trustkey AccessControl

Sicherstellung der Integrität und Vertraulichkeit von Informationen

1

Zugriffskontrollen für Process Experiences und Arbeitsbereiche

2

Zugriffskontrollen für Data Intelligence und Synchronisierung

3

Erweiterte Zugriffskontrolle mit SensitiveDataControl

Zugriffskontrollen für Process Experiences und Arbeitsbereiche

Aktionspakete-Bereich, Ressourcen-Bereich und Wissens-Bereich

Überblick über Process Experiences und Konzepte für Mitgliederrollen und Berechtigungen

	Aktionspakete-Bereich		Ressourcen-Bereich		Wissens-Bereich	
Prozess-struktur	**Template**	**Besitzer Bearbeiter Launcher**	**Template**	**Besitzer Bearbeiter Launcher**	**Template**	**Besitzer Bearbeiter Launcher**
	Shortcut	**Manager Empfänger Mitwirkender Leser** • ***Launcher Mitgliedschafts-kontrolle*** • ***Detaillierte Berechtigungen***	**Shortcut**	***Keine Mitgliedschafts-konfiguration***		
Process Execution	**Board**	**Manager Empfänger Mitwirkender Leser**	**Ressourcen-gruppe**	**Manager Mitwirkender Leser** • ***Privat-Kennzeichen*** • ***Berechtigungsstufen*** • ***Detaillierte Berechtigungen***	**Notizbuch**	**Manager Mitwirkender Leser**
	Aktions-paket	**Manager Empfänger Mitwirkender Leser** ***Detaillierte Berechtigungen***	**Ressource**	**Manager Mitwirkender Leser** ***Berechtigungsstufen: Blockiert/Gewährt***	**Wissens-seite**	**Manager Mitwirkender Leser** ***Detaillierte Berechtigungen***

Eine detaillierte Beschreibung der Mitgliedschaftsrechte finden Sie im Playbook auf trustkey.eu.

Mitglieder und Zugriffskonfigurationen

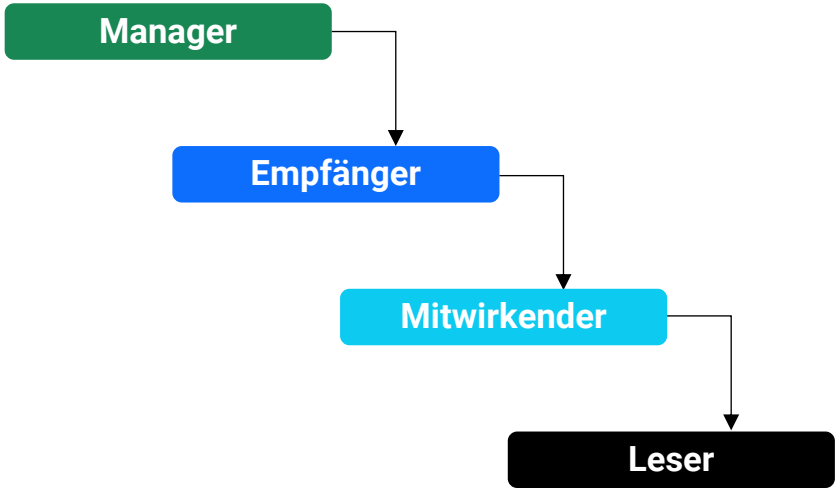
Mitglied	Zusammenfassung
Besitzer	… hat volle Berechtigungen für das Template und kann Templates veröffentlichen und launchen.
Bearbeiter	… hat die Berechtigung, Templates im Entwurfsmodus zu bearbeiten und kann veröffentlichte Templates launchen.
Launcher	… können Templates nicht ändern. Sie können nur veröffentlichte Aktionspaket-Templates starten oder die Ressourcen- und Wissens-Templates für Ressourcengruppen oder Notizbücher auswählen.
Manager	… hat volle Berechtigungen und kann Mitglieder und Berechtigungen verwalten.
Empfänger (Aktionspaket)	… hat die Erlaubnis, die Aktionspakete auszufüllen, und seine Zuständigkeit wird angegeben.
Mitwirkender	… hat die Berechtigung zum Bearbeiten.
Leser	… kann nur den geteilten Inhalt lesen.

Konfiguration	Zusammenfassung
Launcher Mitgliedsschafts-kontrolle (Aktionspaket)	Ermöglicht die Definition der Rolle für Mitglieder, wenn diese einen Shortcut launchen. Insbesondere wertvoll für “Automatisierte Verlinkungen“.
Detaillierte Berechtigungen	Legen Sie für jeden Abschnitt und jede Komponente fest, was jedes Mitglied bearbeiten und lesen darf.
Privat (Ressourcengruppe)	Bestimmen Sie eine Ressourcengruppe als privat: nur Mitglieder der Ressourcengruppe können sie auf der Übersichtsseite sehen und Ressourcen im Dropdown-Menü der Lookup-Komponente anzeigen.
Berechtigungsstufen (Ressourcengruppe)	Für Mitwirkende und Leser können zusätzliche Berechtigungsstufen (Alle, Alle/Eingeschränkt, Eingeschränkt) festgelegt werden. Diese Berechtigungsstufen steuern den Zugriff auf Ressourcen innerhalb einer Ressourcengruppe.
Blockiert/Gewährt (Ressource)	Sperren oder Gewähren des Zugriffs auf bestimmte Ressourcen innerhalb einer Ressourcengruppe.

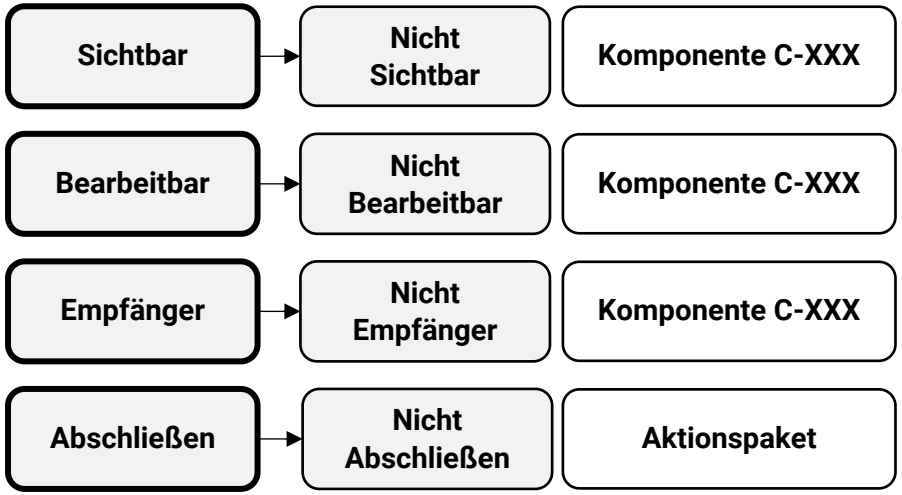
Please check playbook on trustkey.eu for detailed description of membership rights.

Vererbung von Gruppen- und Benutzerberechtigungen

Rolle des Mitglieds

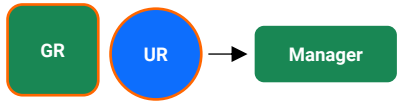


Detaillierte Berechtigungen



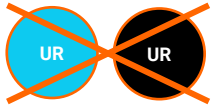
Beispiele für die Konfiguration von trustkey-Berechtigungen

Benutzer ist Mitglied einer Gruppe und verfügt über individuelle Rechte, die jeweils unterschiedliche Zugriffs-ebenen gewähren.



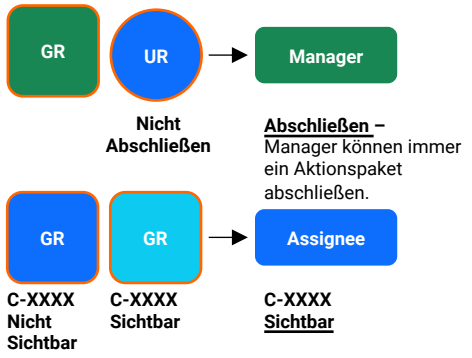
Benutzer ist Mitglied in zwei Gruppen. Beide Gruppen haben unterschiedliche Zugriffsebenen.

Benutzer können nicht gleichzeitig Mitglieder von trustkey-Elementen mit zwei verschiedenen individuellen Benutzerberechtigungen sein.



Beispiele für die Konfiguration von trustkey-Berechtigungen

Benutzer hat zwei Mitgliedschaften mit unterschiedlichen Detail-berechtigungen.



Gruppen- und Benutzer-Mitgliedschaften

GR — Gruppe

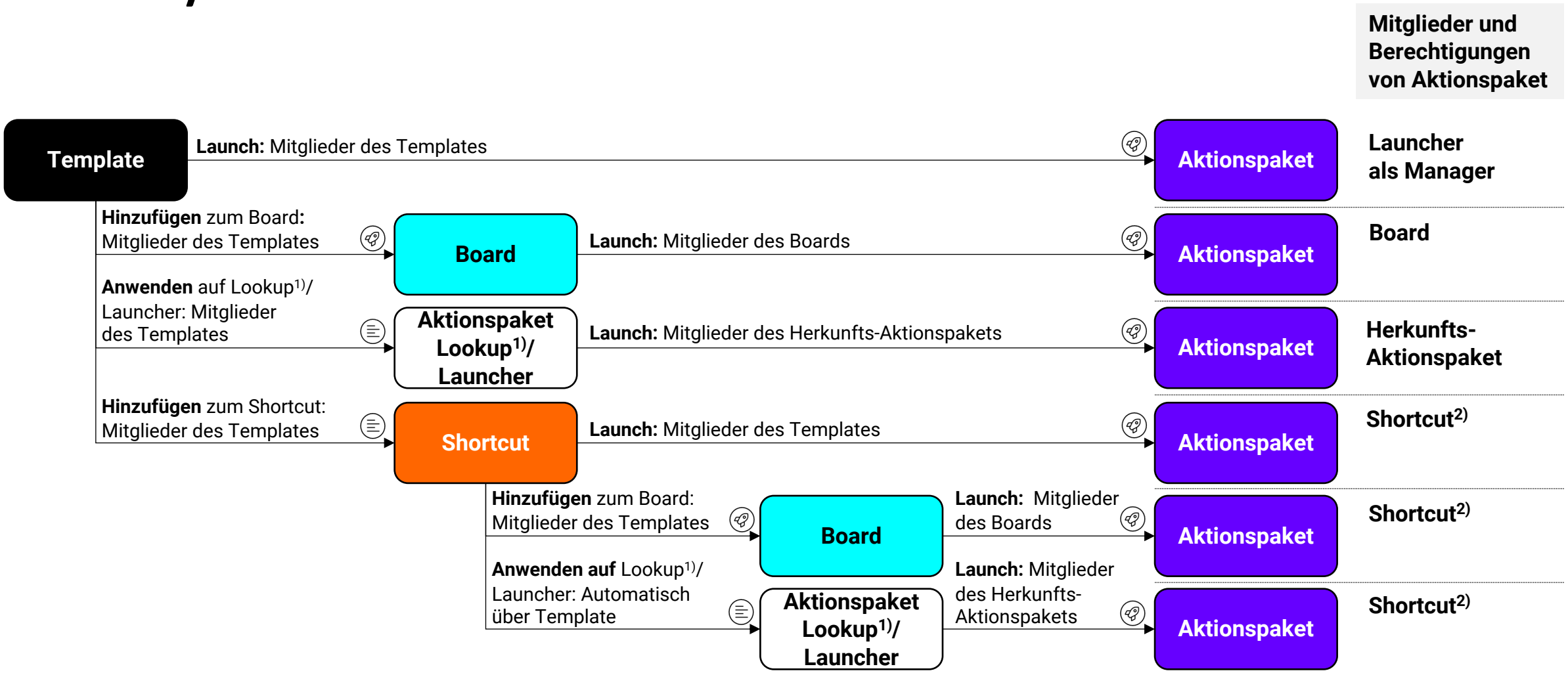
UR — Benutzer

Hinweis

Jedes Aktionspaket, jedes Board, jede Ressourcengruppe, jede Ressource, jedes Notizbuch und jede Wissensseite muss mindestens eine Managerrolle haben.

Wenn ein Benutzer eine Vorlage startet, eine Ressourcengruppe hinzufügt oder ein Notizbuch erstellt, wird ihm automatisch die Rolle „Manager“ zugewiesen.

Vererbung von Mitgliedern und Berechtigungen
Aktionspaket



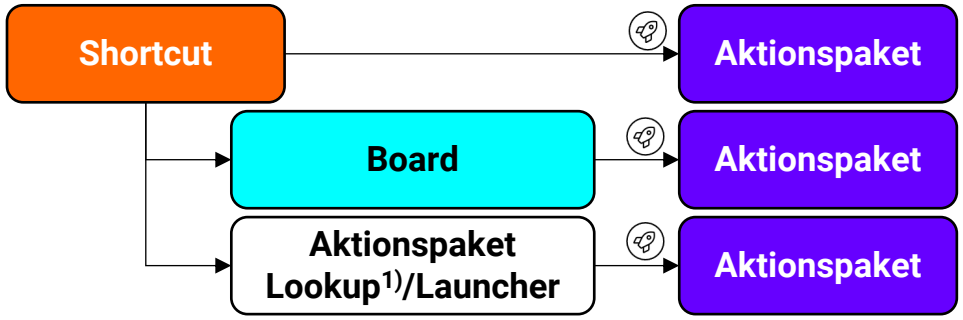
1) Funktion: „Ermöglichen Sie das Launchen neuer Aktionspakete“ aktiviert; Mitglieder des Aktionspakets können nur die Aktionspakete in der Lookup-Komponente sehen, in denen sie auch Mitglied sind.
2 Wenn der Launcher nicht Mitglied des Shortcuts ist und die Launcher-Mitgliedschaftskontrolle deaktiviert ist, wird der Launcher Manager des Aktionspakets.

Vererbung von Mitgliedern und Berechtigungen
Aktionspaket – Launcher-Mitgliedschaftskontrolle

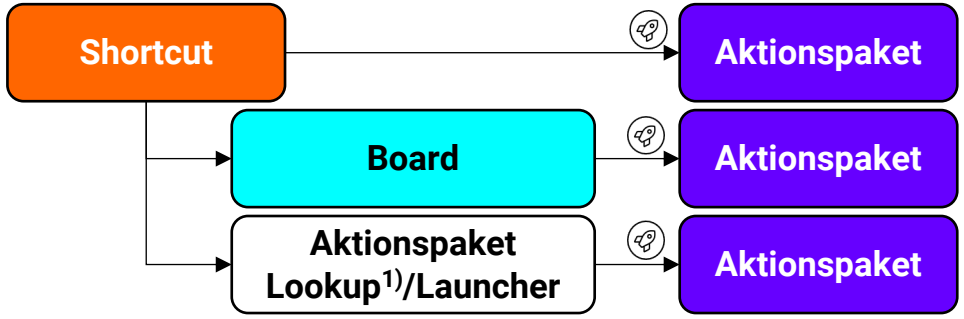
Launcher Mitgliedsschafts-kontrolle

Launching Prozess

Deaktiviert



Aktiviert



Shortcut Mitglieds-schafts	**Launcher Mitgliedsschafts-kontrolle**	**Launcher Mitgliedschaft im gelaunchten Aktionspaket**	
		Wenn Mitglied des Shortcuts	**Wenn NICHT Mitglied** des Shortcuts
Manager	-	Manager	Manager
Empfänger	-	Empfänger	Manager
Mitwirkender	-	Mitwirkender	Manager
Leser	-	Leser	Manager
Manager	Empfänger	Manager	Empfänger
Empfänger	Mitwirkender	Empfänger	Mitwirkender
Mitwirkender	Empfänger	Empfänger	Empfänger
Leser	Leser	Leser	Leser

„Höhere Rolle“ setzt sich durch

1) Function: “Ermöglichen Sie das Launchen neuer Aktionspakete” aktiviert.

Board oder Shortcut – Was ist der richtige Weg, um den Zugriff zu kontrollieren? *Aktionspakete*

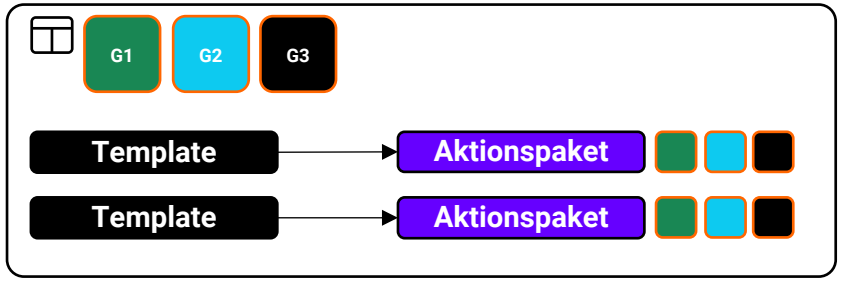
Board

Vorteile

- **Rollenbasierter Zugriff:** Weisen Sie Rollen zu, um zu steuern, wer das Board und seine Inhalte anzeigen, bearbeiten oder verwalten darf.
- **Sichtbarkeit und Organisation:** Boards bieten eine übersichtliche, organisierte Möglichkeit zur Präsentation von Informationen und Ressourcen und stellen sicher, dass Zugriffskontrollen konsistent auf zusammengehörige Elemente angewendet werden.

Anwendungsempfehlung

Projektbezogener Inhalt: Verwalten Sie teamübergreifende Aktionen, für die Mitglieder (unterschiedliche) Zugriffsrechte benötigen, und stellen Sie sicher, dass die Berechtigungen einheitlich auf alle Board-/Arbeitsbereichsinhalte angewendet werden.



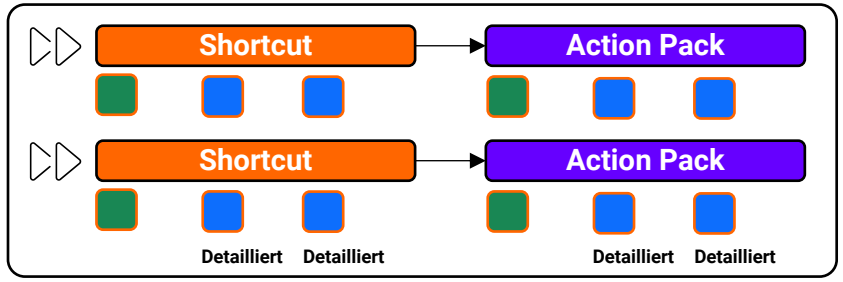
Shortcut

Vorteile

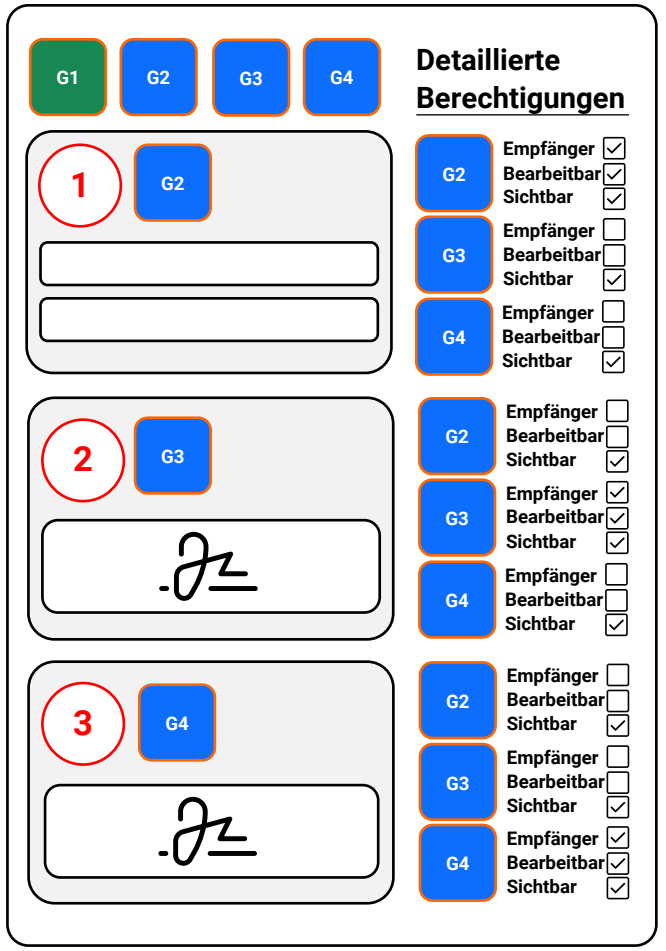
- **Umfassende Zugriffskontrolle:** Shortcuts bieten eine detaillierte und hierarchische Struktur für die Verwaltung von Berechtigungen, was die Kontrolle des Zugriffs auf verschiedenen Ebenen und Rollen erleichtert.
- **Robuste Standardisierung:** Stellen Sie sicher, dass Zugriffskontrolle und Berechtigungen im gesamten Unternehmen einheitlich und effektiv angewendet werden.

Anwendungsempfehlung

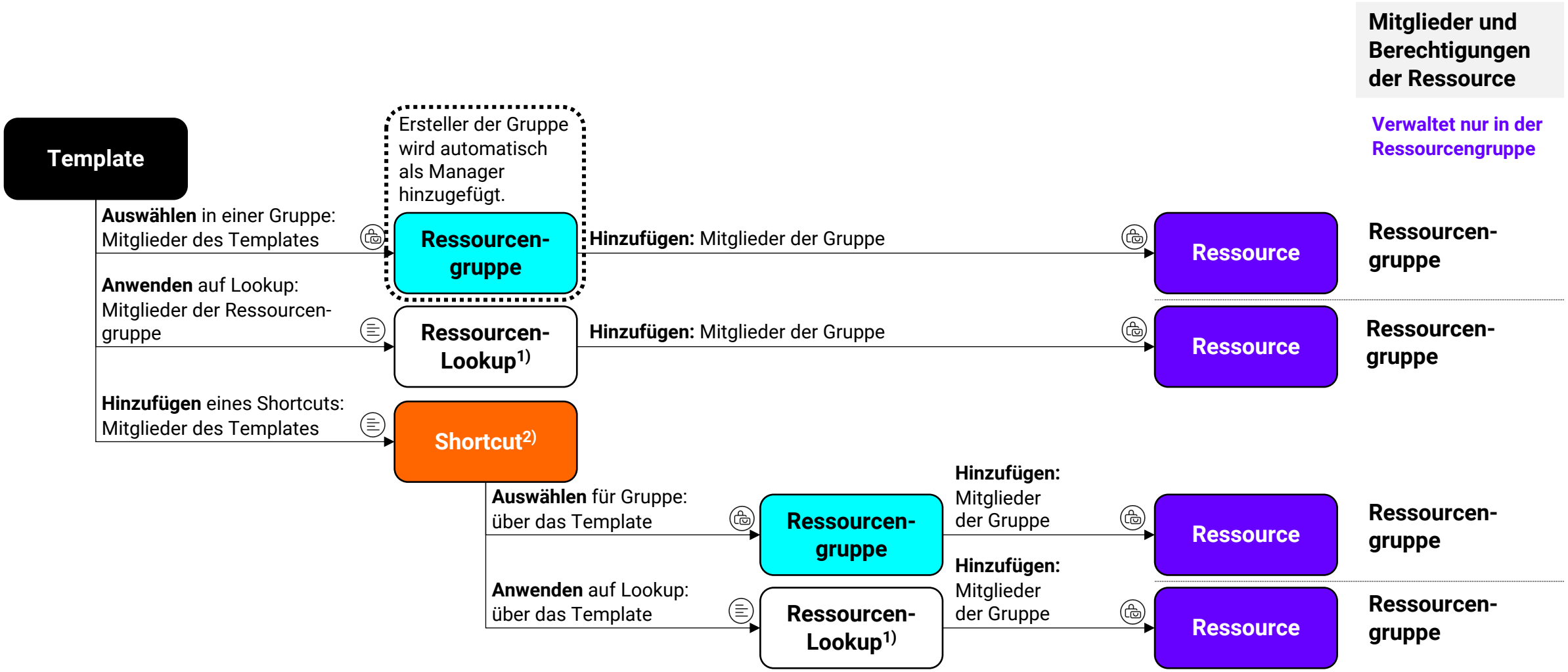
Compliance-bezogener Inhalt: Verwalten Sie teamübergreifende Aktionen, für die Mitglieder unterschiedlich detaillierte Zugriffsrechte benötigen, und stellen Sie sicher, dass die Berechtigungen einheitlich auf alle Prozessinstanzen angewendet werden.



Beispiel Shortcut Konfiguration



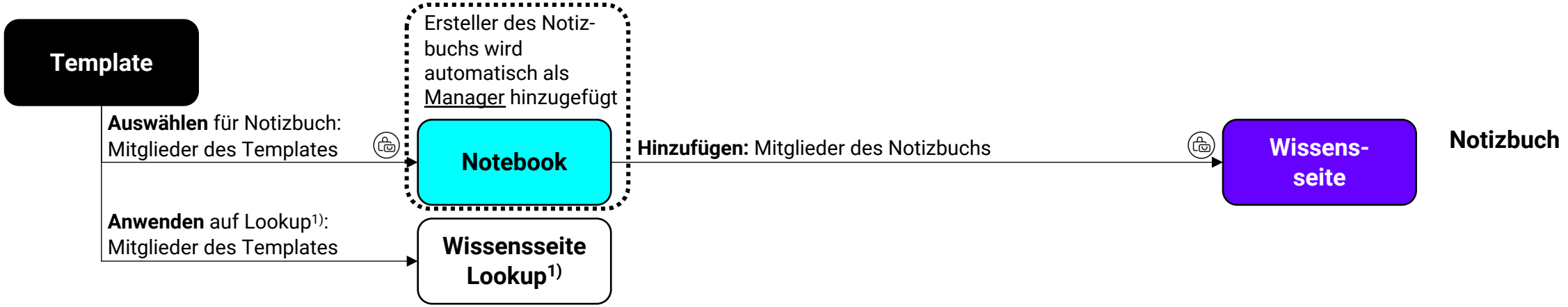
Vererbung von Mitgliedern und Berechtigungen
Ressourcen



1) Funktion „Ressource hinzufügen erlauben“ aktiviert; Alle Mitglieder des Aktionspakets können eine Ressource im Dropdown-Menü der Lookup-Komponente sehen, es sei denn, die Ressourcengruppe ist als privat markiert. Um eine ausgewählte Ressource zu öffnen, muss der Benutzer jedoch eine Mitgliedschaft für diese spezifische Ressource besitzen.
2) Für Ressourcen können keine Mitglieder und Berechtigungen im Shortcut definiert werden.

Vererbung von Mitgliedern und Berechtigungen
Wissen

Mitglieder und Berechtigungen der Wissensseite



1) Alle Mitglieder des Aktionspakets können eine Wissensseite in der Dropdown-List der Lookup-Komponente anzeigen. Um eine ausgewählte Wissensseite zu öffnen, muss der Benutzer jedoch eine Mitgliedschaft für diese Seite besitzen.

Empfohlene Schritte zum Festlegen von Berechtigungen

1

Definieren Sie ein Prozessstruktur-Team
Das Prozessstruktur-Team ist für die Bereitstellung und Pflege von Geschäftsprozessen innerhalb von trustkey verantwortlich.

2

Definieren Sie Gruppen für Ihre Organisation
- Der beste Weg, um zu beginnen, ist die Verwendung Ihres Organigramms, um diese Gruppen in trustkey darzustellen
- Anschließend können Sie die Gruppen basierend auf ihren spezifischen Rollen und Verantwortlichkeiten verfeinern.

3

Erstellen Sie Templates

Aktionspaket
- Eigentümer: Prozessstruktur-Team
- Bearbeiter/Launcher: Prozessausführungs-Team

Ressource
- Eigentümer: Prozessstruktur-Team
- Bearbeiter/Launcher: Prozessausführungs-Team

Wissen
- Eigentümer: Prozessstruktur-Team
- Bearbeiter/Launcher: Prozessausführungs-Team

4

Erstellen Sie Shortcuts für compliance-bezogene Tätigkeiten
- Manager: Prozessstruktur-Team
- Empfänger/Mitwirkender/Leser: Prozessausführungs-Team

Erstellen Sie Shortcuts für Standardisierungs- und Vereinfachungszwecke

5

Erstellen Sie Boards für projektbezogene Tätigkeiten
- Weisen Sie Manager zu: Projektmanager
- Laden Sie das Projekt-Team als Empfänger, Mitwirkende oder Leser ein

Erstellen Sie Ressourcengruppen
- Weisen Sie Manager zu: Prozessstruktur-Team
- Gewähren Sie dem Prozessausführungsteam Zugriff als Mitwirkende oder Leser
- Verfeinern Sie den Zugriff durch detaillierte Berechtigungen und Stufen

Erstellen Sie Notizbücher
- Weisen Sie Manager zu: Prozessstruktur-Team
- Gewähren Sie dem Prozessausführungsteam Zugriff als Mitwirkende oder Leser

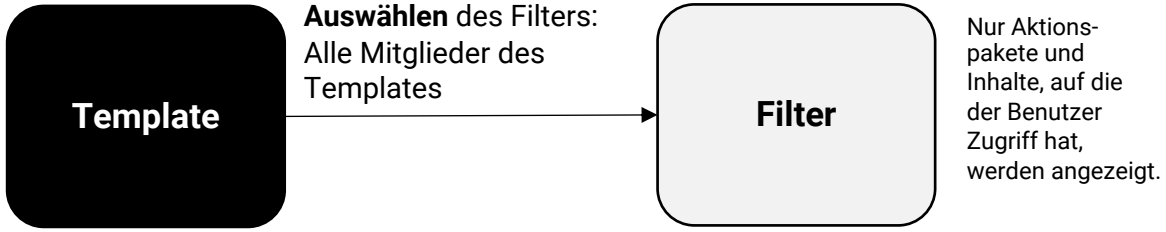
Zugriffskontrolle für Data Intelligence und Synchronisierung

Analytics, Integrationsportal, Designer

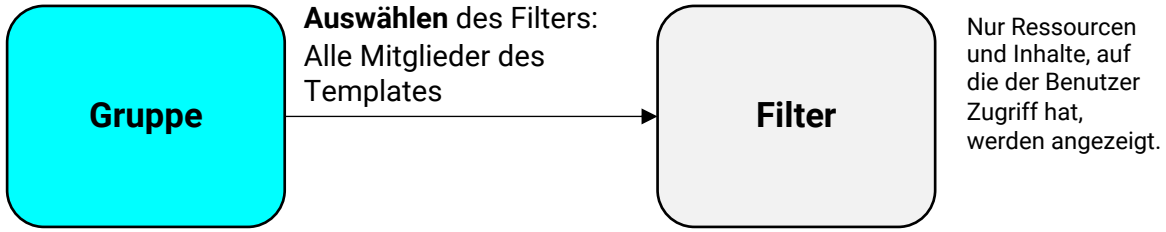
Analytics

Standardberichte

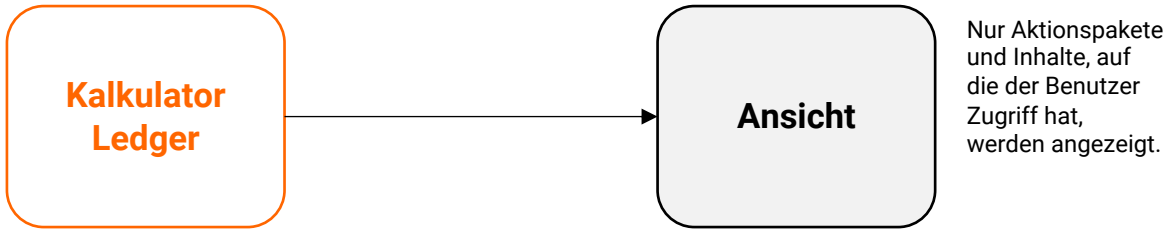
Aktionspakete



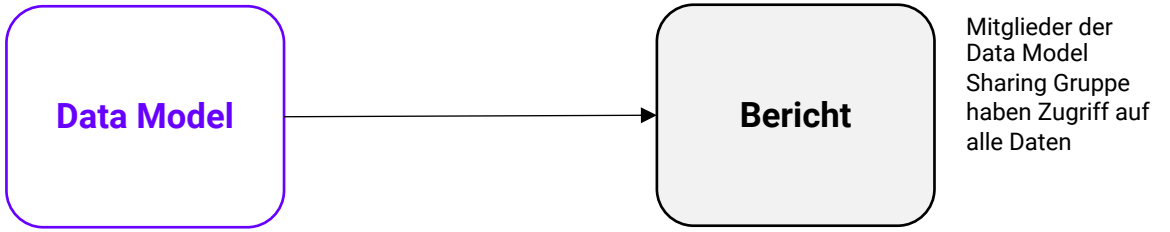
Ressourcen



Ledger

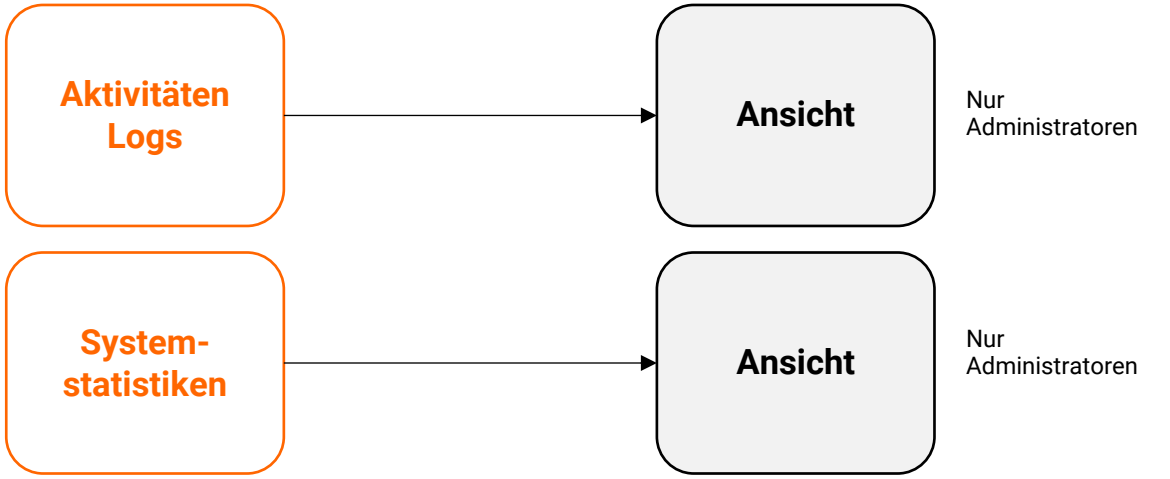


Designer Berichte



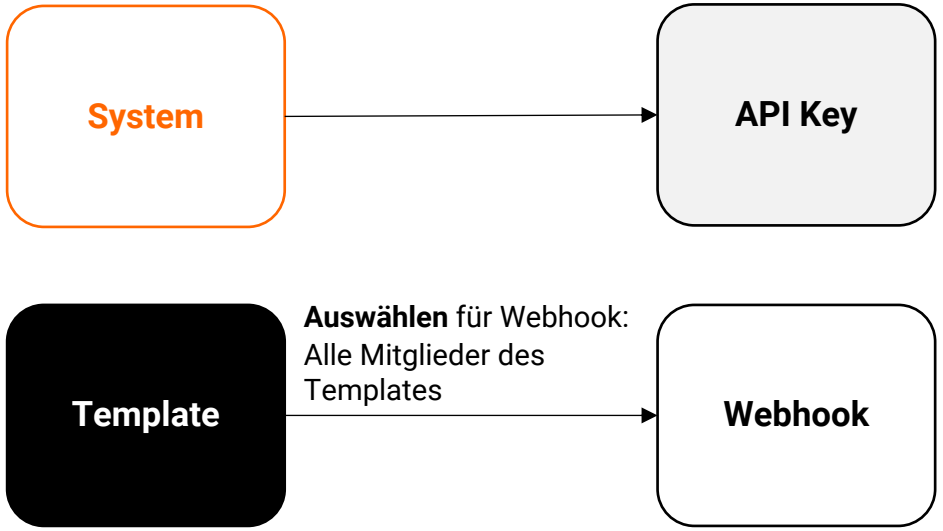
Erforderliches Add-On: Designer

Systemberichte

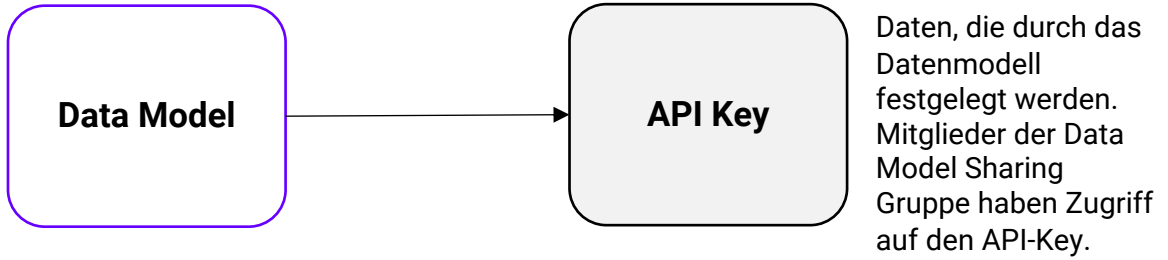


Integrationsportal

Generelle Konnektoren

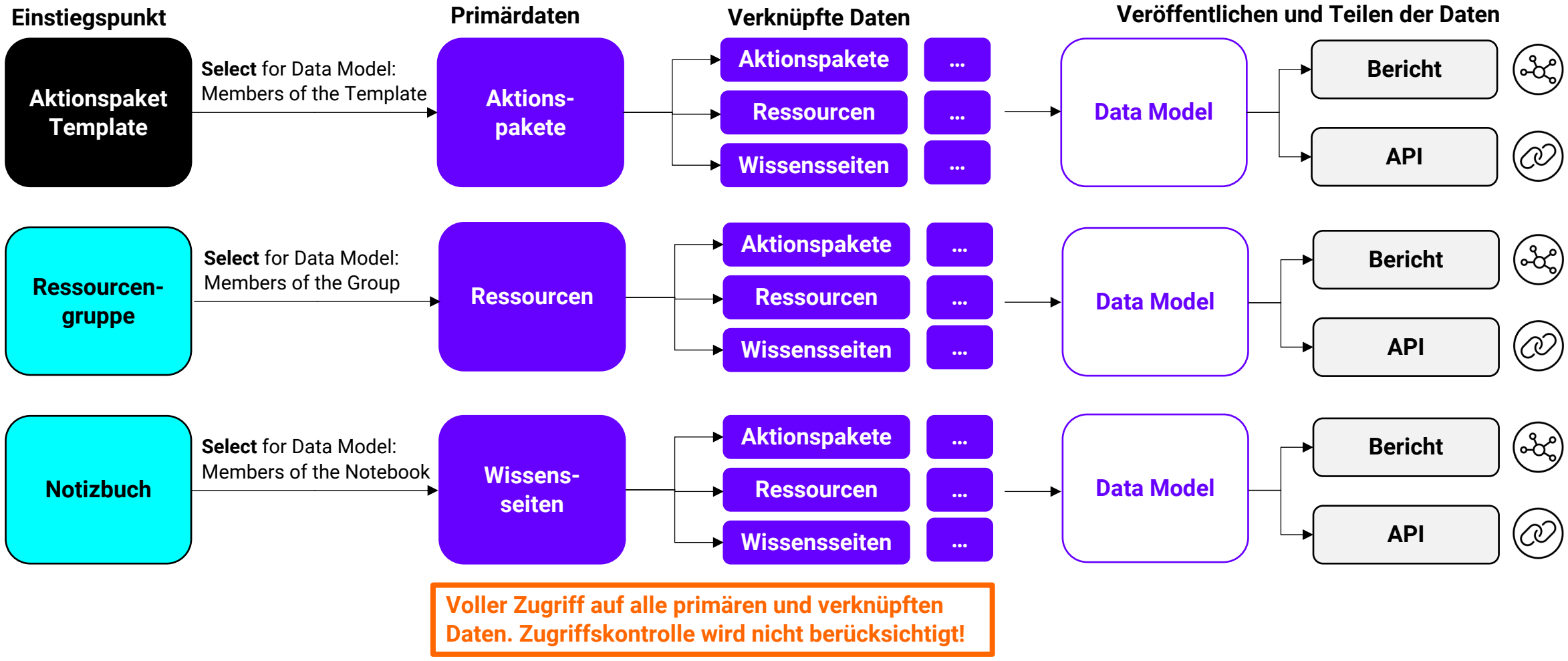


Designer APIs



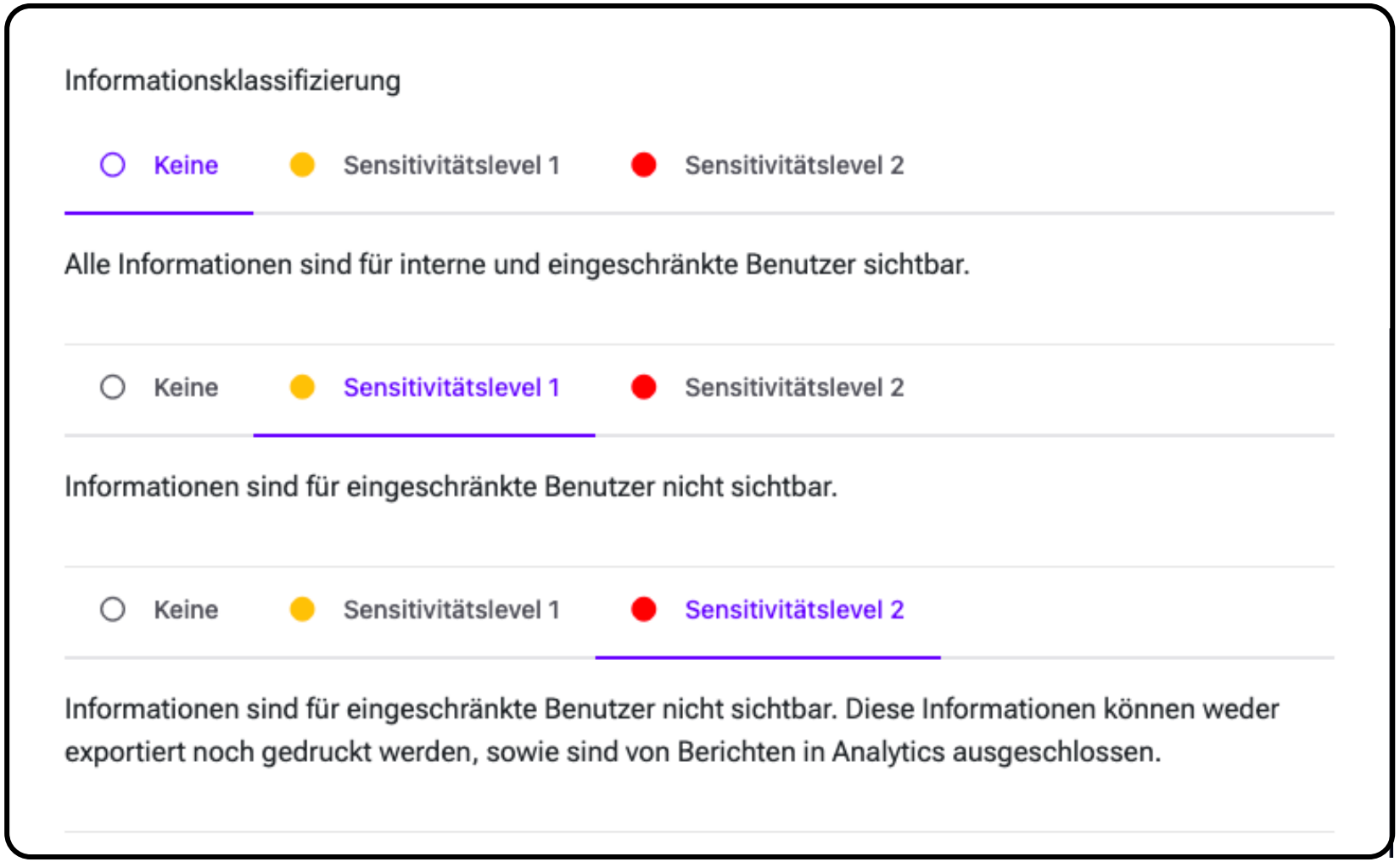
Erforderliche Add-Ons: Designer and Integration Portal+

Designer


Einstiegspunkt
Primärdaten
Verknüpfte Daten
Veröffentlichen und Teilen der Daten
Aktionspaket Template
Select for Data Model: Members of the Template
Aktions-pakete
Aktionspakete
Ressourcen
Wissensseiten
...
Data Model
Bericht
API
Ressourcen-gruppe
Select for Data Model: Members of the Group
Ressourcen
Notizbuch
Select for Data Model: Members of the Notebook
Wissens-seiten
Voller Zugriff auf alle primären und verknüpften Daten. Zugriffskontrolle wird nicht berücksichtigt!

Erweiterte Zugriffskontrolle mit SensitiveDataControl

Mit SensitiveDataControl kann der Zugriff und die Nutzung von Informationen weiter verfeinert werden



Definieren Sie auf der Vorlage pro Komponente die Sensitivitätsstufe einer Information.

Erforderliches Add-On: SensitiveDataContol

Lassen Sie uns in Kontakt bleiben.

trustkey

Rufen Sie uns an:
+49-89-991557-11

Folgen Sie uns:
LinkedIn

Schreiben Sie uns eine E-Mail:
mail@trustkey.eu

Process Execution Plattform

Strukturieren, Verknüpfen, Automatisieren

Besuchen Sie unsere Webpage
https://www.trustkey.eu/

Erkunden Sie unser Playbook
https://www.trustkey.eu/de/help-cemter/

Buchen Sie eine Web-Demo
https://www.trustkey.eu/de/trustkey-live-demo-de/