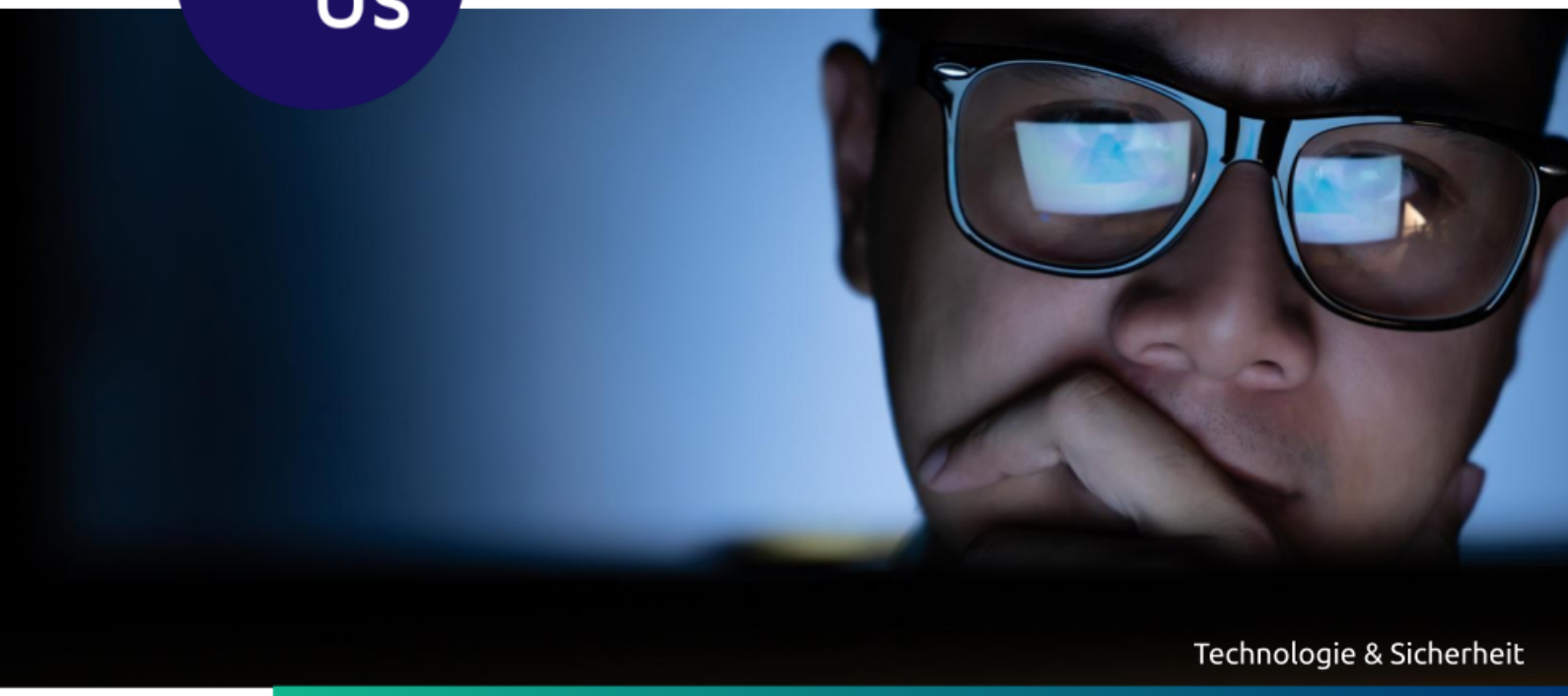

Technologie & Sicherheit

Identity and Access Management

Zugriffskontrolle in einem hochverfügbaren und verteilten System

https://innus.de

Inhalt

Identity and Access Management

In einem hochverfügbaren und verteilten System ist die Zugriffskontrolle von zentraler Bedeutung. Sie ermöglicht die transparente Verwendung aller angebotenen Funktionalitäten mittels eines Benutzerprofils. Die Verwaltung aller Rollen und Berechtigungen sowie die Authentifizierung sollten an einer Stelle gebündelt werden, um die Komplexität für einen Anwender und einen Administrator auf ein Mindestmaß zu beschränken.

Des Weiteren sollte ein hochverfügbares und skalierbares System in der Lage sein, zu jeder Zeit auf Lastveränderungen zu reagieren, um eine effiziente Nutzung der bereitgestellten Ressourcen zu gewährleisten.

innus hat zu diesem Zweck ein Identity and Access Management (IAM) implementiert, das allen beschriebenen Anforderungen bei höchstmöglicher Sicherheit Rechnung trägt. Im Folgenden werden die einzelnen Komponenten von innus.IAM genauer beschrieben.

Authorization und Resource Services

Die innus Banksuite unterscheidet zwischen zwei grundsätzlichen Servicearten: einem Authorization Service und einem Resource Service.

Ein Authorization Service verwaltet alle im System verfügbaren Berechtigungen und Rollen und authentifiziert Benutzer. Bei jedem Aufruf ermittelt er die aktuellen Privilegien eines Benutzers und stellt diese einem Resource Service zur Verfügung. Er selbst stellt keine Funktionalität im Rahmen von Geschäftsprozessen bereit. innus.IAM erfüllt diese Aufgabe innerhalb der innus Banksuite.

Ein Resource Service stellt Funktionalitäten im Rahmen von Geschäftsprozessen bereit. Auf Basis der domänengetriebenen Architektur trägt ein Resource Service die alleinige Verantwortung der von ihm bereitgestellten Ressourcen und Funktionalitäten. Das verwendete Datenmodell und zugehörige Berechtigungen werden dabei vom Resource Service verwaltet und geprüft.

Während des Bootstrapping sendet ein Resource Service notwendige Informationen über eine Message Queue an den Authorization Service. Dieser speichert die Informationen und stellt sie im Rahmen der Rollenverwaltung zur Verfügung.

Folgende Information sind Bestandteil der Nachricht:

Parameter	Typ	Hinweis	Beispiel
name	Text	Name des Service	org
version	Ziffer	Die aktuelle Version des Service	1
apiContextPath	Text	Der Kontextpfad des Service	/api/v1
permissions	Liste	Die Berechtigungen eines Service	OFFICES:READ OFFICES:EDIT OFFICES:FULL

Das Format einer Berechtigung setzt sich zusammen aus der bereitgestellten Ressource und einem der folgenden Zugriffsrechte: READ, EDIT oder FULL. Hierbei stehen die einzelnen Zugriffsrechte für folgenden Aktionen:

Zugriffsrecht	Aktion
READ	Lesen einer Ressource und ihrer Unterressourcen
EDIT	Das Anlegen neuer und das Bearbeiten bestehender Ressourcen
FULL	Vollzugriff auf alle servicespezifischen Prozesse

!HINWEIS! Das verwendete Berechtigungskonzept basiert auf einer impliziten Vererbung der einzelnen Zugriffsrechte. EDIT beinhaltet READ; FULL beinhaltet EDIT und READ.

Rollen und Benutzer

Neben der Authentifizierung von Benutzern, ist die Verwaltung von Rollen und Benutzern ein weiterer Bestandteil von innus.IAM. Hierbei liegt die volle Kontrolle über Rollen und Benutzer beim Administrator des Systems.

Eine Rolle ist die funktionsbasierte Sammlung benötigter Zugriffsrechte zur Nutzung des Systems. Innerhalb der Rollenverwaltung gibt es keine Hierarchie, was den initialen Aufwand nur leicht erhöht, aber die Komplexität bei der späteren Verwendung drastisch reduziert.

Eine Rolle besteht aus folgenden Informationen:

Parameter	Typ	Hinweis	Beispiel
identifier	Text	Die eindeutige Kennung einer Rolle	admin
name	Text	Der Name der einer Rolle	Administrator
description	Text	Erläuternde Beschreibung einer Rolle	Berechtigungen zur Verwaltung von Rollen und Benutzern
permissions	Liste	Die Zugriffsrechte einer Rollen	ORG:OFFICES:READ
state	Text	Der aktuelle Status einer Rolle	ACTIVE

Folgende Status kann eine Rolle einnehmen:

Status	Aktion
ACTIVE	Eine Rolle ist aktiv und frei zuweisbar
LOCKED	Eine Rolle ist gesperrt und kann keinem Benutzer zugewiesen werden
EXPIRED	Eine Rolle wurde gelöscht und ist somit ungültig

!EMPFEHLUNG! Rollen sollten sich an wirklichen Tätigkeitsbereichen innerhalb eines Unternehmens orientieren und nicht künstlich zusammengestellt werden.

Ein Benutzer repräsentiert eine Person oder Anwendung, welche Funktionalitäten der innus Banksuite aufruft oder ausführt.

Ein Benutzer besteht aus folgenden Informationen:

Parameter	Typ	Hinweis	Beispiel
type	Text	Der Typ eines Benutzers	USER
username	Text	Eindeutige Kennung eines Benutzers	dmayer
name	Text	Der Name eines Benutzers	Dominik Mayer

role	Text	Eindeutige Kennung einer zugewiesenen Rolle	admin
state	Text	Der aktuelle Status eines Benutzers	ACTIVE

Folgende Typen stehen zur Verfügung:

Typ	Aktion
USER	Eine natürliche Person
APP	Ein Prozess oder eine Anwendung

Folgende Status kann ein Benutzer einnehmen:

Status	Aktion
ACTIVE	Ein Benutzer ist aktiv und kann sich am System authentifizieren
LOCKED	Ein Benutzer ist gesperrt und kann sich am System nicht mehr authentifizieren
EXPIRED	Ein Benutzer wurde gelöscht und ist somit ungültig

Passwortrichtlinien

Im Rahmen der Benutzerverwaltung kann eine individuelle Passwortrichtlinie konfiguriert werden. Folgende Regeln stehen zur Auswahl:

Parameter	Typ	Hinweis	Beispiel
enabled	Boolean	Ist die Passwortrichtlinie aktiv	TRUE
minLength	Ziffer	Mindestlänge eines Passworts	6
maxLength	Ziffer	Maximale Länge eines Passworts	18
minAge	Ziffer	Gültigkeitszeitraum eines Passworts in Tagen	90
numberOf Alphabetic Characters	Ziffer	Mindestanzahl von Buchstaben	2
numberOf Special Characters	Ziffer	Mindestanzahl von Sonderzeichen	2

numberOf Digits	Ziffer	Mindestanzahl von Ziffern	2
numberOf Characteristics	Ziffer	Anzahl zu verwendender Charakteristiken	2
sequences Allowed	Boolean	Sind einfache Zeichenfolgen erlaubt, z.B. qwert, 12345	FALSE
whitespace Allowed	Boolean	Sind Leerzeichen erlaubt	FALSE

Token

Ein grundlegendes Paradigma eines Cloud Native Systems ist der Verzicht auf einen serverseitigen Zustand. Daraus ergibt sich die Notwendigkeit, mit jeder Anfrage kurzzeitig einen validen Kontext zu erzeugen.

innus.IAM nutzt hierzu JSON Web Tokens (JWT)[1]. Um ein Höchstmaß an Sicherheit zu gewährleisten, unterzeichnet innus.IAM einen Token nicht nur digital, sondern setzt auch die Empfehlungen der OWASP Foundation[2] zum Umgang mit Tokens[3] um.

Zusätzlich verwendet die innus Banksuite zwei verschiedene Token, einen externen und einen interne Token. Es werden unterschiedliche Secrets zur Erzeugung der digitalen Signatur verwendet. Der Algorithmus für die digitalen Signatur ist eine Kombination aus HMAC[4] und SHA-2[5].

Die Lebensdauer eines Tokens kann vom Administrator konfiguriert werden, dabei gelten folgen Standardwert:

Token	Benutzertyp	Lebensdauer
Extern	USER	10 Stunden
Extern	APP	90 Tage
Intern	nicht zutreffend	60 Sekunden

[1] https://tools.ietf.org/html/rfc7519
[2] https://owasp.org/
[3] https://owasp.org/www-project-cheat-sheets/cheatsheets/JSON_Web_Token_Cheat_Sheet_for_Java
[4] https://en.wikipedia.org/wiki/HMAC
[5] https://en.wikipedia.org/wiki/SHA-2

Externer Token

Nach der erfolgreichen Anmeldung, wird dem Benutzer ein externe Token zur Verfügung gestellt. Dieser Token muss bei weiteren Aufrufen im Authorization Header des HTTP-Requests mitgesendet werden.

Der externe Token dient der Authentifizierung eines Benutzers bei jedem Aufruf und beinhaltet nur notwendige Informationen zur Wiederherstellung eines validen Kontext.

!HINWEIS! Es besteht die Möglichkeit alle ausgegebenen Token mit sofortiger Wirkung invalide zu setzen und somit jede weitere Verwendung zu unterbinden.

Folgende Parameter sind Bestandteil eines externen Tokens:

Parameter	Beschreibung
iss	Der Herausgeber eines Tokens
iat	Das Datum und die Uhrzeit der Erstellung
exp	Das Ablaufdatum eines Tokens
sub	Referenz des Aufrufers
https://innus.de/rol	Die Rolle eines Benutzers während der Erzeugung eines Token
https://innus.de/fgp	Ein generierte Fingerabdruck des Aufrufers

Ein valider Kontext wird erst nach der Validierung eines Tokens erzeugt. Während der Validierung werden folgenden Prüfungen durchgeführt:

1. Ist der Authorization Header vorhanden
2. Ist die digital Signatur valide
3. Ist der Token unverändert
4. Wurde der Token von innus-IAM ausgestellt
5. Ist der Token noch innerhalb des Gültigkeitszeitraums
6. Ist der Fingerabdruck vorhanden und valide
7. Wurde der Token nach dem letzten Rücksetzen erstellt
8. Ist der Benutzer noch aktiv
9. Stimmt die aktuelle Rolle des Benutzers noch mit der Rolle zum Zeitpunkt der Tokenerstellung überein

Sollte nur eine dieser Prüfung fehlschlagen, wird keine gültiger Kontext erzeugt und der Zugriff verweigert.

Interner Token

Nachdem der externe Token validiert wurde und ein gültiger Kontext existiert erzeugt innus-IAM für jede systeminterne Weiterleitung einen internen Token. Dieser Token wird speziell für einen Resource Service erstellt und hat nur eine sehr kurze Lebensdauer.

Folgenden Parameter sind Bestandteil des internen Tokens:

Parameter	Beschreibung
iss	Der Herausgeber eines Tokens
iat	Das Datum und die Uhrzeit der Erstellung
exp	Das Ablaufdatum eines Tokens
sub	Referenz des Aufrufers
aud	Der Empfänger eines Tokens
https://innus.de/auth	Ein Liste aller servicebasierten Privilegien eines Benutzers

Die folgenden Prüfungen werden von einem Resource Service durchgeführt:

1. Ist der proprietäre Authorization Header vorhanden
2. Ist die digital Signatur valide
3. Ist der Token unverändert
4. Wurde der Token von innus-IAM ausgestellt
5. Ist der Token noch innerhalb des Gültigkeitszeitraums
6. Ist der Empfänger identisch dem Resource Server

Authentifizierung

Um die innus Banksuite verwenden zu können, ist ein Benutzerprofil notwendig. Ein Benutzerprofil bildet die Identität eines Benutzers innerhalb des Systems ab. Zur Authentifizierung werden der Benutzername und ein Passwort benötigt. Passworte werden generell verschlüsselt in der Datenbank abgelegt und nicht in Klartext geschrieben.

Bei der Authentifizierung wird der Status des Benutzers geprüft und, sollte der Benutzer nicht aktiv sein, gegebenenfalls abgewiesen. Jede Authentifizierung wird für ein späteres Audit festgehalten.

Authorisierung

Nach erfolgreicher Authentifizierung wird ein externer Token erzeugt und für den Benutzer bereitgestellt. Bei jedem weiteren Aufruf muss der Benutzer diesen Token im Authorization Header des HTTP-Requests mit senden.

Wie oben beschrieben, wird nach erfolgreicher Prüfung des externe Tokens ein interner Token erzeugt. Nach erfolgreicher Prüfung des internen Tokens durch den Resource Service nutzt dieser die übermittelten Privilegien zur Autorisierung aller Funktionen.

innus GmbH
Behringstraße 28a
22765 Hamburg
+49 40 303 77 40-0
info@innus.de