stone one
The Web Service Factory

S1 IAM

Identity & Access Management

Systemübergreifende Administration von **Rollen** und **Rechten**

Die Vernetzung von Menschen, Geräten, dem Zuhause, Autos, Maschinen und städtischer Infrastruktur nimmt rasant zu. Immer mehr Unternehmen setzen dabei auf digitale Plattformen und neue, „smarte“, Serviceangebote um ihr Geschäft durch Nutzung des „Internet of Things“ (IoT) zu optimieren und besser mit Kunden, Lieferanten, Mitarbeitern etc. zu interagieren.

In den letzten Jahren haben sich die Anforderungen an Internetdienste stark verändert. Längst sind die Zeiten vorbei, in denen Nutzer sich für jeden Dienst neu registrieren mussten. Seine Identität möchte man einmalig bei Anbietern wie Google oder Facebook verwalten und neuen Diensten lediglich Zugriff auf diese Identität gewähren.

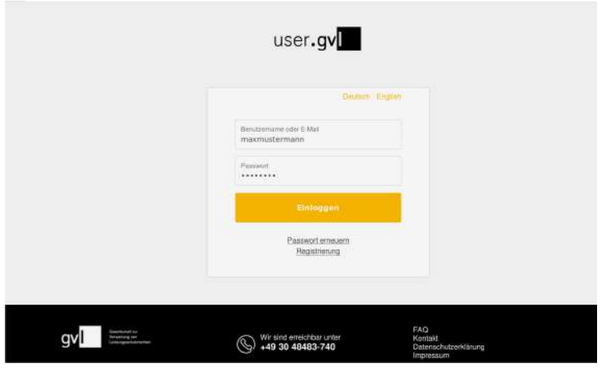
Identity- and Access Management (IAM) steht für alle Prozesse und Anwendungen bei der Administration von Nutzerdaten und die Verwaltung von Zugriffsrechten auf verschiedene Applikationen, Systeme und Ressourcen. Nutzerdaten und Zugriffsrechte müssen applikationsübergreifend administriert und verwaltet werden. Dabei ist auch die Trennlinie zwischen externen Portal-Usern und unterstützenden internen technischen Anwendungen für Unternehmensangehörige besonders zu berücksichtigen.

Um die geforderte, feine Granularität der Zugriffsrechte auf strukturiert abgelegte Dokumente und Informationen auch unter Performance-Gesichtspunkten gewährleisten zu können, ist ein Modell für Rollen, Rechte und Berechtigungen erforderlich, das sowohl komplexen Anforderungen als auch schneller Verfügbarkeit Rechnung trägt. Insbesondere bei systemübergreifenden Suchen muss außerdem ein Kompromiss im Zweifelsfall zugunsten einer schnellen Verfügbarkeit ausfallen, um den Anforderungen z.B. an Skalierbarkeit genügen zu können. Mit unserem S1 IAM Modul lässt sich eine einfache und zentral administrierbare Lösung umsetzen. Hierzu kommen spezielle IAM-Architekturen zum Einsatz, die aus mehreren Softwarekomponenten bestehen können.

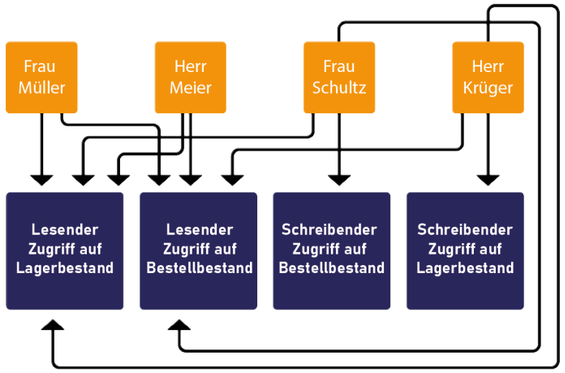
Unser auf Keycloak basierendes S1 IAM Modul bietet eine sichere und gut dokumentierte Alternative zu einer aufwendigen proprietären Eigenentwicklung. S1 IAM nutzt diese Open-Source-Software, um einfach und flexibel ein Identity & Access Management auch für mehrere Applikationen bereitzustellen, so dass nur ein einziger Identity Provider benötigt wird. Dieser agiert außerdem als Identity Broker und kann darüber auch externe Nutzerquellen nahtlos anbinden. So kann nach einer einmaligen Authentifizierung mit Single-Sign-On (SSO) auf alle Applikationen zugegriffen werden. Die Oberfläche kann passend zum Corporate Design des Kunden konfiguriert werden.

Verwaltung und Pflege vereinfachen

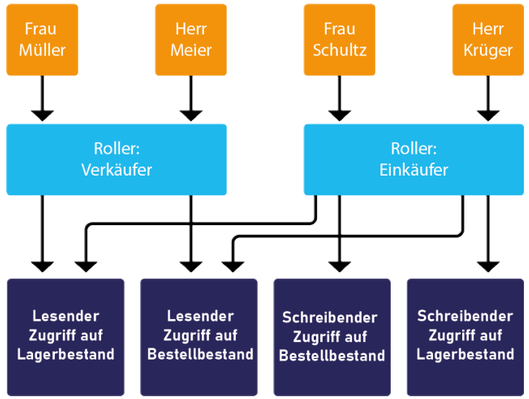
Das S1 IAM Modul vereinfacht die Verwaltung und Pflege von Benutzerkonten und Ressourcen im Netzwerk, einschließlich der Berechtigungsverwaltung für Benutzer von Anwendungen in verteilten Systemumgebungen, auch für verschiedene Lösungen und Portale. Zusätzlich zur integrierten Nutzerdatenbank können auch bestehende Nutzersysteme über Protokolle wie OpenID Connect (OIDC) oder LDAP integriert werden. Die entsprechenden Nutzerdaten werden über konfigurierbares Mapping zwischen den Systemen verbunden und – falls nötig - ggf. mittels LDAP-Schema-Erweiterungen auf ein Backend-System abgebildet.



GVL Corporate Design Login-Seite



Vergabe von Einzelrechten



Vergabe von Rollen

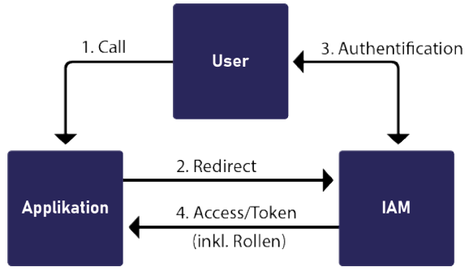
Rollen und Rechte

Eine (Benutzer-) Rolle („Role“) besteht aus einer Menge von einzelnen Rechten („Authorities“). Die Definition von Benutzerrollen ist sinnvoll, weil man auf diese Art und Weise nicht jedem einzelnen Benutzer eine Reihe von Einzelrechten zuweisen muss, die für die Ausübung seiner Tätigkeit nötig sind, sondern lediglich die Rolle. Schon allein das spart erheblichen Verwaltungsaufwand. Besonders zum Tragen aber kommt das Rollenkonzept, wenn einer Rolle Rechte entzogen bzw. Rechte hinzugefügt werden sollen, denn man muss auf diese Art und Weise eben nur die Rolle administrieren, nicht aber die Profildaten eines jeden Benutzers. Auch wenn zum Beispiel ein Mitarbeiter innerhalb eines Unternehmens die Stelle wechselt, so muss ihm lediglich die alte Rolle entzogen und die neue zugewiesen werden.

So erreicht man, dass sowohl Änderungen an den Kompetenzen der einzelnen Mitarbeiter als auch Veränderungen der Geschäftsprozesse jeweils nur an einer Stelle im Berechtigungskonzept aktualisiert werden müssen und dieses dadurch konsistent und übersichtlich bleibt.

Rollen & Authorities implementieren

Das Rollenkonzept kann sehr komfortabel implementiert werden. Zunächst einmal kann sich die Applikation beim Deployment bei dem IAM-Modul registrieren und dabei die eigenen Rollen und Rechte mitbringen. Die Rollen und Authorities einer Applikation können aber auch durch Administration im IAM manuell editiert werden.



Bei einem erneutem Deployment der App lassen sich die Änderungen, die in der Applikation an den Rollen und Rechten vorgenommen wurden, einfach im IAM übernehmen. Um zu vermeiden, dass vorher erfolgte manuelle Änderungen überschrieben werden, können bei S1 IAM manuelle Änderungen der Rollen/Rechte erhalten werden, aber auch die seitens der Applikation gelöschten Rollen/Rechte automatisch im IAM entfernt werden. Vor der Ausführung aller Funktionen kann die Applikation über Roles/Authorities im Login-Token prüfen, ob die erforderliche Berechtigung für die jeweilige Funktion vorhanden ist. Außerdem kann sie die Benutzeroberfläche an die Benutzerrolle anpassen, z.B. durch Ausblenden von Schaltflächen, deren Funktionalität nicht “erlaubt” ist.

In vielen Fällen kann es sinnvoll sein, wenn ein User mehrere Rollen haben kann. In diesem Fall erhält der User beim Login seine Default-Rolle, die er dann später über die Applikation in eine andere Rolle tauschen kann. Mehrere Rollen sind zum Beispiel dann erforderlich, wenn man für einige Aufgaben Admin-Rechte braucht und bei der normalen Arbeit aber nur ein eingeschränktes oder auch unterschiedliches Rechteset benötigt. Der Rollenwechsel erfolgt dann so ähnlich wie beim initialen Login-Authentication-Flow: Der User wählt an der UI der Applikation die neue

Rolle aus, die Applikation fragt den Rollenwechsel am IAM an, falls der User die andere Rolle haben darf, dann wird die Rolle gewechselt, indem ein neues Access-Token mit dem Rechte-Set der anderen Rolle zurückgegeben wird.

Nutzung von Keycloak

Eine Open-Source-Software, die eine zertifizierte Implementierung des OpenID-Connect-Protokolls darstellt, ist Keycloak. Die Software ermöglicht es einfach und flexibel ein IAM auch für mehrere Applikationen bereitzustellen, so dass nur ein einziger Identity Provider benötigt wird. So kann nach einer einmaligen Authentifizierung mit Single-Sign-On (SSO) auf alle Applikationen zugegriffen werden.

Keycloak bietet darüber hinaus auch die Möglichkeit, auf User-Daten eines LDAP– oder AD-LDS-Servers zuzugreifen, indem es bei Anmeldeversuchen zunächst den oder die dahinterliegenden LDAP Server konsultiert. Zusätzlich können auch Identity Provider wie Facebook oder Google angebunden werden. Durch die Bereitstellung von passenden Adaptern wird die Anbindung von Applikationen als Keycloak-Client unterstützt. Unser auf Keycloak basierendes S1 IAM Modul bietet eine sichere und gut dokumentierte Alternative zu einer aufwendigen proprietären Eigenentwicklung. Beispielsweise als Docker-Container erlaubt es eine flexible Anpassung der Konfiguration im Rahmen eines automatischen Deployment-Prozesses in CI/CD Pipeline. Zusätzlich können dabei auch Spezialfunktionen wie Two-Factor Authorisation, Anpassung von UI und Arbeitsabläufen oder die Unterstützung verschiedener Zugangslevel ergänzt werden.

Zusätzliche Attribute ergänzen

Mit “Token-Mappern” kann man bei der Keycloak-Client-Konfiguration festlegen, welche Attribute im Token an den Client übermittelt werden. Das können beispielsweise Rollen, Zugriffsrechte und Berechtigungen sein. Gruppen und Nutzern können auch benutzerdefinierte Attribute zugewiesen werden. Das können z.B. persönliche Daten wie der Vorname des Nutzers sein, oder auch Use-Case spezifische Daten für Ihre Applikation. Über Scopes kann die Applikation dann genau die Daten anfragen, die sie benötigt. So können z.B. auch verschiedene Zugangslevel für verschiedene Applikationen konfiguriert werden.

Beim Einloggen in die Applikation kann optional auch ein Consent-Screen angezeigt werden, über den der Nutzer nachvollziehen kann, welche Daten von der Applikation angefragt werden.

Kundenspezifische Anpassungen

Jedes System zur digitalen Zugangs- und Zugriffskontrolle hat, neben den allgemeinen und etablierten Standardanforderungen, spezifische, branchentypische Bedürfnisse, die ein IAM-System abbilden (können) muss. Alle Projekte werden von uns mit einer sorgfältigen Anforderungsanalyse begleitet, um sowohl funktionale Anforderungen (Sprach-Stacks, Geräteabhängigkeiten, Prüfensembles etc.), als auch nichtfunktionale Anforderungen (Oberflächengestaltung, Reaktionszeiten der Applikation,…) kundenspezifisch abbilden zu können.

IAM kostengünstig schneller umsetzen

Durch die Nutzung der Open Source Software Keycloak kann StoneOne ihren Kunden eine kostengünstige Lösung anbieten, die auch schnell implementierbar ist. Was nutzen wir von Keycloak, was kommt von uns?

Da S1 IAM auf Keycloak basiert, fallen für den Kunden keine Kosten für Lizenzen oder Abonnements an. Es werden lediglich die Erweiterungen seitens StoneOne als Dienstleistung berechnet. Selbstverständlich übernimmt StoneOne auch die Wartung und Pflege sowie die kundenspezifische Weiterentwicklung. Unsere Kunden profitieren von dem Erfahrungsvorsprung, den wir in zahlreichen Projekten in komplexen IT-Umgebungen aufgebaut haben. Wir entwickeln sowohl im Kundenauftrag das gesamte IAM-System, aber auch im Joint Development gemeinsam mit der Entwicklungsabteilung des Kunden.

Gregor Hintz
Kommunikation | Verwaltung
GVL mbH

gvl Gesellschaft zur Verwertung von Leistungsschutzrechten

„Die Experten von StoneOne sind im Identity and Access Management geschätzte Sparringspartner unserer IT-Mannschaft.“

stoneone
The Web Service Factory

StoneOne AG
Keithstrasse 6
10787 Berlin, Deutschland
Tel: +49 (0)30 469 99 07 18
Fax: +49 (0)30 469 99 07 19
info@stoneone.de
www.stoneone.de

Ihr Weg zu uns:

Sie wollen mehr Infos? Dann besuchen Sie uns auf unserer Website.
Dort haben Sie auch die Möglichkeit mit uns einen Termin zu vereinbaren.

www.stoneone.de