NOVA
Berechtigungskonzept

Historie

Version	Gremium	Datum	Status
Erste Lesung (V0.8)	Arbeitsgruppe IT	Im Oktober 2023	Erfolgt
Erste Lesung (V0.9)	Kommission Vertrieb	31.10.2023	Erfolgt
Verabschiedung (V1)	Kommission Vertrieb	11.12.2023	Freigabe

Alliance SwissPass Länggassstrasse 7 3012 Bern Tel +41 31 359 22 40
info@allianceswisspass.ch allianceswisspass.ch

Inhaltsverzeichnis

Abbildungsverzeichnis

0 Vorbemerkungen

Die Eidgenössische Finanzkontrolle (EFK) hat 2019 die NOVA-Plattform einer IT-Anwendungsprüfung unterzogen. Im Herbst 2022 erfolgte aufgrund des Projekts GITA (heute myRIDE) eine Nachprüfung. Die EFK empfiehlt der Alliance SwissPass, für NOVA Anbieter ein übergeordnetes, durchgängiges Berechtigungskonzept anzugehen.
Das bestehende Berechtigungskonzept der Mandatsträgerin soll auf die Anwendbarkeit aller angeschlossenen TU/Verbünde weiterentwickelt werden. Gegenwärtig gibt es im Bereich NOVA verschiedene Dokumente, die sich mit dem Thema Autorisierung/Zugang zu NOVA befassen, jedoch ist keines davon übergreifend.
Dieses Konzept zu einem übergeordneten, durchgängiges Berechtigungskonzept wurde im Auftrag des Strategierates erarbeitet. Um die verschiedenen Ansprüche berücksichtigen zu können und eine breite Akzeptanz zu erreichen, werden verschiedene Gremien konsultiert.

0.1 Gegenstand und Zweck

Das Rollen- und Berechtigungskonzept dient dem Schutz der Vertraulichkeit und der Integrität. Dieses Dokument ist die Grundlage für die Alliance SwissPass zur Implementierung der Berechtigungen.

Ziele des Rollen- und Berechtigungskonzepts sind:

- Klarheit bei der Vergabe von Rechten
- Übergreifende, verbindliche Definition der Berechtigungsvergabe
- Verringerung des administrativen Aufwands

Die Plattform «NOVA» ist das zentrale Vertriebs-Backend des öffentlichen Verkehrs Schweiz, über welches die angeschlossenen Transportunternehmen Angebote erstellen und über unterschiedliche Vertriebskanäle verkaufen können. Das Berechtigungskonzept dokumentiert die Abläufe und Schnittstellen des Freigabeprozesses der NOVA. Dabei sollen mögliche Optimierungen identifiziert und beschrieben werden. In diesem Dokument werden folgende Themen erläutert:

- Governance
- Übersicht der kritischen Services und Rollen
- Zugriffsprozesse
- IKS und Revision

0.2 Rahmenbedingungen und Prämissen

Gegebenheiten, die in der aktuellen Situation entweder nicht beeinflusst werden können oder sollen, die jedoch für die Erreichung der gesetzten Ziele von Bedeutung sind. Sie beeinflussen also die Zielwirksamkeit von Massnahmen.

0.3 Abgrenzungen

Der Fokus dieses Konzepts liegt auf den NOVA Anbietern und seinen Tools. Folgende Themen werden nicht berücksichtigt, weil sie schon in anderen Dokumenten beschrieben oder auf die Finanzkette keinen Einfluss haben:

- NOVA Abrechnung
- NOVA Services ohne finanziellen Impact (Bsp. SwissPass Tools, etc.)

0.4 Geltungsbereich

Dieses Rollen- und Berechtigungskonzept gilt für alle Mitarbeitenden der TU der Alliance SwissPass. Die Mitarbeitenden im IT-Mandat werden zur Einhaltung der entsprechenden Anforderungen vertraglich verpflichtet.

1 Governance

Der Nationale Direkte Verkehr (NDV) mit seiner überregional ausgerichteten und streckenbasierten Tarifstruktur und die öV-Verbünde mit ihrer Zonenlogik und ihrem Fokus auf den Orts- und Agglomerationsverkehr sind in ihrer Systematik unterschiedlich. Sie verfolgen jedoch gleiche Ziele, bedienen mitunter dieselbe Kundschaft und engagieren sich in vergleichbaren Themenfeldern.
Zudem funktionieren beide Systeme nach dem gesetzlich verankerten Grundprinzip von «Eine Reise, ein Ticket».
Deshalb haben sich die öV-Verbünde und die am Nationalen Direkten Verkehr teilnehmenden Transportunternehmen ab dem Jahr 2020 in einer gemeinsamen Organisation zusammengeschlossen: der Alliance SwissPass. In der Alliance SwissPass verschmolzen die vorher getrennten Gremien und Entscheid Strukturen des NDV und der öV-Verbünde. Sämtliche Kompetenzen, welche bisher in den Händen der Gremien des NDV respektive der öV-Verbünde lagen, fielen an die neue Organisation. Die innerhalb der Alliance SwissPass behandelten Themen sind grundsätzlich weiterhin in NDV und Verbünde aufgeteilt. Allerdings haben neu alle Beteiligten ein Mitbestimmungsrecht. Im gemeinsamen Geschäftsfeld «öV» behandelt die Branchenorganisation zudem Themen, die beide Tarifsysteme betreffen. Damit ermöglicht sie zum Wohle der Kundinnen und Kunden sowie des öffentlichen Verkehrs ein gemeinschaftlicheres, harmonischeres Zusammenspiel, effizientere Prozesse und abgestimmter Weiterentwicklungen in den beiden Tarifwelten. Gegenüber der Politik, den Behörden und anderen Anspruchsgruppen kann die Alliance SwissPass zudem als legitime Vertretung des gesamten öffentlichen Verkehrs auftreten. Im Nationalen Direkten Verkehr koordiniert die Alliance SwissPass weiterhin die gemeinsamen Tätigkeiten in den Bereichen Tarif, Sortiment und Vermarktung. In der Verbundwelt unterstützt sie die Bestrebungen zu einer verstärkten Harmonisierung unter Berücksichtigung der regionalen Rahmenbedingungen. Die Governance-Strukturen erlauben es der Branchenorganisation zudem, zugunsten der Kundinnen und Kunden auch Harmonisierungen und Vereinheitlichungen im gesamten öffentlichen Verkehr einzuführen – also sowohl im NDV als auch in den Verbünden.

Änderungen an der Governance, müssen jeweils durch einen Gremien-Entscheid genehmigt werden. Kleinere Anpassungen im Dokument (Bsp.: Ergänzungen, Abänderungen, Streichungen, etc.) können durch ch-integral in Zusammenarbeit mit der Mandatsträgerin geändert werden.

Rolle der Geschäftsstelle
Im Rahmen eines Mandatsvertrages des Strategierates führt der Verein ch-integral die Geschäftsstelle der Alliance SwissPass. Die Geschäftsstelle (GS) ist unabhängig von einzelnen Transportunternehmen und Verbünden.
Die Geschäftsstelle muss deshalb für jede kritische Rolle eine Berechtigung definieren. Alternativ, definiert die GS mandatierte SBB-Stellen, die wiederum die Berechtigungen vergeben.
Die GS definiert welche Berechtigungen für den IT Mandatsträger oder der TU, Verbunde oder Dritte bestimmt sind.

Kontakt
Bei Fragen zum Berechtigungskonzept:
Alliance SwissPass
c/o ch-integral
Länggassstrasse 7
3012 Bern

tarife@allianceswisspass.ch

Rolle der SBB als IT Mandatsträger und Support (CC Brig)
Administrative, Zuweisung von unkritischen Rollen oder, falls zwingend, Entscheidung, wem eine kritische Rolle zugewiesen wird.

Rolle der Kanäle (TU, Verbunde oder Dritte)
Die Governance definiert, welche Berechtigungen für den IT Mandatsträger oder der TU, Verbunde oder Dritte bestimmt sind. Wenn die Unternehmen bewilligt sind, bestimmten Berechtigungen zu bekommen, wird eine delegierte Person (und zusätzlich eine Stellvertretung) pro Unternehmen definiert, wer die Berechtigungen bestellt oder validiert wird. Die delegierte Person nimmt die Verantwortung für die korrekte Nutzung des Zugriffs, inkl. die Aufhebung der Berechtigung, wenn es nicht mehr notwendig ist. Sie darf für sich selbst keine Berechtigung bestellen oder validieren.
Die Unternehmen sind verpflichtet, die delegierten Personen aktuell zu halten.

Revision
Eine regelmässige Revision wird durch die NDV-Revisionsstelle in Auftrag gegeben.

1.1 Entscheidungskompetenzen für die Berechtigungen der Rollen

Die Rollen im Tool werden in kritisch und unkritisch getrennt.

- Nicht kritische Rollen: keine wesentliche Relevanz für wichtige Funktionstrennungen oder Zugriffsbeschränkungen innerhalb von finanz- und/oder betriebsrelevanten Prozessen von NOVA.
- Kritische Rollen: relevant für wichtige Funktionstrennungen oder Zugriffsbeschränkungen innerhalb von finanz- und/oder betriebsrelevanten Prozessen von NOVA Anbieter.

Für die nicht kritischen Rollen gibt NOVA Partnermanagement die Freigabe frei.
Für alle kritischen Rollen entscheidet der Themenverantwortliche Vertrieb, Kontrolle und Einnahmensicherung der Geschäftsstelle Alliance SwissPass, ob die Berechtigung freigegeben wird.

Die Liste der kritischen Rollen wird kontinuierlich aktualisiert und publiziert. Dort findet sich auch eine Beschreibung, wie eine Genehmigung bestellt werden kann.
Siehe https://confluence.sbb.ch/display/NOVAUG/NOVA+access+and+roles

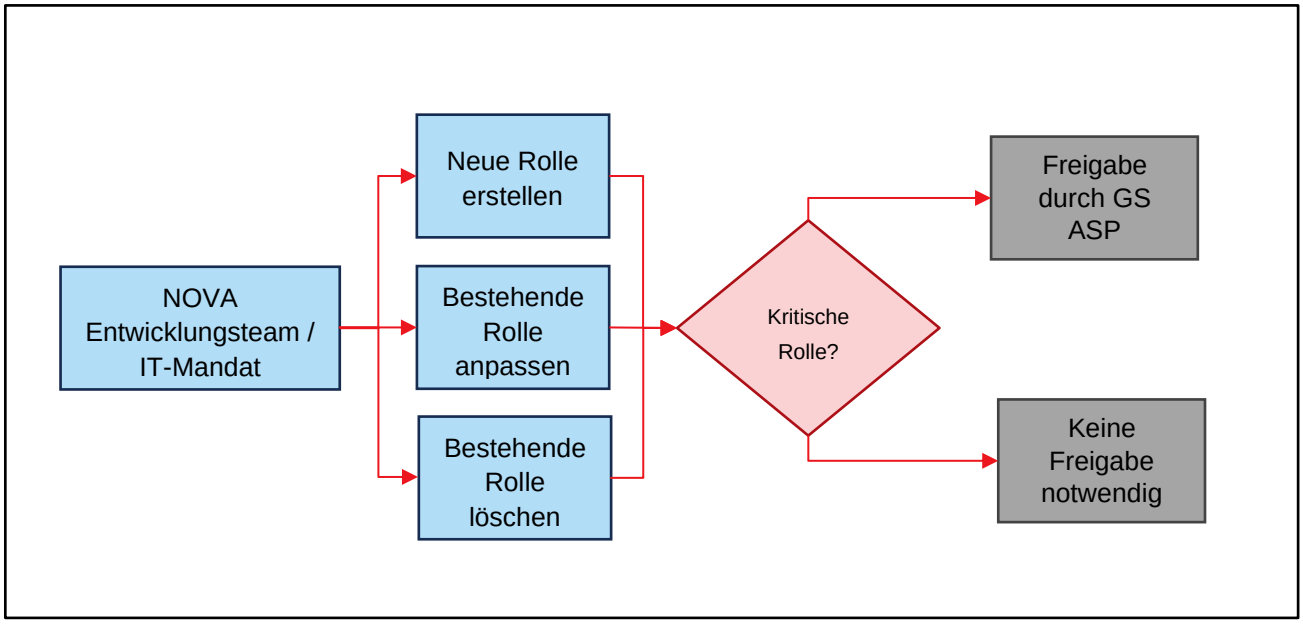

Abbildung 1 – Pflege-Prozess der Rollen

2 Übersicht der kritischen Services

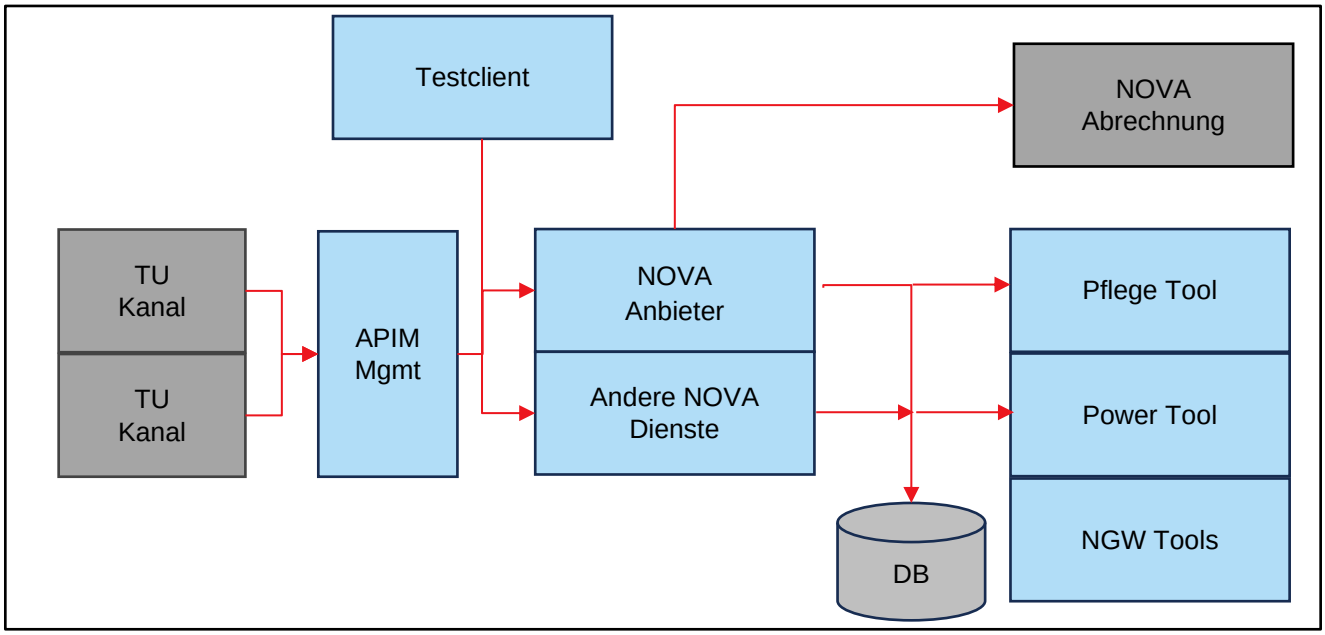

Abbildung 2 – Übersicht der Services

NOVA Anbieter ist die Komponente der NOVA Plattform, welche sicherstellt, dass allen Verkäufern von öV-Leistungen (Leistungsvermittler) nach einheitlichen Kriterien erstellte und tarifierte Angebote des öffentlichen Verkehrs (öV) der Schweiz zur Verfügung stehen. Konkret übernimmt NOVA Anbieter die gesamte Preisberechnung für öV-Billette sowie die Berechnung, wie die aus Verkäufen von öV-Leistungen erwirtschafteten Erträge auf, die begünstigen Organisationen verteilt werden.

Das Pflegetool erlaubt Stammdaten und Konfigurationen zu verwalten.

Das **Power Tool** erlaubt, Kundendaten zu pflegen und deren verkauften Leistungen zu bearbeiten (z.B sperren und entsperren).

Der **Testclient** erlaubt Kanäleoperationen zu simulieren.

Die **APIM** = Advanced Programming Interface Management erlaubt den Zugang auf die NOVA Plattform.

NGW Tools = steuern die Coupons und die Kampagnen der Neuen Gutscheinwelt

3 Übersicht der Arbeitsrollen

Die verschiedenen Rollen bei der Entwicklung und Wartung von NOVA können wie folgt in Funktionsbereiche gruppiert werden (für mehr Details siehe Anhang 1):

- Entwicklung & Datenpflege mit Finanzrelevanz
  - Entwicklung NOVA Anbieter
  - Datenpflege finanzrelevanter NOVA Stammdaten
- Transportwesen, Betrieb, Systemadministration
  - Transportwesen
  - Betrieb und Produktionsmonitoring
  - Systemadministration – Vergabe und Prüfung Zugriffsrechte
  - Verwaltung der NOVA Prod-DB (Leistungsdatenbank), der technischen Konfiguration von NOVA Anbieter und des produktiven NOVA Test-Clients
- Fachprüfung
  - Fachprüfung NOVA Anbieter
  - Fachprüfung NOVA Stammdaten
- Customizing Sparangebot
  - Mutation der Rahmenbedingungen und Kontingente, die als Basis für die Sparangebot-Algorithmen dienen
- Weitere NOVA Funktionen
  - Entwicklung und Betrieb Pflege-Infrastruktur für Stammdaten
  - Entwicklung und Datenpflege für NOVA-Komponenten ohne Finanzrelevanz
  - Entwicklung und Datenpflege für SAP-basierte NOVA Komponenten

3.1 Entwicklung & Datenpflege (finanzrelevant)

Gruppierung, da unter diesen Funktionen kein kritische Funktionentrennung besteht, da diese artgleich sind. Die NOVA Anbieter Software-Entwicklung und die NOVA Stammdatenpflege unterliegen eigener Fachprüfung, um die Segregation of Duties (SoD) zu gewährleisten, selbst wenn jemand sowohl an der Softwareentwicklung als auch an der Stammdatenmutation beteiligt ist.
Wichtiger Spezialfall - Stammdatenpflege durch «externe Datenpfleger»: Im Allgemeinen wird die NOVA Stammdatenpflege vom NOVA Datenmanagement im Mandat im Auftrag aller Transportunternehmen. hauptsächlich von SBB-Mitarbeitern durchgeführt. Gelegentlich werden jedoch auch «externe Datenmanager» der Transportunternehmen eingesetzt, um Tarifdaten für ihre eigenen Unternehmen zu pflegen. Zum Beispiel pflegen Mitarbeiter der Postauto AG Tarifnetz- und Produktdaten ausschliesslich für von der Postauto AG betriebene Strecken. Derzeit besteht keine Zugriffsrechttrennung zwischen diesen Mitarbeitern, sodass SBB-Mitarbeiter auf die Tarifdaten der Postauto AG und umgekehrt zugreifen können. Dies wird derzeit als unproblematisch erachtet:

- Externe Datenmanager die NOVA Stammdaten verwalten dürfen, werden in die NOVA-Betriebsorganisation intergiert. Dies ist notwendig, da die Datenpflege-Tools Expertenwissen voraussetzen, um sie richtig anzuwenden. Die Integration beinhaltet Schulungen, die gleiche Qualitätsorientierung und die Einhaltung der gleichen Änderungsprozesse für externe Datenverwalter.
- Jegliche Datenmutationen unterliegen den für die «Finanzrelevante Stammdaten für NOVA Anbieter» etablierten Change Prozessen, auch wenn sie durch externe Datenmanager erfasst werden. Diese Änderungsprozesse stellen sicher, dass alle wichtigen Anpassungen der finanzrelevanten Stammdaten zumindest durch eine unabhängige Vier-Augen-Prüfung verifiziert werden (IKS-NOVAAN-04 – «Datenrelease geprüft und freigegeben»). Im Rahmen der Regressionstests würde auffallen, dass Unbefugte nicht beauftragte Änderungen an den Tarifstammdaten anderer Verkehrsunternehmen vornehmen.

Aus heutiger Sicht wird deshalb der Grad an Qualitätssicherung als ausreichend eingestuft auch ohne weitere Auftrennung der Zugriffsrechte. Ergänzend bieten die «generischen Datenpflege-Rechte» die Möglichkeit für flexible Stellvertretungen und einfache Prozesse in Notfällen (wenn beispielsweise alle Vertreter des Postauto AG verhindert wären und dringend eine Anpassung an ihren Tarifdaten gemacht werden muss). Gerade bei kleineren Unternehmen können keine grossen Teams für die Datenpflege finanziert werden und eine Stellvertretung nicht in jedem Fall sichergestellt werden.

Eine funktionale Trennung der Zugriffsrechte von Datenmanagern der verschiedenen Transportunternehmen wäre technisch möglich, aber nicht trivial. Diese könnte zukünftig in Betracht gezogen werden, es wird jedoch empfohlen, den technischen und finanziellen Aufwand für die Umsetzung gegen den tatsächlichen Gewinn an Sicherheit im System aufzuwiegen. Wenn sich folgende Rahmenbedingungen verändern, wären dies Gründe für eine Neubeurteilung der Lage:

- die Anzahl der externen Datenpfleger und/oder Transportunternehmen, die ihre eigenen Daten pflegen, nimmt erheblich zu
- die Vorgaben für die Qualitätskontrollen in den Stammdaten-Change Prozessen werden gelockert

3.2 Transportwesen, Betrieb, Systemadministration

Gruppierung, dass trotzdem alle notwendigen, kritischen Funktionentrennungen im Betrieb von NOVA gewährleistet werden können. Gewährleistet sind:

- die Trennung von Entwicklung und Transportwesen
- die Trennung von Stammdatenpflege und Transportwesen
- die Trennung von Rollen-Entwicklung und Zugriffsrechtvergabe
- die Trennung «Verwaltung der Prod-DB und der technischen Konfiguration von NOVA Anbieter» von nicht-Betriebsrollen

3.3 Fachprüfung

Gruppierung, da unter diesen Funktionen keine kritische Funktionentrennung besteht, da diese artgleich sind. Eine Person darf prinzipiell an der Fachprüfung neuer NOVA Anbieter Software wie auch an der Fachprüfung von NOVA Stammdaten beteiligt sein. Wichtig ist die Trennung zwischen Fachprüfung und Entwicklung - diese ist gewährleistet. Dass eine Person sowohl Daten wie auch Software fachlich prüft, tritt generell im Betrieb von NOVA zurzeit jedoch nicht auf.

3.4 Customizing Sparangebote

Der Bereich «Customizing Sparangebote» beschränkt sich auf lediglich diese Funktion - es existiert keine Gruppierung.

Es gilt jedoch zu beachten, dass das Customizing dieser Parameter an die jeweiligen Tarifeigner ausgelagert wird. Es ist daher wichtig, dass die Rollenprofile für das Customizing jedem Tarifeigner nur Zugriff auf die durch ihn verantworteten Streckenabschnitte ermöglichen.

3.5 Weitere NOVA Funktionen

Diese Funktionen haben keine direkte Relevanz für die Finanzflüsse über die NOVA Applikation oder werden bereits durch separate IKS validiert. Der Einfachheit halber können sie daher für «IKS NOVA» als «nicht relevante Gruppe» zusammengefasst werden.

4 Zugriffsprozesse

Die Zugriffe müssen beantragt und freigegeben werden. Die Governance legt fest, wer das Recht hat, den Zugang zu nutzen, und wer das Recht hat, ihn zu genehmigen. Die Zugriffe müssen jährlich validiert werden.

4.1 Beantragung und Zuweisung neuer Zugriffsrechte

1. Neues Zugriffsrecht wird beantragt
2. Die Rolle wird gemäss Governance zuerst geprüft
3. Kritischer Zugriff muss gemäss Governance bestätigt werden. Wenn ein Transportunternehmen mehrere kritischen Rollen benötigt, wird die Verantwortung der Bestätigung delegiert. Eine Person pro TU ist bestimmt, um diese Berechtigung zu evaluieren.
4. im Falle einer Ablehnung erfolgt eine begründete Benachrichtigung
5. Wenn die Berechtigungsanfrage bestätigt wird, werden die Zugriffsrechte erteilt.

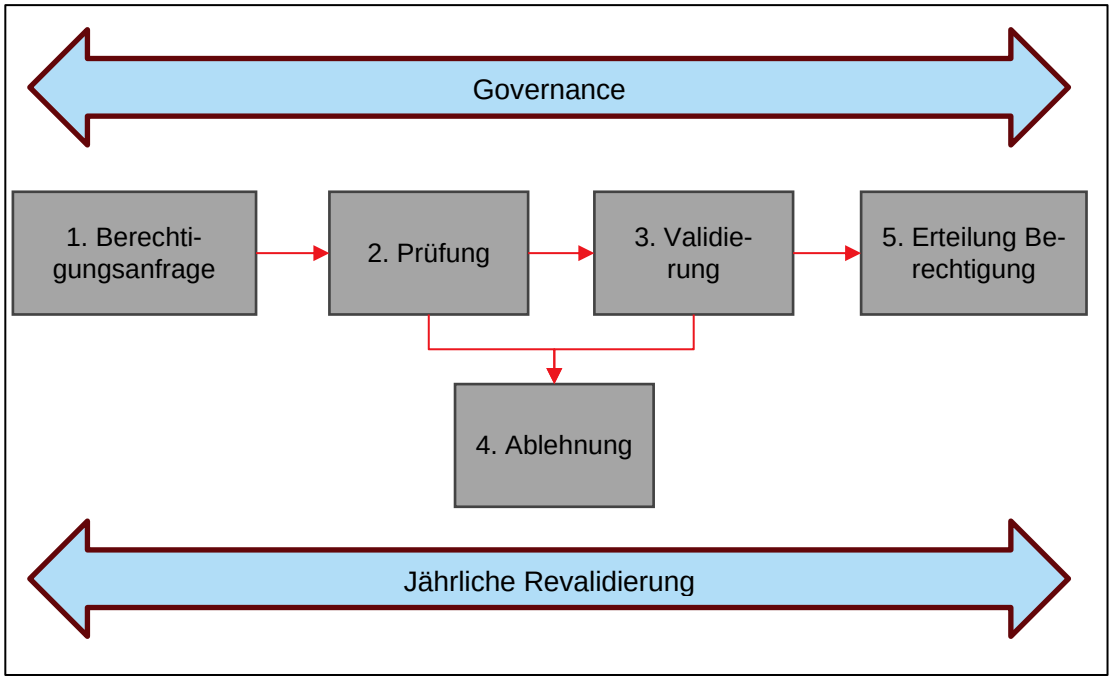

Abbildung 3 – Zugriffprozesse

4.2 Bereinigung der Zugriffsrechte

Im Falle eines Wechsels der funktionalen Rolle / Ausscheiden einer Person aus seiner Organisation.

1. Wenn eine Person seine Rolle innerhalb seiner Organisation ändert, was zur Gewährung neuer Zugriffsrechte führen kann, müssen die aktuellen Zugriffsrechte der Person überprüft und bereinigt werden, bevor neue Rechte gewährt werden. Dadurch wird sichergestellt, dass Konflikte bei der Funktionstrennung vermeidet werden.
2. Falls eine Person aus seiner Organisation ausscheidet, müssen alle Zugriffsrechte entfernt werden.

4.3 Berechtigungsprüfung

Die Berechtigungen werden jährlich durch die Mandatsträgerin oder die verantwortlichen Mitarbeiterinnen und Mitarbeiter der TU oder der kritischen Services überprüft.

5 IKS und Revision

In Anbetracht der zentralen, finanzrelevanten Funktion von NOVA Anbieter in der IT-Prozesskette des öffentlichen Verkehrs, sowie der erheblichen Umsätze, die über die Plattform generiert werden, wurde beschlossen, ein «Internes Kontrollsystem» (IKS) für NOVA Anbieter zu etablieren. Dieses IKS stellt sicher, dass angemessene Kontrollen und Prozesse implementiert und gelebt werden, die sicherstellen, dass die Tarifierung und Umsatzverteilung via NOVA korrekt und nachvollziehbar funktioniert.

Link zum IKS NOVA Anbieter: https://confluence.sbb.ch/display/NOVAUG/IKS+NOVA+Anbieter

Die Kontrollen sind:

1. Einhaltung 4-Augenprinzip bei Software-Releases
2. Für Major Releases: Keine produktionsverhindernden Mängel beanstandet durch die Nutzer der Plattform vor der Produktivschaltung
3. Software-Releases geprüft und freigegeben
4. Datenrelease geprüft und freigegeben
5. Einhaltung 4-Augenprinzip bei TPS (Tarif Perioden Stammdaten) -Wechseln
6. Stichproben für die korrekte Umsetzung der wöchentlichen Tarifnetzanpassungen
3. Einhaltung Vorgaben bei der Vergabe von zu Zugriffsrechten
4. Korrekte Einlieferung von öV-Leistungen in die Abrechnungssysteme

Im Jahr 2022 hat die KoV entschieden, jährlich eine Revision durchzuführen (ISAE 3402 Typ 2). Der Bericht dokumentiert die Dienstleistungen der SBB im Bereich NOVA und schliesst die Angemessenheit der Ausgestaltung und das wirksame Anwenden der Kontrollen zur Erreichung der beschriebenen Kontrollziele mit ein. Der Zweck der Beschreibung besteht darin, Dienstleistungsbezügern Informationen über die NOVA-Dienstleistungen der SBB zu vermitteln, insbesondere über die Kontrollen, die vorgesehen sind, um die von der SBB definierten Kontrollziele zu erfüllen

6 Glossar

Begriff	Erklärung
Alliance SwissPass	Branchenorganisation des öffentlichen Verkehrs, bestehend aus rund 250 Transportunternehmen und 18 Verbünden.
Autorisierung	siehe Berechtigung
Berechtigung	Regelt, wer mit welchen Daten was tun darf, und zwar bezogen auf die ganze Spannweite zwischen Personen und Daten.
Funktion	Hier sind organisatorische Funktionen gemeint, also Aufgaben, Ämter, Stellen – auf der Seite der Subjekte. Daneben gibt es – auf der Seite der Objekte – auch Softwarefunktionen wie z.B. das Anzeigen von Adresslisten.
Geschäftsstelle ASP	Die Geschäftsstelle führt die Geschäfte der Alliance SwissPass gemäss den Vorgaben des Übereinkommens 500
IKS	Unter IKS versteht man die Gesamtheit des internen Kontrollsystems, die zur Überwachung wichtiger betrieblicher Abläufe im Unternehmen beitragen.
ISAE 3402 Typ 2	ist ein von der International Federation of Accountants (IFAC) veröffentlichter internationaler Prüfungsstandard, in dem die Prüfung eines internen Kontrollsystems bei einem Dienstleistungsunternehmen inklusive Berichterstattung durch einen Wirtschaftsprüfer geregelt ist. Typ2 prüft zusätzlich, ob die Kontrollen über den gesamten Prüfungszeitraum (üblicherweise ein Wirtschaftsjahr) wirksam waren (Funktionsprüfung).
NOVA-Plattform	Nationale Plattform für den Verkauf von Fahrausweisen. Produktname: «Netzweite ÖV-Anbindung»
Rolle	≈Aufgabe ≈Stelle ≈Funktion. Eine Rolle bündelt und vereinfacht die zig-tausend möglichen Beziehungen zwischen Personen und Objekten.
Segregation of Duties (SoD)	auch bekannt als „Prinzip der Funktionstrennung“ ist ein Geschäftsprozess innerhalb einer Organisation. SoD-Richtlinien fungieren als Sicherheitsvorkehrung, denn viele Geschäftsprozesse können, wenn sie von einer einzigen Person ausgeführt werden, zu einem Interessenkonflikt führen.
Zugriffsrecht	siehe Berechtigung
Zugriffskontrolle, Zugriffsschutz	Systemlogik (Mechanismus), die nur diejenigen Zugriffe erlaubt, für die jemand berechtigt ist.

7 Anhang 1 – Liste der inkompatiblen Rollen (Segregation on Duties)

Tätigkeiten / Aufgaben (Funktion oder Transaktion)	Entwicklung NOVA Anbieter	Datenpflege finanzrelevanter NOVA Stammdaten	Fachprüfung NOVA Anbieter	Fachprüfung NOVA Stammdaten	Transportwesen	Betrieb und Produktionsmonitoring	Verwaltung der NOVA Prod-DB #1)	Systemadministration - Vergabe und Prüfung Zugriffsrechte	Customizing Sparangebote	Entwicklung & Betrieb Pflegeinfrastruktur für Stammdaten	Entwicklung & Datenpflege für NOVA-Komponenten ohne Finanzrelevanz	Entwicklung & Datenpflege für SAP-basierte NOVA-Komponenten
Entwicklung NOVA Anbieter			Konflikt K 01		Konflikt K 03		Konflikt K 05	Konflikt K 06	Konflikt K 07			
Datenpflege finanzrelevanter NOVA Stammdaten				Konflikt K 02	Konflikt K 04		Konflikt K 05		Konflikt K 07			
Fachprüfung NOVA Anbieter							Konflikt K 05		Konflikt K 07		Konflikt K 09	
Fachprüfung NOVA Stammdaten							Konflikt K 05		Konflikt K 07			
Transportwesen									Konflikt K 07		Konflikt K 10	
Betrieb und Produktionsmonitoring									Konflikt K 07			
Verwaltung der NOVA Prod-DB, #1)									Konflikt K 05 / K 07	Konflikt K 05	Konflikt K 05	Konflikt K 05
Systemadministration - Vergabe und Prüfung Zugriffsrechte									Konflikt K 07	Konflikt K 08	Konflikt K 11	
Customizing Sparangebote										Konflikt K 07	Konflikt K 07	Konflikt K 07
Entwicklung und Betrieb Pflegeinfrastruktur für Stammdaten												
Entwicklung & Datenpflege für NOVA-Komponenten ohne Finanzrelevanz												
Entwicklung & Datenpflege für SAP-basierte NOVA-Komponenten												

Tabelle 1 - inkompatiblen Rollen (SoD)

#1: Verwaltung der NOVA Prod-DB (Leistungsdatenbank), der technischen Konfiguration von NOVA Anbieter und des produktiven NOVA Test-Clients

Legende für die Kennzeichnung eines SoD-Konfliktes

	Nicht relevante Felder. Entweder weil es sich um die gleiche Funktion handelt oder weil der Konflikt bereits auf der anderen Seite der Diagonale abgehandelt wird.
	Es besteht kein SoD-Konflikt (Erklärungen warum kein Konflikt: siehe Lasche «unkritische Funkt-Kombinationen»)
	Es besteht kein SoD-Konflikt (die Funktionen gehören dem gleichen, gruppierten Bereich an)
Niedriger Konflikt	Diese Kombination zweier Tätigkeiten ist ein SoD-Konflikt mit tiefer Einstufung. Die Rollen sollten prinzipiell getrennt sein, die Kombination kann aber keinen oder höchstens marginalen Einfluss auf die Finanzflüsse über die NOVA Plattform haben. Dieser Konflikt wird nicht überwacht.
Konflikt	Diese Kombination zweier Tätigkeiten ist ein SoD-Konflikt mit hoher Einstufung. Sie führt potenziell zu wesentlichem Schaden mit Hinblick auf die Finanzflüsse über die NOVA Plattform. Dieser Konflikt wird aktiv gemanagt und überwacht durch folgende Möglichkeiten: - Trennung der Rollen durch technische Zugriffsrechte (Überwachung der Zugriffsrechte durch den SoD-Risk Owner mit kompensierenden Kontrollen) - Wo keine Trennung durch Zugriffsrechte sinnvoll oder praktikabel: Die Einhaltung der SoD wird durch den SoD-Risk Owner mit kompensierenden Kontrollen überwacht / eingeschränkt

Kritische Rollenkombinationen - Konflikte

K01: Entwicklung NOVA Anbieter - Fachprüfung NOVA Anbieter • Beide Funktionen führen dazu, dass ein Entwickler seine eigenen Softwareanpassungen fachprüfen kann • Dies stellt einen Verstoss gegen das 4-Augen-Prinzip dar • Risiko besteht in einer Brutto-Sicht • Folge: nicht durch 4-Augenkontrolle geprüfte Änderungen können in produktiven Software-Versionen enthalten sein. Dies kann ungewünschte Folgen für finanzrelevante Funktionen von NOVA haben	K02: Datenpflege finanzrelevanter NOVA Stammdaten - Fachprüfung NOVA Stammdaten • Beide Funktionen führen dazu, dass ein Datenmanager seine eigenen Datenmutationen fachprüfen kann • Dies stellt einen Verstoss gegen das 4-Augen-Prinzip dar • Risiko besteht in einer Brutto-Sicht • Folge: nicht durch 4-Augenkontrolle geprüfte Änderungen können in produktiven, finanzrelevanten Stammdaten enthalten sein. Dies kann ungewünschte Folgen für finanzrelevante Funktionen von NOVA haben
K03: Entwicklung NOVA Anbieter – Transportwesen • Beide Funktionen führen dazu, dass ein Entwickler seine eigenen Softwareanpassungen eigenständig in Produktion transportieren kann. Dadurch kann die Fachprüfung umgangen werden. • Dies stellt einen Verstoss gegen das 4-Augen-Prinzip dar • Risiko besteht in einer Brutto-Sicht • Folge: ungeprüfte Änderungen können in produktiven Software-Versionen enthalten sein. Dies kann ungewünschte Folgen für finanzrelevante Funktionen von NOVA haben	K04: Datenpflege finanzrelevanter NOVA Stammdaten – Transportwesen • Beide Funktionen führen dazu, dass ein Datenmanager seine eigenen Datenmutationen eigenständig in Produktion transportieren kann. Dadurch kann die Fachprüfung umgangen werden. • Dies stellt einen Verstoss gegen das 4-Augen-Prinzip dar • Risiko besteht in einer Brutto-Sicht • Folge: ungeprüfte Änderungen können in produktiven, finanzrelevanten Stammdaten enthalten sein. Dies kann ungewünschte Folgen für finanzrelevante Funktionen von NOVA haben
K05: Alle Funktionen ausserhalb des Bereichs Transportwesen, Betrieb, Systemadministration - Verwaltung der NOVA Prod-DB (Leistungsdatenbank), der technischen Konfiguration von NOVA Anbieter und des produktiven NOVA Test-Clients • Diese Funktionskombinationen führen dazu, dass Mitarbeiter ausserhalb der engeren NOVA Betriebsorganisation Schreibzugriff auf kritische Produktionsdaten wie die Leistungsdaten und Konfigurationsparameter von NOVA Anbieter erhalten. Ebenso könnten diese Personen über den produktiven Test-Client von NOVA Anbieter «scharfe» Verkäufe und Erstattungen von öV-Leistungen auslösen, die in die öV-Finanzabrechnung einfliessen würden. • Der Zugriff auf die Prod-DB und die NOVA Konfiguration bedarf einer systemkritischen Administratoren-Berechtigung, die nur an wenige, für den Betrieb der Plattform zuständige Personen vergeben werden sollte • Risiko besteht in einer Brutto-Sicht • Folge: viele Personen könnten potenziell produktive Leistungsdaten verändern, hinzugefügten oder löschen, bzw. Konfigurationsparameter verändern. • Beides kann die Finanzflüsse über NOVA beeinflussen.	K06: Entwicklung NOVA Anbieter - Systemadministration - Vergabe und Prüfung Zugriffsrechte • Beide Funktionen führen dazu, dass ein Entwickler Berechtigungen für NOVA Anbieter entwickeln und selbstständig vergeben könnte • Dies stellt einen Verstoss gegen das 4-Augen-Prinzip dar • Risiko besteht in einer Brutto-Sicht • Folge: ein Entwickler könnte sich oder anderen Zugriffe auf kritische Systemkomponenten von NOVA Anbieter verschaffen und dadurch Finanzflüsse beeinflussen.

Alliance Swiss

K07: Alle NOVA Funktionen - Customizing Sparangebote • Eine Kombination dieser Funktionen führt dazu, dass Mitarbeiter der Betriebsorganisation für NOVA die Rahmenbedingungen für das Angebot von Sparbilletten und -Tageskarten verändern könnten • Dies stellt einen Verstoss gegen die NOVA Nutzungsbedingungen dar, die diese Mutationen lediglich für Vertreter der Tarifeigner vorsieht • Risiko besteht in einer Brutto-Sicht • Folge: Personen, die nicht Vertreter der Tarifeigner sind, könnten die Rahmenbedingungen für das Angebot von Sparbilletten und -Tageskarten verändern und dadurch die Finanzflüsse beeinflussen	K08: Entwicklung und Betrieb Pflegeinfrastruktur für Stammdaten - Systemadministration - Vergabe und Prüfung Zugriffsrechte • Beide Funktionen führen dazu, dass ein Entwickler Berechtigungen für die NOVA Pflegeinfrastruktur, mithilfe derer die finanzrelevanten Stammdaten von NOVA Anbieter mutiert werden, entwickeln und selbstständig vergeben könnte • Dies stellt einen Verstoss gegen das 4-Augen-Prinzip dar • Risiko besteht in einer Brutto-Sicht • Folge: ein Entwickler könnte anderen die Mutation von finanzrelevanten Stammdaten von NOVA Anbieter ermöglichen (die beispielsweise gleichzeitig über Berechtigungen für den Transport verfügen). Dadurch könnten die Finanzflüsse beeinflusst werden.
K09: Fachprüfung NOVA Anbieter - Entwicklung & Datenpflege für NOVA-Komponenten ohne Finanzrelevanz • Beide Funktionen führen dazu, dass ein Entwickler oder Datenmanager seine eigenen Softwareanpassungen bzw. Datenmutationen fachprüfen kann • Dies stellt einen Verstoss gegen das 4-Augen-Prinzip dar • Risiko besteht in einer Brutto-Sicht • Folge: nicht durch 4-Augenkontrolle geprüfte Änderungen können in produktiven Software-Versionen oder Stammdaten enthalten sein. Dies hat jedoch für diese Komponenten keinen Einfluss auf die Finanzflüsse von NOVA Anbieter.	K10: Transportwesen - Entwicklung & Datenpflege für NOVA-Komponenten ohne Finanzrelevanz • Beide Funktionen führen dazu, dass ein Entwickler oder Datenmanager seine eigenen Software-Änderungen oder Datenmutationen eigenständig in Produktion transportieren kann. Dadurch kann die Fachprüfung umgangen werden. • Dies stellt einen Verstoss gegen das 4-Augen-Prinzip dar • Risiko besteht in einer Brutto-Sicht • Folge: ungeprüfte Änderungen können in produktiven, finanzrelevanten Software-Versionen oder Stammdaten enthalten sein. Diese Änderungen haben in diesem Szenario keine Auswirkungen auf die Finanzflüsse.
K11: Systemadministration - Vergabe und Prüfung Zugriffsrechte - Entwicklung & Datenpflege für NOVA-Komponenten ohne Finanzrelevanz • Beide Funktionen führen dazu, dass ein Entwickler oder Datenmanager seine eigenen Software-Änderungen oder Datenmutationen eigenständig in Produktion transportieren kann. Dadurch kann die Fachprüfung umgangen werden. • Dies stellt einen Verstoss gegen das 4-Augen-Prinzip dar • Risiko besteht in einer Brutto-Sicht • Folge: ungeprüfte Änderungen können in produktiven, finanzrelevanten Software-Versionen oder Stammdaten enthalten sein. Diese Änderungen haben in diesem Szenario keine Auswirkungen auf die Finanzflüsse.	