



**BankingGuide**  
GmbH

# IT-Sicherheitskonzept

VR Payment-Leistungspaket



## Inhalt

1	Übersicht.....	1
2	Systemarchitektur.....	2
2.1	Frontend.....	3
2.2	Backend.....	3
2.3	Bausteinsicht.....	3
3	Glossar.....	4
4	Sicherheitsmaßnahmen .....	5
5	Anwendungsbetreuung .....	6
6	Abkürzungen, Begriffe und Definitionen .....	7

# 1 Übersicht

Der (Kundenselbst-)Beratungsanwendungen und Antragsstrecken des VR Payment-Leistungspakets unterstützen die Bank beim omnikanischen Vertrieb und Abschluss von VR Payment-Lösungen.

Weitere Informationen zu den Lösungen finden Sie in der in der Anwenderdokumentation „Self-Services für Firmenkunden mit BankingGuide Express“ im ATRUVIA Hub.

## 2 Systemarchitektur

### Kontextabgrenzung

Der Kontext ergibt sich aus dem Betrieb der Anwendungen im Online-Banking sowie dem Banking-Workspace. Die genannten Anwendungen bieten als Plattform Services Schnittstellen in das Kernbankverfahren und zu anderen Anwendungen auf der Plattform. Die Nutzung der Anwendungen auf der Homepage (#webbank) erfolgen per iFrame-Einbindung.

Zu den Services zählt neben dem Betrieb eine zentrale Benutzerverwaltung mit Rechtemanagement. Auf der Plattform kann die Multimandantenfähigkeit über ein Framework und die Datenbanken der Plattform abgebildet werden.

### Fachlicher Kontext

Anzubindende Schnittstellen:

Kommunikationsbeziehung	Eingabe	Ausgabe
Benutzerverwaltung	x	
Schnittstelle Kunde	x	
Schnittstelle Konto	x	
Schnittstelle Mandanten	x	
Schnittstelle VR Payment		x

### Technischer Kontext

Anbindung an die Schnittstellen der Omnikanalplattform.

Um die Multimandantenfähigkeit der Omnikanalplattform in Richtung der Datenbank zu integrieren, wird das Atruvia AG Framework (SPIN Plugin) verwendet.

Weitere Services der Omnikanalplattform:

- CAS für Berater - User, Login, Rechte
- CAS für Kunden - User, Login, Rechte
- Mandanteninformationen (Bank)

### Technische Grenzen

Mit der Architektur wird es für alle Mandanten immer dieselbe Version geben und für einzelne Mandanten keine Sonderwünsche umsetzbar sein.

### Technologien

Liste der in der Anwendung verwendeter Technologien.

- Java 11 mit Sprint Boot
- Angular 8
- Oracle Datenbankserver
- Laufzeitumgebung: Docker Container

## Datenhaltung

Die Datenhaltung innerhalb der o.g. Plattformen erfolgt im Oracle Datenbank-Cluster. Jede Backend-Anwendung erhält ein Schema, in dem alle Daten aller Mandanten liegen, für die Unterscheidung wird ein Discriminator (RZBK) in den Tabellen verwendet.

## 2.1 Frontend

Die Anwendung besteht aus den folgenden Frontend-Anwendungen, welche als Angular SubPath Apps und WebComponents in die Plattformen integriert sind.

- (Kundenselbst-)Beratungsanwendung
  - Analyse
  - Bestellprozess
  - Optimiert für das iPad Pro und Windows-Convertibles
  - Aufruf in einem separaten Tab
- Konfigurator
  - Bearbeiten und Individualisierung des Inhalts der Anwendung
  - Verwaltung von Instanzen und Usern
  - Aufruf in einem separaten Tab

## Akteure

Übersicht über die Akteure, welche mit der Anwendung interagieren.

- (Kundenselbst-)Beratungsanwendung
  - Homepage & Online-Banking
    - Bank-Kunde
  - BankingWorkspace
    - Bank-Mitarbeiter
- Konfigurator (nur BankingWorkspace)
  - Bank-Mitarbeiter

## 2.2 Backend

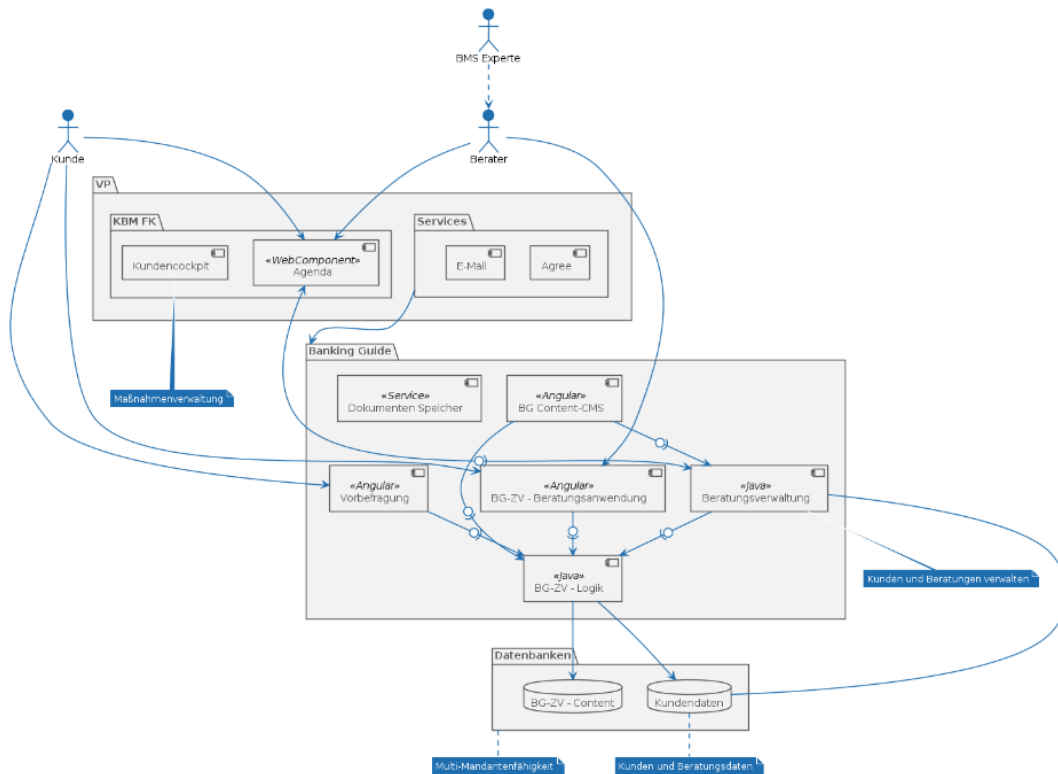
Java Backend Anwendungen:

- (Kundenselbst-)Beratungsanwendung
  - Anwendung mit der Businesslogik für die Beratung
  - Die Inhalte können durch den Mandaten über den Konfigurator individualisiert werden
  - Multi-Instanz fähige Anwendung
- Konfigurator (nur BankingWorkspace)
  - Verwaltung von BankingGuide Anwendungen und deren Instanzen
  - Zentrale Speicherung und von Kundendaten und durchgeführten Beratungen, auf diese greifen alle BankingGuide Anwendungen zu

## 2.3 Bausteinsicht

### Whitebox-Gesamtsystem

Übersicht über das Gesamtsystem auf Ebene der Bausteine mit Akteuren und Schnittstellen.

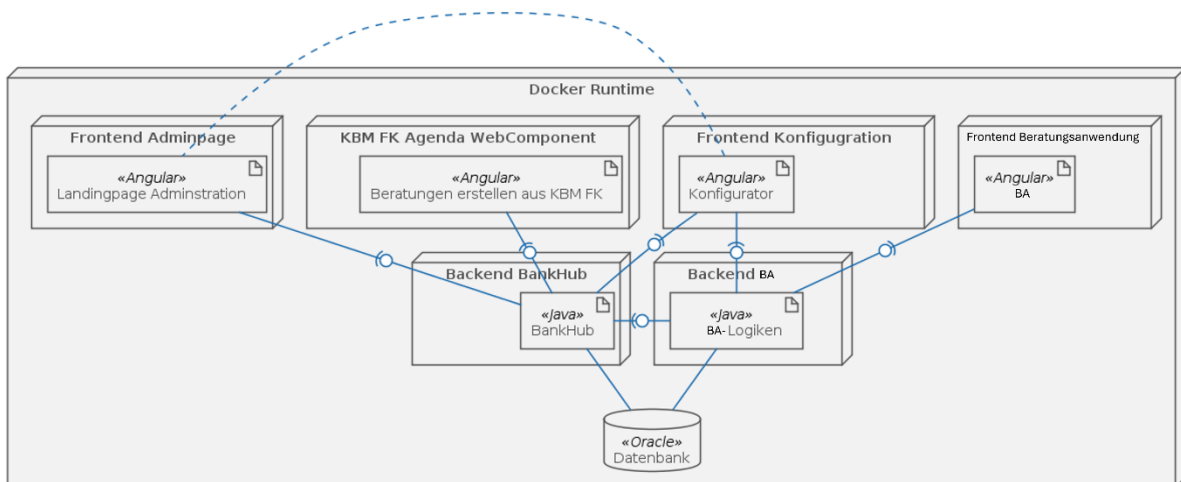


### Verteilungssicht

Deployment-Diagramm auf Basis von Containern.

Jedes Frontend einer Abschlussstrecke wird in einem einzelnen Container betrieben.

BA = Beratungsanwendung



## 3 Glossar

Begriff	Definition
BA	Beratungsanwendung
Mandant	Ein Kunde der eine BA kauft, dies sind die einzelnen VR Banken

<i>Content</i>	Produkte, Fragen, Lösungen etc. Daten des Systems
<i>OKP</i>	Omnikanalplattform der Atruvia AG
<i>Instanz</i>	Eine lauffähige Instanz der Anwendung.

## 4 Sicherheitsmaßnahmen

Die Beratungsanwendungen des Leistungspakets werden, wie beschrieben, im Online-Banking bzw. BankingWorkspace von ATRUVIA betrieben. Wesentliche Teile der Sicherheitsmaßnahmen sind daher über die allgemeinen Sicherheitsmaßnahmen der genannten Plattformen abgebildet.

Den Link zu den aktuellen Sicherheitsmaßnahmen, Sicherheitskonzept Services von ATRUVIA, finden Sie hier (im Netz von ATRUVIA aufrufbar):

<https://securityportal.rz.bankenit.de/ism.html>

Über die IT-Sicherheitsmaßnahmen, welche die Anwendungen des Leistungspakets seitens der Plattformen nutzen, wurden hinsichtlich der Schutzanforderungen nachfolgende, Paket-spezifischen, Sicherheitsmaßnahmen umgesetzt:

### Verfügbarkeit

Die Verfügbarkeit der Anwendungen stehen in einem unmittelbaren Zusammenhang mit der Verfügbarkeit des Online-Bankings bzw. des BankingWorkspace, welche in den oben verlinkten Sicherheitskonzepten geregelt ist.

Darüber hinaus wurde für die Anwendungen des Leistungs-Pakets ein Systemmonitoring implementiert, welches die Verfügbarkeit sowie die Performance der Anwendungen stetig überwacht. Im Falle von Problemen mit der Anwendung besteht so die Möglichkeit rechtzeitig einzugreifen. Sollte es dennoch zu einem unerwarteten Systemabsturz kommen, steht das Supportteam des BankingGuide von Mo-Fr. in den Kernarbeitszeiten von 8-18 Uhr in Kontakt mit der Systemadministration der Omnikanalplattform. Hierüber wird gewährleistet, dass ein Neustart des BankingGuide innerhalb von 2 Stunden erfolgen kann.

Hinsichtlich der technischen Entwicklung der Anwendung sind die Systemumgebungen strikt voneinander getrennt. Neben der Produktivumgebung, auf welcher die Bank arbeitet, existieren sowohl eine Entwicklungs- auch als eine Testumgebung. Entwicklungs- oder testbedingte Systemfraktionen in der Produktivumgebung werden hierdurch ausgeschlossen. Ebenfalls werden Systemupdates in der Entwicklungs- und Testumgebung ausgiebig getestet bevor diese in die Produktivumgebung überführt werden um eine stabile Produktivversion zu gewährleisten.

## Integrität

Hinsichtlich des Schutzziels der Integrität – Korrektheit der Daten und korrekte Funktionsweise des Systems – durchläuft der BankingGuide im Entwicklungsprozess folgende Teststufen:

1. Technische Entwicklungsphase: Schwerpunktmäßig technische Tests durch automatisierte Testvorgänge und dedizierte Tester im Entwicklungsteam
2. Fachliche Entwicklungsphase: Verprobung des MasterContents durch dedizierte Tester und Pilotbanken
3. Publication: Verprobung jedes Updates im Rahmen der Publication im Rahmen einer 14-tägigen Testphase durch die OKP-Pilotbanken welche den BankingGuide lizenziert haben

Die Volksbank Raiffeisenbank hat darüber hinaus die Möglichkeit die fachliche Konfiguration des BankingGuide zu individualisieren. Diese Funktionalität ist jedoch nur einem definierten Admin-Benutzerkreis gestattet, welcher über BAP-Kompetenzen / Funktions-IDs berechtigt wird.

## Vertraulichkeit

Die Daten im BankingGuide unterliegen dem Datenschutz und sind nur für den berechtigten Personenkreis verfügbar. Hinsichtlich der Einrichtung und Konfiguration des BankingGuide sind definierte BAP-Kompetenzen / Funktions-IDs notwendig (siehe Leitfaden Grundlagen OKP).

Zur Sicherstellung der technischen Vertraulichkeitsanforderungen werden im Wesentlichen die Verschlüsselungs- und Rechtekonzepte der Omnikanalplattform in Anspruch genommen. Mitarbeiter der BankingGuide GmbH haben keinen Zugriff auf die Anwendung BankingGuide. Die einzige Ausnahme stellt die Fernwartung über das Banksystem dar, für welche eine gesonderte AV-Vereinbarung mit der BankingGuide GmbH getroffen wird.

## Authentizität

Der BankingGuide übernimmt in der Beratungsanwendung die User-Token der Omnikanalplattform. Diese Usertoken differenzieren den Anwender in Berater und Kunde. Das Rollen-Rechte-Konzept innerhalb des BankingGuide differenziert diese Rollen-Rechte ebenfalls. Eine ergänzende Konfiguration durch die Bank oder separate Anmeldungen sind daher nicht notwendig.

## 5 Anwendungsbetreuung

Für die Anwendung stehen durch die BankingGuide GmbH zum Anwendungsbetrieb fachliche und technische Ansprechpartner zur Verfügung. Diese Ansprechpartner sind primär erreichbar über das Ticketsystem der Atruvia AG, in Ausnahmefällen ebenfalls unter [support@bankingguide.de](mailto:support@bankingguide.de) zentral erreichbar.



## 6 Abkürzungen, Begriffe und Definitionen

Verfügbarkeit	Verfügbarkeit bedeutet, dass die Daten im erforderlichen Zeitraum zur Verfügung stehen.
Vertraulichkeit	Vertraulichkeit verlangt, dass Daten nicht unberechtigt weitergegeben oder veröffentlicht werden.
Integrität	Integrität von IT-Systemen ist gegeben, wenn die Daten vollständig und richtig zur Verfügung stehen und vor Manipulation und ungewollten oder fehlerhaften Änderungen geschützt sind.
Authentizität	Authentizität ist gegeben, wenn ein Geschäftsvorfall einem Verursacher eindeutig zuzuordnen ist.

