Security • Trust** (siehe Abbildung 2.17).

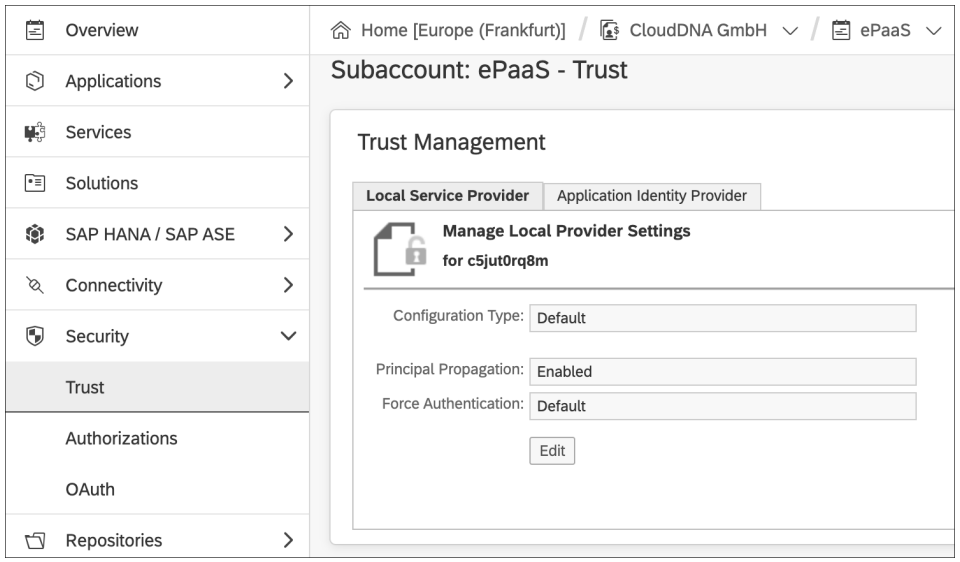

Abbildung 2.17 Trust-Konfiguration im Subaccount der Neo-Umgebung

SAP Platform Identity Provider Service

Falls die Registerkarte **Platform Identity Provider** nicht sichtbar ist, muss zunächst der *SAP Platform Identity Provider Service* für die SAP BTP auf Ebene des Subaccounts aktiviert werden:

1. Navigieren Sie dazu, wie in Abbildung 2.18 dargestellt, im Subaccount in den Bereich **Services**, und suchen Sie nach »Platform Identity Provider«.

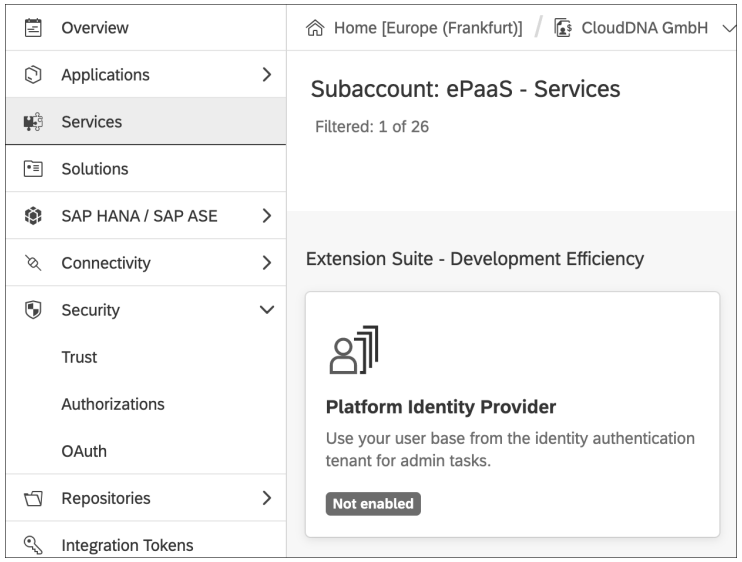

Abbildung 2.18 Kachel zur Aktivierung des SAP Platform Identity Provider Service

2. Klicken Sie auf die Kachel **Platform Identity Provider**, um in die Servicedetails abzuspringen.
3. Dort klicken Sie auf den Button **Enable** (siehe Abbildung 2.19).

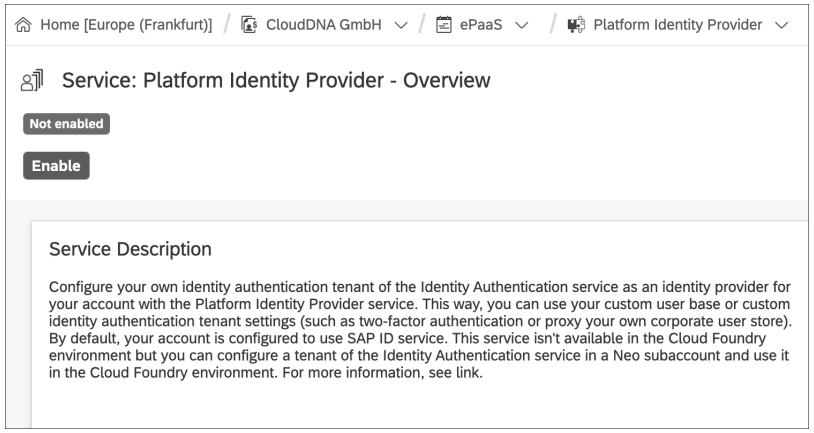

Abbildung 2.19 SAP Platform Identity Provider Service aktivieren

Die Aktivierung des SAP Platform Identity Provider Service führt dazu, dass der SAP ID Service als Standard-Plattform-Identity-Provider hinterlegt wird. Dies erkennen Sie daran, dass auf der Registerkarte **Platform Identity Provider** als **Name** die URL *https://accounts.sap.com* hinterlegt ist (siehe Abbildung 2.20).

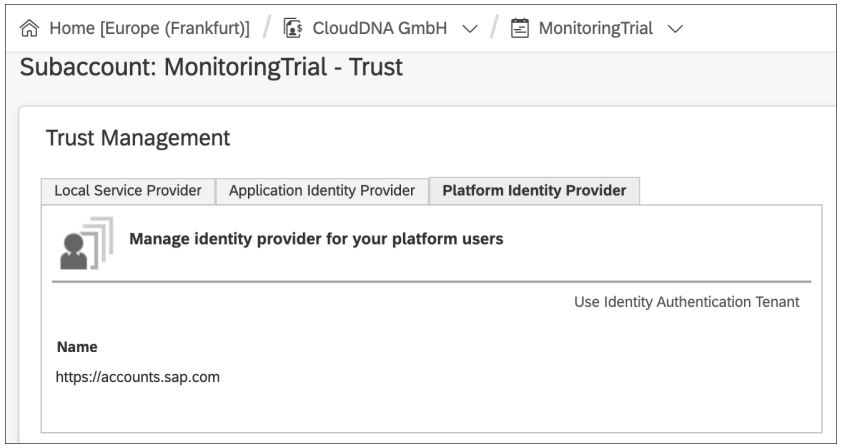

Abbildung 2.20 Standardeinstellung für den Plattform-Identity-Provider

Identity Authentication Tenant

Klicken Sie auf den Link **Use Identity Authentication Tenant**, wenn Sie den Identity Authentication Tenant als Plattform-Identity-Provider verwenden möchten. Dass der Identity Authentication Tenant als Plattform-Identity-Provider verwendet wird, erkennen Sie daran, dass der Button **Cockpit** für den Absprung in das SAP BTP Cockpit und der Button **Administration Console** für den Absprung in die Administrationskonsole sichtbar sind (siehe Abbildung 2.21).

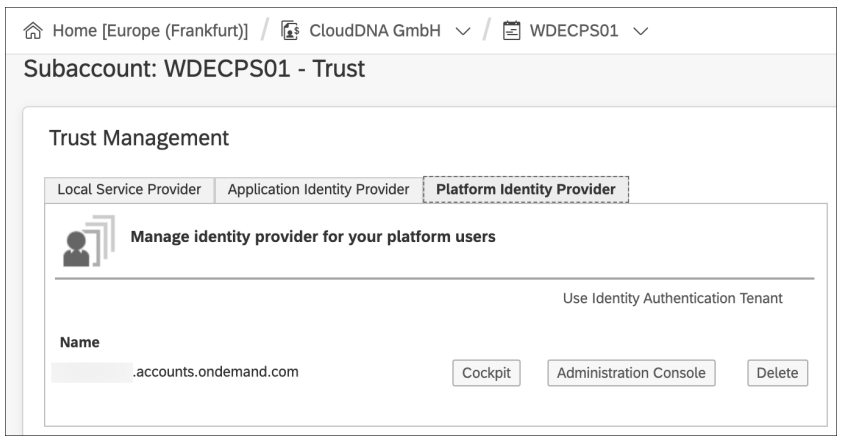

Abbildung 2.21 Identity Authentication Tenant als Plattform-Identity-Provider konfigurieren

Sie können die Verbindung zwischen Ihrem SAP-BTP-Subaccount und dem Identity Authentication Tenant durch einen Klick auf den Button **Delete** löschen.

Konfiguration des Identity Providers in der Cloud-Foundry-Umgebung

In der Cloud-Foundry-Umgebung der SAP BTP erfolgen sowohl die Konfiguration des Plattform-Identity-Providers als auch die des Anwendungs-Identity-Providers auf Ebene des Subaccounts im Bereich **Security • Trust Configuration**.

Standard-Identity-Provider

Der SAP ID Service ist auch hier als Default-Identity-Provider vorkonfiguriert (siehe Abbildung 2.22). Wenn Sie stattdessen den Identity Authentication Service als Plattform-Identity-Provider verwenden möchten, müssen Sie zunächst eine Vertrauensbeziehung zwischen dem Cloud-Foundry-Subaccount und dem Identity Authentication Service herstellen. Die Konfiguration dieser Vertrauensbeziehung zeigen wir in Abschnitt 4.3.2, »Plattform-Identity-Provider einrichten«.

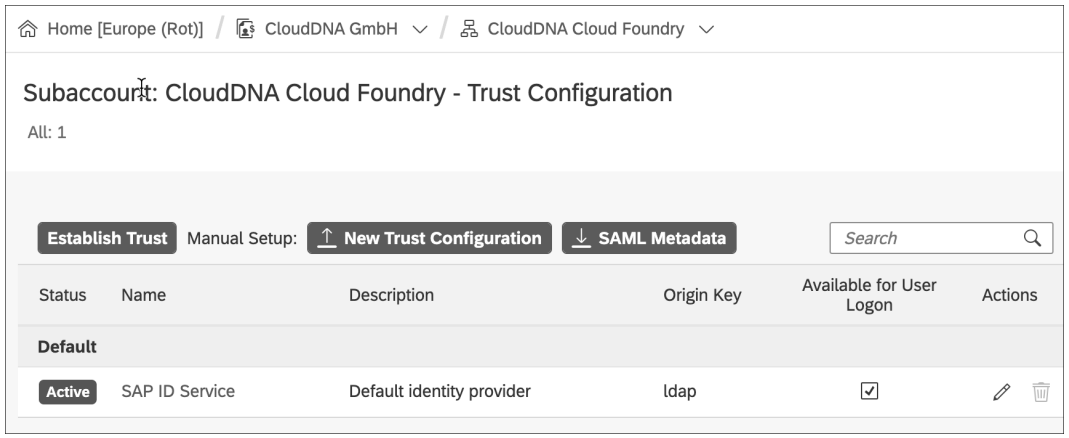

Abbildung 2.22 Default-Identity-Provider in der Cloud-Foundry-Umgebung

Konfiguration von Identity Providern von Drittanbietern

Identity Provider von Drittanbietern werden typischerweise in der Rolle eines Anwendungs-Identity-Providers verwendet. Wechseln Sie zur Konfiguration im Bereich **Security • Trust** auf die Registerkarte **Application Identity Provider**. Grundsätzlich kann ein Identity Provider eines Drittanbieters jedoch auch als Plattform-Identity-Provider verwendet werden. Dafür ist es erforderlich, den Identity Authentication Service als Proxy einzusetzen.

2.2.2 Lightweight Directory Access Protocol

LDAP

Das *Lightweight Directory Access Protocol* (LDAP) ist ein Netzwerkprotokoll zur Kommunikation mit einem Verzeichnisdienst. Es handelt sich bei LDAP also nicht um den Verzeichnisdienst selbst, sondern lediglich um das Zugriffsprotokoll. LDAP ermöglicht es, ein auf mehrere Server verteiltes, in einer Baumstruktur aufgebautes Verzeichnis einfach zu durchsuchen.

Datenmodell

Die hierarchische Baumstruktur des Verzeichnisdienstes ist dabei in wesentlichen Zügen vorgegeben. Das LDAP-Datenmodell ist einfach gehalten. LDAP basiert auf Objekten und folgt Ansätzen der objektorientierten Programmierung wie der Vererbung und der Polymorphie. An oberster Stelle der Verzeichnisstruktur steht immer das Wurzelelement (*Root*). Darunter kann in folgende Elemente verzweigt werden:

- `C`: Country (Länder)
- `O`: Organization (Organisationen)
- `OU`: Organisational Unit (Organisationseinheiten)
- `DC`: Domain Component (Individuen)

Individuen können Dokumente, Personen oder Gegenstände sein.

Distinguished Name

Die Bezeichnung von Objekten erfolgt durch den *Distinguished Name* (DN). Ein gültiger Distinguished Name für ein Objekt kann beispielsweise wie folgt aussehen:

```
CN=Martin Koch,OU=Beratung,DC=clouddna,DC=at
```

`CN` steht hier für Common Name. Das bedeutet, dass das Individuum Martin Koch der Organisationseinheit Beratung innerhalb der Domäne CloudDNA in Österreich zugeordnet ist. Abbildung 2.23 zeigt die Position eines Distinguished Names innerhalb eines LDAP-Hierarchiebaumes.

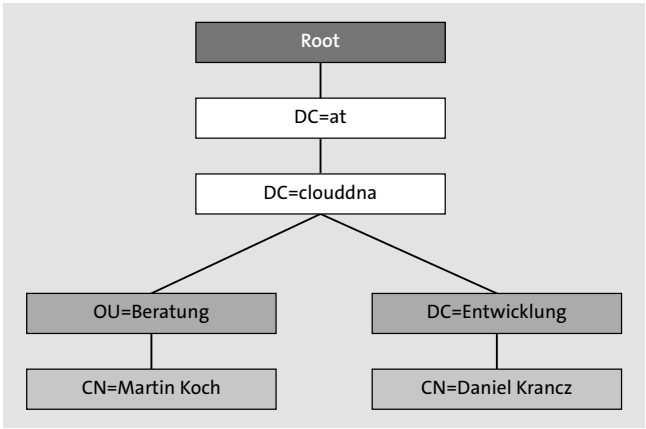

Abbildung 2.23 Beispiel für eine LDAP-Struktur

Einsatz als Benutzerspeicher

Sie können die SAP BTP so konfigurieren, dass ein vorhandenes LDAP-Verzeichnis aus einem On-Premise-System als Benutzerspeicher verwendet wird. Voraussetzung dafür ist die Verwendung des Cloud Connectors.

Haben Sie die Applikationen der SAP BTP entsprechend konfiguriert, können diese den On-Premise-Benutzerspeicher für die folgenden Tätigkeiten nutzen:

- Zugangsdaten prüfen
- Benutzersuche
- Benutzerdetails auslesen
- Gruppenzugehörigkeit

Einsatz im Identitätsverbund

Eine weitere Möglichkeit für den Einsatz von LDAP ist die Verwendung im Identitätsverbund durch den Identity Authentication Tenant. In diesem Fall agiert der Identity Authentication Service als Proxy zum On-Premise-LDAP-Verzeichnis. Voraussetzung für dieses Szenario ist die Verwendung des *Identity Authentication Add-ons*. Dieses Add-on ermöglicht die Nutzung der Schnittstelle zur Authentifizierung am Subaccount (im Gegensatz zum Identity Authentication Service, bei dem die Schnittstelle am Identity Authentification Tenant eingesetzt wird). Wechseln Sie dazu im SAP BTP Cockpit in Ihren Subaccount und suchen Sie im Bereich **Services** nach »Identity Authentication Add-on« (siehe Abbildung 2.24).

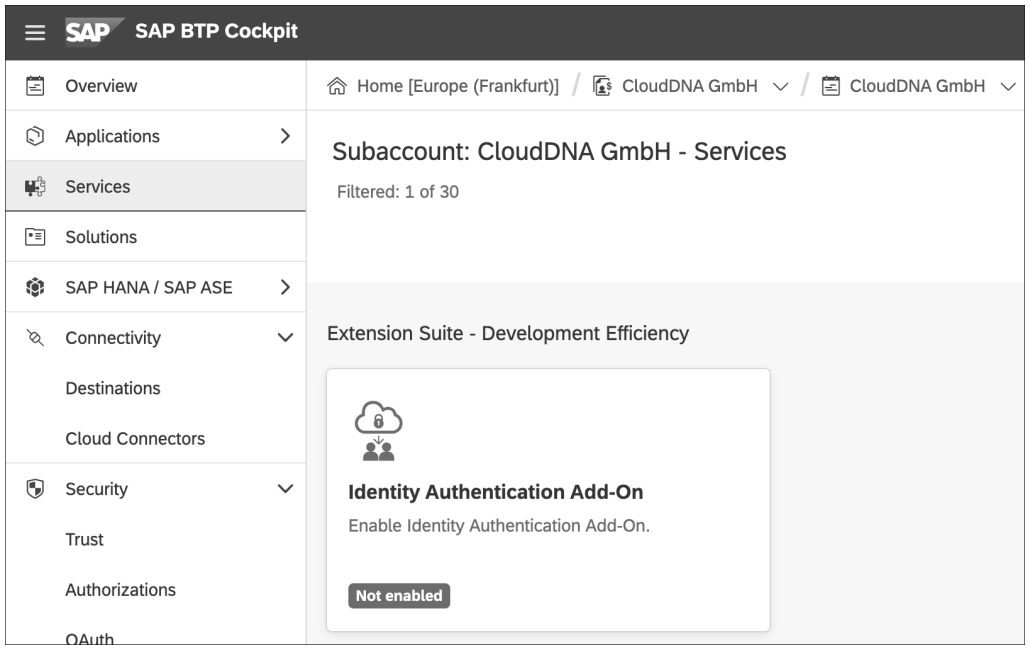

Abbildung 2.24 Kachel zur Aktivierung des Identity Authentication Add-ons

In der Detailssicht des Add-ons können Sie den Service über den Button **Enable** aktivieren.

Sofern Sie den Identity Authentication Tenant für die Verwendung eines LDAP-Servers in Ihrer On-Premise-Landschaft konfiguriert haben, fungiert das Identity Authentication Add-on als Proxy in die On-Premise-Landschaft. Es steht aktuell nur in der Neo-Umgebung zur Verfügung.

Architektur der Authentifizierung

Der Identity Authentication Tenant authentifiziert sich über das offene *OAuth*-Protokoll (siehe auch Abschnitt 2.3, »Autorisierung«) gegenüber dem Subaccount, in dem das Add-on bereitgestellt wird. Das Identity Authentication Add-on stellt anschließend eine Verbindung zum LDAP-Server über den Cloud Connector her (siehe Abbildung 2.25).

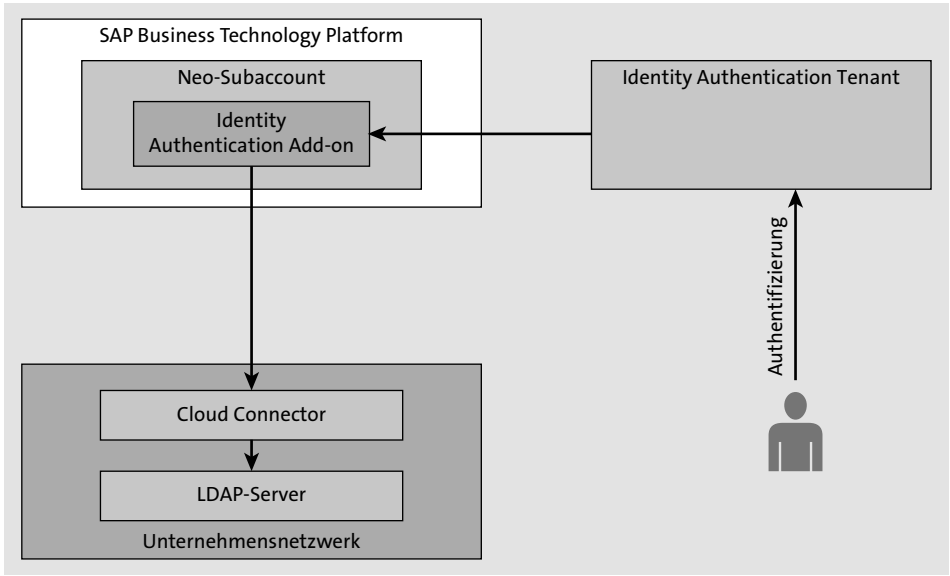

Abbildung 2.25 Benutzerauthentifizierung gegen einen On-Premise-LDAP-Server

2.3 Autorisierung

Als *Autorisierung* bezeichnet man den Prozess, um einem Benutzer die Erlaubnis zu erteilen, auf eine bestimmte Ressource oder Funktionalität zuzugreifen. Dieser Begriff wird meist synonym mit dem Begriff *Zugriffskontrolle* verwendet. Ein Beispiel für einen Autorisierungsvorgang ist es, wenn Sie jemandem die Erlaubnis erteilen, eine bestimmte Datei auf Ihrem Server herunterzuladen. Ein weiteres Beispiel ist es, wenn Sie einem einzelnen Benutzer administrativen Zugriff auf eine Anwendung gewähren.

Autorisierung und Authentifizierung

In sicheren Umgebungen erfolgt die Autorisierung immer nach der Authentifizierung. Die Benutzer müssen zunächst nachweisen, dass ihre Identität echt ist, bevor ihnen der Zugang zu den angeforderten Ressourcen gewährt wird.

In der SAP BTP werden zwei verschiedene Standards zur Autorisierung verwendet, SAML und OAuth.

SAML

Security Assertion Markup Language (SAML) ist ein offener Standard zum Austausch von Authentifizierungs- und Autorisierungsidentitäten zwischen Sicherheitsdomänen. SAML wurde 2003 in einer ersten Version veröffentlicht und 2005 als OASIS-Standard in der Version 2.0 ratifiziert.

Das entscheidende Prinzip des Standards ist die Ausstellung von sogenannten *SAML Tokens* durch einen *SAML Service Provider*. Diese Tokens werden über eine Vertrauensposition von anderen Anwendungen akzeptiert. Ein anderer Name für die SAML Tokens lautet *SAML Assertion*. Die Authentifizierung in der Neo-Umgebung der SAP BTP basiert auf SAML Tokens.

OAuth

Das Autorisierungs-Framework *OAuth 2.0* ermöglicht es einer Fremdanwendung, eingeschränkten Zugriff auf einen HTTP-Dienst zu erhalten. Die Autorisierung erfolgt dabei entweder im Namen eines Ressourcenbesitzers, indem eine Genehmigungsinteraktion zwischen dem Ressourcenbesitzer und dem HTTP-Dienst orchestriert wird, oder der Fremdanwendung wird der Zugriff in ihrem eigenen Namen erlaubt.

OAuth 2.0 vereinfach die Implementierung der Autorisierung für Client-Entwickler*innen und bietet gleichzeitig spezifische Autorisierungsabläufe für unterschiedliche Anwendungstypen. Der OAuth-2.0-Standard und dessen Erweiterungen werden von der Internet Engineering Task Force (IETF) definiert. Das Framework wird im RFC 6749 spezifiziert. RFC steht hier für *Request for Comments*, die Sammlung der Internetspezifikationen.

Rollen

OAuth definiert vier Rollen innerhalb des Autorisierungsprozesses:

- **Ressourcenbesitzer**
  Der *Ressourcenbesitzer* ist eine Einheit, die in der Lage ist, Zugang zu einer geschützten Ressource zu gewähren. Wenn der Ressourcenbesitzer eine Person ist, wird er als *Benutzer* bezeichnet.
- **Ressourcenserver**
  Der Server, auf dem die geschützten Ressourcen gehostet werden, ist in der Lage, Anfragen nach geschützten Ressourcen unter Verwendung von Zugriffs-Token anzunehmen und zu beantworten.
- **Client**
  Der Client ist eine Anwendung, die im Namen des Ressourcenbesitzers und mit dessen Genehmigung geschützte Ressourcen anfragt. Der Be-

griff *Client* impliziert keine besonderen Implementierungsmerkmale (z. B. einen Formfaktor oder die Bauart des Geräts).

- **Autorisierungsserver**
  Der Server, der nach erfolgreicher Authentifizierung des Ressourcenbesitzers und dessen Autorisierung Zugriffs-Token an den Client ausgibt, wird *Autorisierungsserver* genannt.

Um einen Zugriffs-Token anzufordern, erhält der Client die Autorisierung vom Ressourcenbesitzer. Die Autorisierung wird in Form einer Berechtigungserteilung (*Authorization Grant*) ausgedrückt. Mit dieser Berechtigung fordert der Client dann das Zugriffs-Token an (siehe Abbildung 2.26).

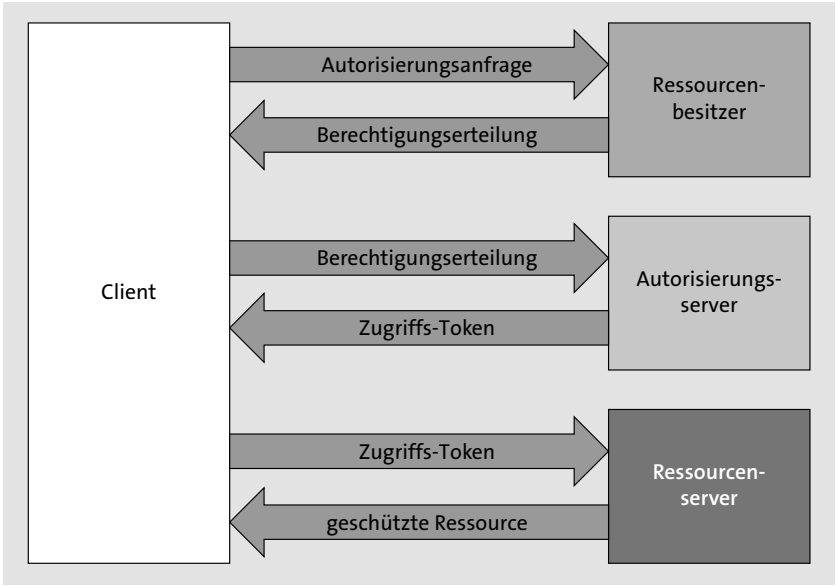

Abbildung 2.26 Ablauf des Autorisierungsprozesses mit OAuth

OAuth definiert vier Arten der Berechtigungserteilung (*Grant Types*):

- über einen Autorisierungscode
- implizite Autorisierung
- über die Anmeldedaten (Passwort) des Ressourcenbesitzers
- über die Anmeldedaten des Clients (Client Credentials)

Zusätzlich sieht OAuth einen Erweiterungsmechanismus für die Definition zusätzlicher Arten der Berechtigungserteilung vor.

Berechtigungserteilung in der SAP BTP

Die SAP BTP unterstützt in der Neo-Umgebung die folgenden Arten der Berechtigungserteilung mit OAuth 2.0:

- **Autorisierungscode**
  Bei dieser Variante gibt es einen menschlichen Nutzer oder eine Nutzerin, der oder die eine mobile Anwendung autorisiert, in seinem oder ihrem Namen auf Ressourcen zuzugreifen.
- **Client Credentials**
  Bei dieser Variante gibt es keinen menschlichen Benutzer, sondern ein Gerät gewährt die Berechtigung. In diesem Fall wird das Zugriffs-Token nur auf der Grundlage der Client-Anmeldeinformationen gewährt.

OpenID Connect

OpenID Connect ist eine Identitätsschicht, die auf dem Protokoll OAuth 2.0 basiert. Clients können damit die Identität der Anwender*innen auf Grundlage der von einem Autorisierungsserver durchgeführten Authentifizierung verifizieren und grundlegende Profilinformationen über Anwender*innen auf REST-ähnliche Weise erhalten. Durch die Verwendung des REST-Formats wird eine Weiterverwendung in Services der SAP BTP erleichtert, da für dieses Format eine Menge vorgefertigte Bibliotheken und Beispiele existieren.

Autorisierung in den Umgebungen

In der Cloud-Foundry-Umgebung der SAP BTP werden alle Services über den sogenannten *Anwendungsrouter* aufgerufen. Er ist der zentrale Einstiegspunkt für alle Anwendungen, die in der Cloud-Foundry-Umgebung ausgeführt werden. Der Anwendungsrouter wird verwendet, um statische Inhalte bereitzustellen, Benutzer zu authentifizieren und URLs umzuschreiben. Er leitet Anfragen an andere Microservices weiter oder fungiert als Proxy, wobei die Benutzerinformationen ebenfalls an Microservices weitergereicht werden.

In der Cloud-Foundry-Umgebung basiert die Authentifizierung auf dem OAuth-Protokoll. Alle Zugriffsrechte auf Anwendungen (*Application Scopes*), die dem aktuellen Benutzer gewährt wurden, werden in Form eines Tokens weitergeleitet. Dabei handelt es sich um das *JSON Web Token* (JWT). Dieses Token wird im RFC 7519 spezifiziert. Das Token wird vom Anwendungsrouter erstellt, indem dieser mit der Benutzer-Account- und Authentifizierungsinstanz der SAP BTP kommuniziert.

Einleitung

In den letzten Jahrzehnten hat sich die Informationstechnologie wesentlich verändert. Konnten wir uns beispielsweise vor 20 Jahren noch nicht vorstellen, dass Medienangebote *on demand*, also auf unmittelbare Nachfrage, bereitgestellt werden, ist es heute normal, dass in einem Haushalt mehrere Personen unterschiedliche Inhalte streamen. Die *Cloud* ist heute überall, immer verfügbar und auf allen Endgeräten. Häuser werden nicht mehr verdrahtet, sondern es reicht aus, Funknetze zu bilden. Aber was ist der Preis? Der neue Funklautsprecher hört immer mit bei allen Gesprächen, die in seiner Umgebung stattfinden. Spätestens, seit in den USA ein großer Anbieter verpflichtet wurde, die Aufzeichnungen seines Lautsprechers für ein Gerichtsverfahren zur Verfügung zu stellen, wissen wir, dass Orwell mit seinem Werk »1984« der visionäre Elon Musk seiner Zeit war.

Neue Risiken der IT

Nun gilt es, als Unternehmen den Spagat zu finden zwischen der Volldigitalisierung mit einer weitreichenden Optimierung, aber komplett neuen Risiken und einem eher konservativen, risikoaversen Ansatz, der versucht, die Risiken der Digitalisierung in Schach zu halten. In Horrorberichten liest man selbst von Universitäten, die zweistellige Millionenbeträge an Hacker zahlen, nur um ihre eigenen Daten wieder nutzen zu dürfen. Oder von Consulting-Firmen, die ihren kompletten Notebook-Bestand wegen Unbenutzbarkeit durch ein Computervirus oder eine Verschlüsselungsanwendung austauschen müssen. Es zeigt sich einerseits, dass die Digitalisierung nicht aufgehalten werden kann, aber andererseits stehen nun ganz andere Vertriebs- und Vermarktungsmöglichkeiten zur Verfügung.

Umgang mit schützenswerten Daten

Im Bereich der Geschäftsanwendungen hat Marktführer SAP den Weg in die Cloud für Großunternehmen mit Anwendungen aus dem Bereich Personalwirtschaft begonnen. *SAP SuccessFactors* und *SAP Concur* haben als Lösungen für die Verwaltung von Personalstammdaten und die Reisekostenabrechnung den Anfang gemacht. Damit wurden einerseits besonders schützenswerte Daten, aber wenig geschäftskritische Prozesse in die Cloud gehoben. Das hat dazu geführt, dass oftmals sensibelste, aber geschäftlich verhältnismäßig unkritische Daten in der Cloud verarbeitet wurden.

In den späten 1990er und frühen 2000er Jahren hat sich die Industrie mit *Outsourcing* bzw. *Outtasking* beschäftigt. Fragestellung war damals, ob man seine Systeme selbst hostet und wer Routineaufgaben übernimmt. Später war die Virtualisierung der Rechenzentren Thema. Man sprach nicht mehr von *Servern*, sondern nur mehr von *virtuellen Instanzen*, die man zwischen Sao Paulo, Los Angeles und Frankfurt nach Belieben hin- und herschieben konnte.

Cloud vs. on premise

Heute spricht man von *Cloud* vs. *on premise* und muss damit ganz ähnliche Entscheidungen in anderem Kontext treffen. Hebe ich die Datenbank in die Cloud, oder nutze ich einen Service? Welche Komponenten verbleiben on premise? Da oftmals nicht mehr transparent ist, wo die Daten genau liegen, ist es vielleicht doch nötig, etwas mehr Dokumentationen als üblich anzulegen. Es stellt sich die Frage, ob man in der Cloud noch selbst Verantwortung übernehmen muss. Oder läuft man dem Cloud-Service hinterher? Wie sicher ist es, sich auf einen Telekommunikations-Provider zu verlassen? Welche Sicherheitsrisiken geht man in Bezug auf Daten, Prozesse, Betriebsgeheimnisse etc. ein?

In diesem Zusammenhang kann nur wiederholt werden, was immer wieder gesagt wird: Die Lösungen, die ausgearbeitet werden, werden in der Regel von den Fachabteilungen beauftragt oder zumindest von den Fachabteilungen genehmigt. Wenn es um Sicherheit und Berechtigungen geht, kann man als IT-Verantwortliche*r zuarbeiten, doch die Verantwortung für die Prozesse bleibt bei den Fachabteilungen, die den Mehrwert einer cloudbasierten Lösung gegen die Anforderungen und Risiken abwägen müssen.

Dieses Buch soll Ihnen dazu sowohl als Inspiration als auch als Anleitung dienen. Wir möchten die richtigen Fragen stellen und Empfehlungen daraus ableiten. Auch wenn es ein Buch von Technikern für Techniker*innen ist, versuchen wir immer wieder einen Blick über den Tellerrand.

Zielgruppen

Wir richten uns mit diesem Buch gleichermaßen an technikaffine Einsteiger*innen in die SAP-Cloud und Profis. Sollten Sie gerade vor Ihrem ersten Cloud-Projekt stehen, finden Sie sicherlich passende Informationen. Fachlich richtet sich das Werk vornehmlich an IT-Administrator*innen. Aber auch Entwickler*innen finden hilfreiche Tipps zu relevanten Cloud-Services. Interessierte Personen aus den Fachabteilungen, die gerne über ihren Tellerrand schauen oder beispielsweise eine eigene Risikobewertung treffen wollen, werden ebenfalls fündig werden.

Der Aufbau des Buches

Wir beginnen dieses Buch mit der Positionierung von SAP und seiner Strategie im Kontext von Cloud-Produkten, um anschließend die SAP Business Technology Platform (SAP BTP) als PaaS-Angebot (Platform as a Service) von SAP detailliert vorzustellen und ihre Sicherheitsaspekte zu beleuchten. Wir betrachten dann die Verbindungen zwischen der Cloud und Ihren Unternehmensnetzwerken, bis wir uns schließlich der Administration und Absicherung einzelner Cloud-Services widmen.

Checklisten

Die meisten Kapitel schließen mit einer Checkliste ab. Anhand der Checklisten können Sie überprüfen, ob Sie die richtigen Fragen zu Ihrer hybriden

Systemlandschaft gestellt haben, und Themen gegebenenfalls noch einmal von einer anderen Seite durchdenken. Außerdem können Sie überprüfen, ob Sie beim Lesen des jeweiligen Kapitels alle wichtigen Inhalte verstanden haben. Wenn Sie beispielsweise die Neo-Umgebung der SAP BTP schon kennen, können Sie auch zuerst die entsprechende Checkliste durchgehen und so feststellen, ob das zugehörige Kapitel für Sie lesenswert wäre.

Wir stellen die Checklisten auch im Download-Bereich dieses Buches zum Herunterladen und Ausdrucken zur Verfügung. Sie finden sie auf der Seite *www.sap-press.de/5262* im Bereich **Materialien**.

Praxisszenarien

Am Ende der meisten Kapitel finden Sie außerdem Praxisszenarien, in denen wir häufige Anforderungen Schritt für Schritt durchgehen. Diese Beispiele dienen der weiteren Vertiefung und können am eigenen System ausprobiert werden.

Informationskästen

In hervorgehobenen Informationskästen finden Sie in diesem Buch Inhalte, die wissenswert und hilfreich sind, aber etwas außerhalb der eigentlichen Erläuterung stehen. Damit Sie diese Informationen sofort einordnen können, haben wir die Kästen mit entsprechenden Symbolen gekennzeichnet:

- In Kästen, die mit diesem Symbol gekennzeichnet sind, finden Sie Informationen zu *weiterführenden Themen* oder wichtigen Inhalten, die Sie sich merken sollten.

- Dieses Symbol weist Sie auf *Besonderheiten* hin, die Sie beachten sollten. Es *warnt Sie* außerdem vor häufig gemachten Fehlern oder Problemen, die auftreten können.

- Die mit diesem Symbol gekennzeichneten *Tipps* geben Ihnen spezielle Empfehlungen aus unserer Projektpraxis, die Ihnen die Arbeit erleichtern können.

- *Beispiele*, durch dieses Symbol kenntlich gemacht, weisen auf Szenarien aus der Praxis hin und veranschaulichen die dargestellten Funktionen.

Kapitel dieses Buches

Im Folgenden stellen wir Ihnen die Inhalte der einzelnen Kapitel dieses Buches vor.

In **Kapitel 1**, »Einführung in die SAP Business Technology Platform«, führen wir Sie in die SAP BTP und die damit verbundene Terminologie ein. Wir erklären die Struktur und Positionierung der Plattform und legen dabei besonderes Augenmerk auf die Relevanz und die Einordnung in die SAP-Produktstrategie. Abschließend stellen wir die Nutzungsoptionen vor.

Kapitel 2, »Sicherheit auf der SAP Business Technology Platform im Überblick«, beginnt mit einer Einführung in die verschiedenen Sicherheitsmechanismen des PaaS-Angebots von SAP. Authentifizierungs- und Autorisierungsmöglichkeiten werden eingeführt. Dabei erläutern wir die Unter-

schiede zwischen den verschiedenen Umgebungen der SAP BTP. Abschließend zeigen wir Ihnen die Anlage von Benutzerkonten und Berechtigungen auf Ebene der Global Accounts.

In **Kapitel 3**, »Sicherheit und Berechtigungen in der Neo-Umgebung konfigurieren«, beleuchten wir die Sicherheitsfunktionen in der Neo-Umgebung der SAP BTP im Detail. Wir zeigen zunächst, wie man unterschiedliche Trust-Konfigurationen einrichtet. Anschließend erläutern wir die Verwaltung von Benutzern, Rollen und Benutzergruppen.

In **Kapitel 4**, »Sicherheit und Berechtigungen in der Cloud-Foundry-Umgebung konfigurieren«, erläutern wir Sicherheitsaspekte der Cloud-Foundry-Umgebung der SAP BTP. Anhand einer Best-Practice-Implementierung zeigen wir Ihnen, wie der Betrieb sicher und günstig gestaltet werden kann.

Das **Kapitel 5**, »Cloud Connector«, widmen wir uns dem *Cloud Connector*, der zur Verbindung von Cloud- und On-Premise-Systemen eingesetzt wird. Dabei handelt es sich um eine zentrale Komponente für den Aufbau hybrider Systemlandschaften. Nachdem wir die Architektur erläutert haben, finden Sie eine Anleitung zur Installation und Konfiguration des Cloud Connectors. Die Absicherung wird detailliert beschrieben. Abschließend zeigen wir die Einrichtung des *SAP Destination Service*, der das Gegenstück zum lokal installierten Cloud Connector in der Neo- und Cloud-Foundry-Umgebung der SAP BTP bildet.

In **Kapitel 6**, »Administrationswerkzeuge der SAP Business Technology Platform«, geben wir Ihnen Empfehlungen zur Administration der SAP BTP, um die Organisation nicht mehr als unbedingt nötig zu belasten. Wir stellen Ihnen Konsolenwerkzeuge und APIs vor, die eine effiziente Administration ermöglichen.

In **Kapitel 7**, »Sicherheitsaspekte wichtiger Cloud-Services«, möchten wir Ihnen einen Überblick über die unserer Einschätzung nach wichtigsten Services der SAP BTP geben und diese unter sicherheitstechnischen Gesichtspunkten betrachten.

Zusammenfassend haben wir versucht, ein möglichst rundes und vollständiges Bild der Sicherheitsthemen im Zusammenhang der SAP BTP zu zeichnen. Wir danken Ihnen für das Interesse an unserem Buch und wünschen Ihnen viel Vergnügen bei der Lektüre!

Martin Koch und **Siegfried Zeilinger**

Auf einen Blick

Inhalt