ANWENDERBERICHT: DZ BANK

Intelligentes und regelkonformes Identity & Access Management im Bankwesen

Die DZ BANK duldet in puncto Identity & Access Management (IAM) keine Kompromisse. Ein bereichsübergreifendes Fachkonzept richtet das Berechtigungswesen der DZ BANK konsequent nach Business-Rollen aus. Ab jetzt gibt es nur noch eine einheitliche, auf SailPoint IdentityIQ basierende Software-Lösung, an welche alle Anwendungen der Zentralbank angeschlossen sind.

Steigende Ansprüche an IAM

Im Spannungsfeld zwischen der Europäischen Zentralbank (EZB) und der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) musste sich die DZ BANK im IAM-Bereich komplexen, compliance-getriebenen Anforderungen stellen. Mit dem aus der Wartung laufenden IAM-Altsystem auf Basis von Oracle Waveset ließen sich die gestellten Anforderungen nicht effizient bewältigen. Folglich war die Konsolidierung des IAM auf einer modernen, einheitlichen technischen Plattform geboten. Zudem war geplant, den Fachanwendern Dialoge und Prozesse nach Maß bereitzustellen.

Neues Fachkonzept für das Baselining

Als Rahmen für die Weiterentwicklung und Umstellung des Berechtigungsmanagements wurde in der DZ BANK ein übergreifendes Fachkonzept erarbeitet. „Das Fachkonzept spielt bei der Weiterentwicklung und im Betrieb eine essenzielle Rolle als Baseline zur Orientierung und Beschreibung des Soll-Zustandes“, so Lothar Wirkner, Gruppenleiter und Projektverantwortlicher bei der DZ BANK.

„Wir haben auf Basis des neu erstellten Fachkonzepts und einer Use-Case-Landkarte, welche die fachlichen Domänen von Anwendungsfällen und deren Input-Output-Beziehungen grafisch darstellt, über 90 Anwendungsfälle im Detail konzipiert,“ schildert Andreas Michel, Spezialist Identity & Access Management bei der DZ BANK.

Die Konzeption der Anwendungsfälle wurde durch KOGIT IAM-Consultants durchgängig begleitet. Als Prämissen galten dabei die technische und fachliche Umsetzbarkeit, die Umsetzung der Compliance-Vorgaben, die Machbarkeit und Release-Festigkeit sowie der Implementierungsaufwand.

DZ BANK – DEUTSCHE ZENTRAL- UND GENOSSENSCHAFTSBANK AG

Die DZ BANK ist die zweitgrößte Geschäftsbank in Deutschland und das Spitzeninstitut der Genossenschaftlichen FinanzGruppe Volksbanken Raiffeisenbanken. Sie ist die Zentralbank für alle rund 800 Genossenschaftsbanken in Deutschland, denen sie mehrheitlich gehört. Als „DZ BANK. Die Initiativbank“ unterstützt sie die Geschäfte der eigenständigen Genossenschaftsbanken vor Ort, um deren Position im Wettbewerb zu stärken. Dabei hat sich das Zusammenspiel aus dezentraler Kunden- und zentraler Produktkompetenz bestens bewährt.

Das Leistungsspektrum der DZ BANK reicht von klassischen und innovativen Produkten über Strukturierung und Emissionen bis hin zu Handel und Vertrieb im Aktien- und Rentenmarkt. Zusätzlich betreut die DZ BANK als Geschäftsbank Unternehmen und Institutionen. Mit ihren Niederlassungen und Repräsentanzen in den wichtigen Wirtschaftsregionen der Welt unterstützt sie Unternehmen bei Ihren internationalen Geschäften.

Daneben hat die DZ BANK die Holdingfunktion für die Unternehmen der DZ BANK Gruppe mit deren starken Marken. Sie gehören zu den Eckpfeilern des Allfinanzangebots der Genossenschaftlichen FinanzGruppe Volksbanken Raiffeisenbanken, die – gemessen an der Bilanzsumme – eine der größten privaten ▶

Wechsel zu moderner Software-Plattform

Als Ersatz für die aus der Wartung gelaufene IdM-Bestandslösung von Oracle setzte sich SailPoint IdentityIQ unter allen potenziellen Software-Kandidaten durch. Ausschlaggebend war dabei, dass KOGIT den geforderten Proof-of-Concept mit einer Referenzinstallation in sehr kurzer Zeit bereitstellen konnte und die Out-of-the-box-Fähigkeiten der SailPoint-Software hervorstachen. Das von KOGIT vorgestellte Adapter-Framework überzeugte als „außer Konkurrenz". Zudem legte KOGIT ein attraktives kaufmännisches Angebot vor.

„Die Einbindung des Implementierungspartners KOGIT war bei diesem Projekt wesentlich, da im Gegensatz zu einer Eigenentwicklung der DZ BANK die Möglichkeiten und Restriktionen von SailPoint IdentityIQ in das Fachkonzept einfließen mussten", sagt Lothar Wirkner.

Rollout als „Big Bang"

Die technologische Nähe zur Vorgängerversion von SailPoint IdentityIQ 6.4 erwies sich bei der Migration der vorhandenen Identitäts- und Zugriffsdaten nach SailPoint IdentityIQ 7.2 als vorteilhaft. Die flächendeckende Fusion der IAM-Prozesse auf der neuen Software-Plattform verlief planmäßig. Der Rollout der neuen IAM-Lösung erfolgte im März 2020.

„Wir sind auf die gelungene Migration als „Big Bang" besonders stolz. Die Migrationsarbeiten fanden an einem Wochenende statt – und nach einem Tag Downtime konnten alle Anwender mit dem neuen Tool arbeiten."

LOTHAR WIRKNER
Gruppenleiter und Projektverantwortlicher, DZ BANK

DZ BANK
Die Initiativbank

- Finanzdienstleistungsorganisationen Deutschlands ist. Zur DZ BANK Gruppe zählen die Bausparkasse Schwäbisch Hall, DZ HYP, DZ PRIVATBANK, R+V Versicherung, TeamBank, Union Investment Gruppe, VR Smart Finanz und verschiedene andere Spezialinstitute.
  Gemeinsam unterstützt die DZ BANK Gruppe mit ihrem umfangreichen Allfinanzangebot die Genossenschaftsbanken im Privatkundengeschäft, Firmenkundengeschäft, Kapitalmarktgeschäft und Transaction Banking. Damit sind diese in der Lage, ihren Kunden ein komplettes Spektrum an herausragenden Finanzdienstleistungen anzubieten.

  www.dzbank.de

„Wir sind auf die gelungene Migration als „Big Bang" besonders stolz. Die Migrationsarbeiten fanden an einem Wochenende statt – und nach einem Tag Downtime konnten alle Anwender mit dem neuen Tool arbeiten," so Wirkner. „Sicher gab es Bugs und auch einige spannende Situationen, aber insgesamt ist die Migration vor dem Hintergrund der Komplexität sehr gut gelaufen."

Als weiteres Highlight erleben die Experten der DZ BANK den von SailPoint stammenden JDBC-Connector zur Enterprise Applikation Integration Plattform (EAI). Dazu Jochen Gärtner: „Der JDBC-Connector ermöglicht uns das fließbandartige Anbinden von Anwendungen und ist bezüglich der Nachvollziehbarkeit von Provisionierungen unschlagbar. In Gesprächen mit anderen Branchenexperten weckt das Thema immer sehr großes Interesse."

Automatismen und verbindliche Regelungen

Zunächst werden die Anwendungen und deren Verantwortlichkeiten in ServiceNow als führendes Service- und Configuration-Management-System angelegt. Die für das Access Management benötigten Objekte werden daraufhin über den definierten Onboarding-Prozess per selbstentwickelter REST-Schnittstelle in SailPoint IdentityIQ automatisiert erzeugt. Werden Anwendungen im führenden System hingegen auf den Status „retired" gesetzt, wird automatisiert der Offboarding-Prozess gestartet und der Rückbau der gesamten Objekthierarchie in SailPoint IdentityIQ initiiert.

Die Fachbereiche müssen alle genutzten Applikationen, einschließlich Web-Applikationen, im Asset-Bestand registrieren sowie deren Schutzbedarf festlegen und dabei die Berechtigungsrelevanz bestimmen. Sofern eine Berechtigungsrelevanz vorliegt, ist zwingend ein Onboarding an das zentrale Identity- und Access-Management-System durchzuführen.

Fürs Tagesgeschäft gut aufgestellt

Aktuell werden bei der DZ BANK ca. 10.000 Identitäten und über 35.000 Rollen mit über 350.000 Zuweisungen von rund 100.000 Entitlements für über 500 technisch oder manuell angebundene Zielsysteme verwaltet. Fast der gleiche Datenbestand wurde aus der früheren SailPoint IdentityIQ-Implementierung im ersten Quartal 2020 migriert.

Pro Monat verzeichnet die Bank im Schnitt 6 Onboardings mit ca. 6.000 Rollenveränderungen. Die Gesamtanzahl der Identitäten bleibt mit monatlich rund 500 Zu- und Abgängen relativ konstant.

Alle Ein- und Austritte (Joiner bzw. Leaver) werden vollautomatisiert zum Zeitpunkt der Aktivierung/Deaktivierung verarbeitet. Dabei finden diverse Schwellwertprüfungen statt um ungewollte Massenänderungen zu verhindern. Bei Eintritten werden regelbasierte Berechtigungen, z.B. Basisberechtigungen, automatisiert zugewiesen; bei Austritten werden die im Soll zugeordneten Business-Rollen automatisiert abgebaut.

„Der JDBC-Connector ermöglicht uns das fließbandartige Anbinden von Anwendungen und ist bezüglich der Nachvollziehbarkeit von Provisionierungen unschlagbar.“

JOCHEN GÄRTNER
Spezialist Identity & Access Management, DZ BANK

Zur Sicherstellung der Einhaltung von Funktionstrennungen wurde eine einheitliche Segregation-of-Duties-Matrix eingeführt. Mit dieser lassen sich regulatorische Vorgaben abbilden.

Langjährige, konstruktive Zusammenarbeit

KOGIT begleitet das IAM-Programm der DZ BANK seit dem Projekt zur Optimierung der IT-Sicherheit der Bank (ab 2012) über die Stabilisierungsphase bis hin zur Umsetzung des neuen Fachkonzepts.

„Insgesamt verfügen die KOGIT-Spezialisten über einen ausgezeichneten Architektur-Skill und die Kenntnis von Best Practices, die sehr wertvoll für unsere Projektarbeit ist“, so Lothar Wirkner. „Das KOGIT- Entwicklungsteam ist kompetent, engagiert und zuverlässig. Insbesondere haben wir durch die Corona-bedingte nahezu 100%-Remote-Arbeit keine nennenswerten Einschränkungen festgestellt.“

Das Projekt im Überblick

Zielsetzung

- Zuverlässige Erfüllung Compliance-getriebener Anforderungen
- Ablösung der Altsysteme im Bereich IDM
- Konsolidierung auf eine moderne technische Plattform
- Bereitstellung von Dialogen und Prozessen für Fachanwender

Lösung

- Konnektor-Architektur für automatisierte und manuelle Verfahren
- Einführung von Rückmeldeverfahren aus den Applikationen
- Einführung präventiver und aufdeckender Compliance-Kontrollen
- Integration mit HR-, OM- und ITSM-Prozessen
- Einführung von Business-Rollen

KOGIT-Lösungsbeiträge

- Beratung und Überprüfung der technischen Realisierbarkeit des neuen Fachkonzepts
- Erstellung des Release-Plans zur Umsetzung
- Design und Implementierung der Konnektor-Architektur
- Implementierung der Prozesse und Kontrollen
- Unterstützung der Fusion bezüglich der IAM-Prozesse
- Technisches Onboarding von über 500 Applikationen

Ergebnisse

- Höhere Transparenz durch einheitliche Plattform
- Stärkere Integration der Fachbereiche in den IAM-Prozessen
- Durchgehend risikobasierender Ansatz der IAM-Prozesse
- Reaktionsfähigkeit auf neue regulatorische Anforderungen

PARTNERSCHAFT KOGIT & SAILPOINT

KOGIT wurde 2007 der erste europäische SailPoint-Partner. Als einziger deutscher Partner gehört KOGIT dem SailPoint Partner Advisory Board an und ist Mitglied der Identity+ Alliance. Mit über 50 Mitarbeitern – davon mehr als 40 SailPoint Beratern – ist KOGIT der Partner mit dem größten SailPoint-Kompetenzteam in Europa. KOGIT kann mehr als 10.000 Personentage an Erfahrung in SailPoint-Projekten vorweisen.
Nach der Auszeichnung als „Partner of the Year Europe 2015“ wurde KOGIT in den Jahren 2018, 2019 2020 und 2021 als einziger deutscher Partner von SailPoint zum Top Delivery Admiral ernannt.

KONTAKT

KOGIT GmbH
Rheinstr. 40-42
64283 Darmstadt

Telefon: +49 6151 7869-0
info@kogit.de · www.kogit.de