

Version 1.0

12.08.2024

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

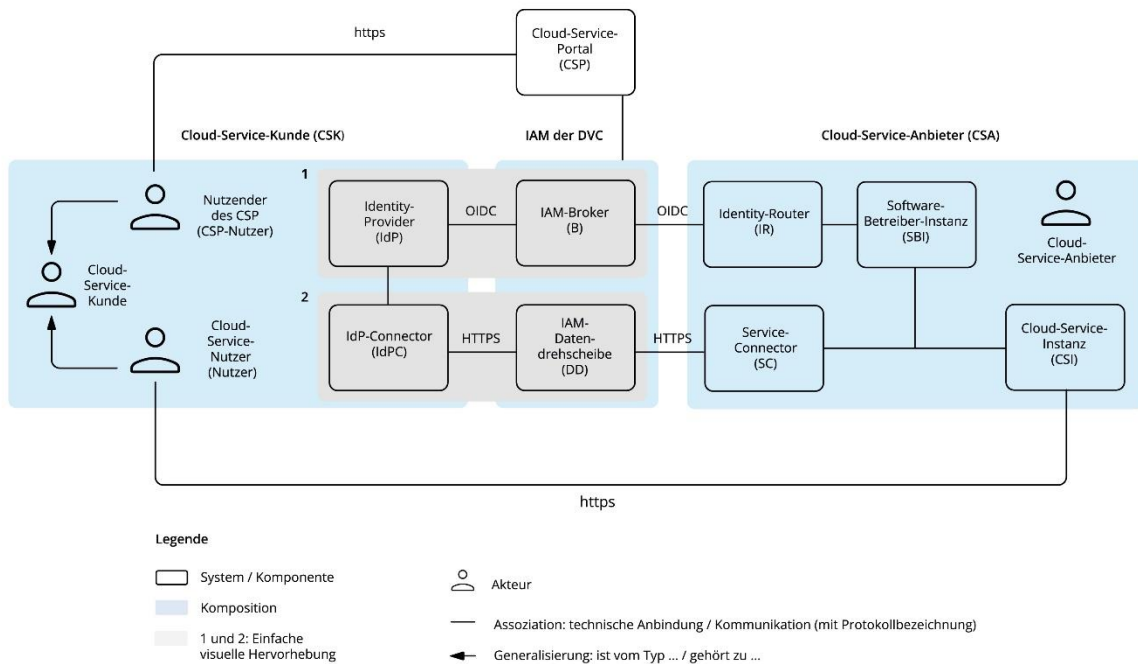
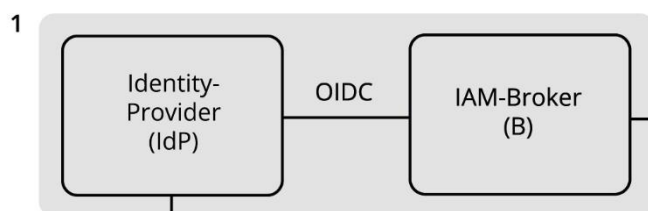


Abbildung 1: Begriffsdefinition, Abkürzungen und strategische Architektur der Anbindungen an das IAM der DVC

3 Prozess zur Anbindung

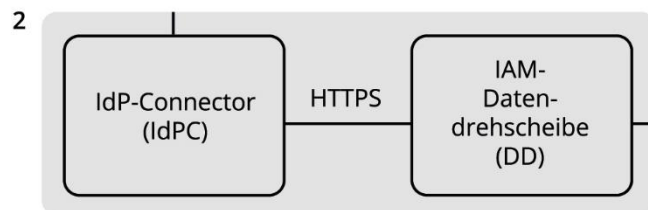
3.1 Verbindung des IdPs des Cloud-Service-Kunden mit dem IAM-Broker



- 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).

