EIN PROJEKT
DES IT-PLANUNGSRATS

DEUTSCHE VERWALTUNGSCLOUD

# Handreichung zum Anschluss des lokalen Identity-Providers (IdP) an das Identity and Access Management (IAM) der DVC

## Single-Sign-On bei Nutzung von Cloud-Services und Cloud-Service-Portal der DVC

Version 1.0

15.08.2024

# Inhaltsverzeichnis

# 1 Allgemeine Informationen zur Handreichung

Ziel ist es, den Benutzer:innen des Cloud-Service-Portals (CSP) und zukünftig auch der Cloud-Services selbst ein Single-Sign-On (SSO) zu ermöglichen. Das Management der Identitäten und der Rollen soll weiterhin durch die Administrator:innen auf Seiten der Cloud-Service-Kunden und -Anbieter in ihren bestehenden Systemen erfolgen.

Diese Handreichung gibt einen ersten Überblick wie der lokale Identity Provider (IdP) des Cloud-Service-Kunden oder Cloud-Service-Anbieters an das Identitäts- und Rollenmanagement (IAM-Broker und Datendrehscheibe) der Deutschen Verwaltungscloud (DVC) angebunden werden kann. Die im Detail auszuführenden Aktivitäten hängen von den konkret genutzten Systemen der Cloud-Service-Kunden resp. Cloud-Service-Anbieter ab.

Für ein Login am CSP ist ein Anschluss an das IAM erforderlich. Dies kann entweder durch Anbindung des lokalen IdP erfolgen oder durch Anlage und Pflege von Benutzern in einem von govdigital zentral bereitgestellten IdP. Die Pflege der Nutzerkonten im IdP verbleibt in beiden Fällen in der Verantwortung der jeweiligen lokalen Administrator:innen.

Für die Nutzung von Services, die vom Anbieter bereits an das IAM der DVC angeschlossen wurden, ist auf Kundenseite ebenfalls ein Anschluss an das IAM erforderlich. Ziel ist, dass sukzessive in den nächsten Jahren alle oder möglichst viele Services an das IAM angeschlossen werden.

Nähere Informationen zum Angebot des zentral bereitgestellten IdP sowie zum Anschluss Ihres lokalen IdP an das IAM erhalten Sie durch Ihren DVC-Lotsen.

## 1.1 Hinweis

Die Handreichung richtet sich hauptsächlich an Interessierte, die für den Betrieb, die Pflege und Wartung der IdP- und IAM-Systeme beim Cloud-Service-Kunden (ggf. vertreten durch einen IT-Dienstleister) zuständig sind. Sie gibt einen ersten Überblick

über die notwendigen Schritte und Abläufe. Für weiterführende Informationen stehen Ihnen die DVC-Lotsenden jederzeit zur Verfügung.

# 2 Gesamtübersicht

Das nachfolgende Schaubild zeigt die Verbindungen zwischen Cloud-Service-Kunde (CSK), Cloud-Service-Anbieter (CSA), IAM der DVC und der Cloud-Service-Instanz. Wie der Grafik zu entnehmen ist, besteht das IAM der DVC aus einem IAM-Broker, der zur Übertragung der Identitätsinformationen dient, sowie der IAM-Datendrehscheibe, die zur Übermittlung der Berechtigungsinformationen dient.

Beim Cloud-Service-Kunden wird zur Anbindung des IdP eine zusätzliche Softwarekomponente, der IdP-Connechtor (IdPC) benötigt, der Informationen zu den Attributen der Cloud-Service-Nutzenden überträgt. Der IdP bestätigt also Identitäten und der IdP-Connector liefert die Attribute, mit denen die Gruppen und Rollen im Service zugeordnet werden. Der IAM-Broker stellt einen zentralen Zugriff auf alle IdPs der Cloud-Service-Kunden zur Verfügung und in der IAM-Datendrehscheibe werden die Attribute der Identitäten konfiguriert und übertragen.

Die vorliegende Handreichung fokussiert sich hauptsächlich auf die Verbindung des IdP des Cloud-Service-Kunden und dem IAM-Broker sowie der IAM-Datendrehscheibe über den IdP-Connector (farblich umrandete Bereiche). Die Anbindung des Cloud-Services an das IAM der DVC erfolgt in einer separaten Anleitung.

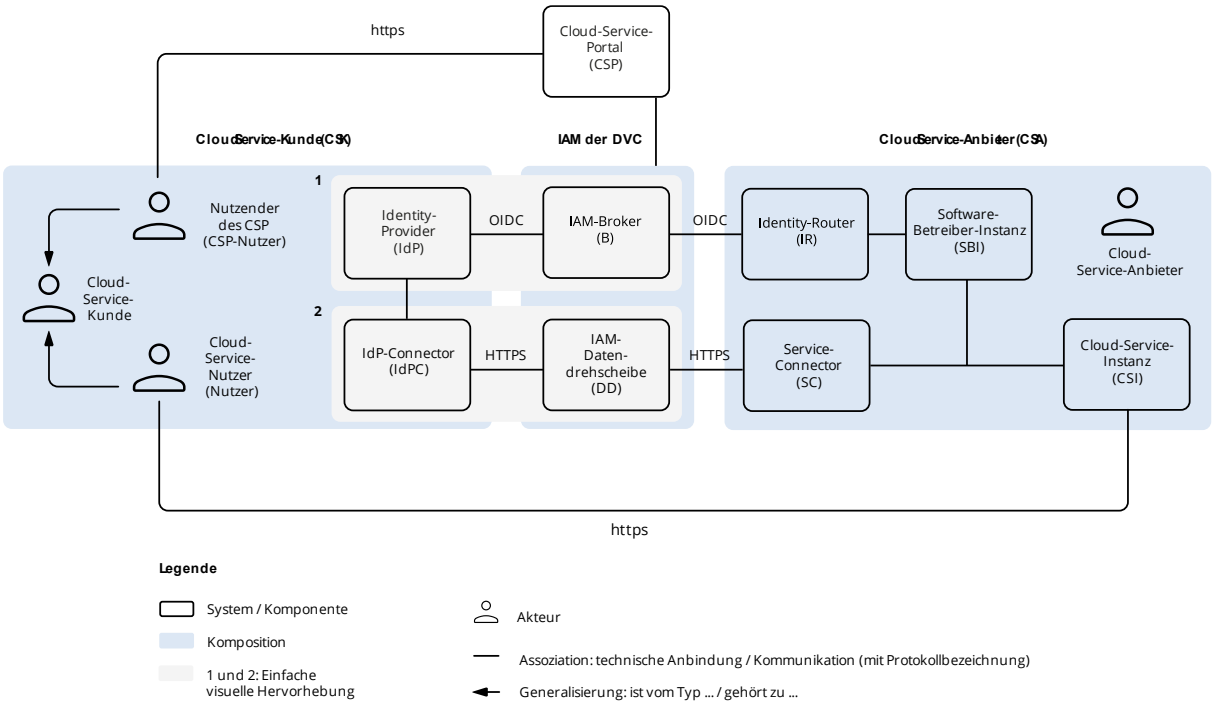
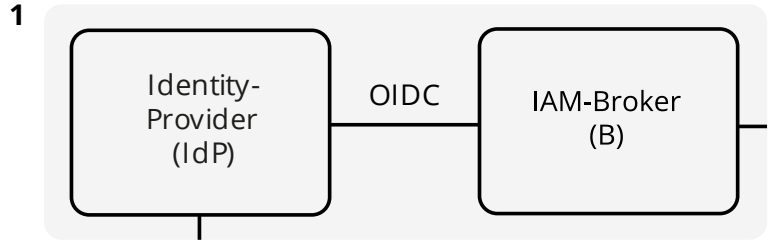



Abbildung 1: Begriffsdefinition, Abkürzungen und strategische Architektur der Anbindungen an das IAM der DVC

# 3 Prozess zur Anbindung

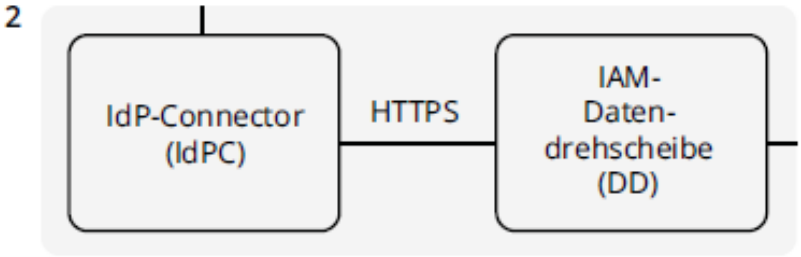
## 3.1 Verbindung des IdPs des Cloud-Service-Kunden mit dem IAM-Broker




- Im IdP des Cloud-Service-Kunden wird eine OIDC-Verbindung (OpenID Connect mit Direct Flow) zum IAM-Broker eingerichtet.
- Damit die OIDC Direct Flow Verbindung funktioniert, werden das IdP und der IAM-Broker untereinander bekannt gemacht.

- Hierfür werden im Rahmen des Registrierungsprozesses die notwendigen Informationen bereitgestellt, hierzu zählt der gegenseitige Austausch der Zertifikate und der Secrets für OpenID Connect.
- Zur Authentifizierung des Cloud-Service-Nutzenden wird im Rahmen der DVC ein OIDC-Token aufgebaut.
- Das Token enthält neben der ID ein Authentifizierungslevel als inhaltliches Attribut. Hierfür wird in der Regel eine „Konstante“ festgelegt.
- Eine direkte Netzwerkverbindung zwischen IdP und IAM-Broker muss nicht bestehen. Der Datentransport findet über den Browser auf dem Endgerät des Cloud-Service-Nutzenden statt.

## 3.2 Verbindung IdP-Connector des Cloud-Service-Kunden mit IAM-Datendrehscheibe




- Beim IdP des Cloud-Service-Kunden wird der sogenannte IdP-Connector eingerichtet. Idealerweise sollte dieser gemäß den DVC-Grundsätzen in Kubernetes betrieben werden.
- Falls keine geeignete Kubernetes-Umgebung zur Verfügung steht, kann der IdP-Connector auch serverbasiert betrieben werden.
- Die speziellen Parameter (z.B. für die Verschlüsselung), die der IdP-Connector für die Kommunikation mit der IAM-Datendrehscheibe benötigt, werden im Rahmen des Registrierungsprozesses bereitgestellt.

- Für die Anbindung des IdP-Connectors an den IdP des Cloud-Service-Nutzenden werden Referenzimplementierungen für Keycloak und Active Directory angeboten. Für die Anbindung anderer Quellen sind Schnittstellen vorgesehen, die vom Cloud-Service- Kunden (oder seinem IT-Dienstleister) zu realisieren sind.
- Der IdP-Connector benötigt eine ausgehende Verbindung ins Internet zur Kommunikation mit der IAM-Datendrehscheibe. Die Kommunikation basiert ausschließlich auf HTTPS (Port 443).

# 4 Abschließende Bemerkungen

Die vorangehende Beschreibung skizziert die erforderlichen Schritte zur Anbindung der Cloud-Service-Kunden an den IAM-Broker und die IAM-Datendrehscheibe. Im Rahmen des Registrierungsprozesses werden die individuellen und vertraulichen Informationen den handelnden Personen zur Verfügung gestellt. Artefakte und Dokumentationen werden schrittweise auf Open CoDE (https://opencode.de) veröffentlicht.

Für eine persönliche Beratung und weiterführende technische Informationen wenden Sie sich gerne an Ihre DVC-Lotsenden.