

## **1. Methodischer Rahmen:**

Die Lösungsentwicklung folgt einem klaren Vorgehen: Problemerkennung → Lösungsentwurf → Auswahl → Umsetzung. Dieses Vorgehen ist wichtig, weil es zeigt, dass wir die Lösung nicht „aus dem Bauch“ entwickelt, sondern systematisch aus Symptomen, Ursachen und Zielen abgeleitet haben

## **2. Problemerkennung: Symptome, Messgrößen und Ursachen als Ausgangspunkt**

Im aktuellen Ablauf wirkt der Einlass wie eine Kette: Ankommen auf dem Campus, Check-in am Eingang, Intranet-Abgleich, Rückfrage beim Unternehmen, manuelle Ausweisprüfung und dann Wartezeit. Diese Abfolge zeigt, wieso es zu Verzögerungen kommt: Jeder Medienbruch kostet Zeit, und bei vielen Abläufen summiert sich das zu Stau. Die Problemlage wurde anhand konkreter Messdaten festgemacht (z. B. 10 Minuten Wartezeit, Voranmeldequote rund 30 %, Ladezeit ca. 6 Sekunden, hoher Anteil manueller Ausweisprüfungen). Bei der Ursachenanalyse tauchen wiederkehrende Punkte auf: veraltetes Intranet, analoge Voranmeldung, manuelle Ausweisprüfung, fehlende Liefersteuerung, keine klare Fahrzeugübersicht, Walk-ins, Medienbrüche, fehlende zentrale Datengrundlage, Zeitdruck und fehlende Vorabinfos.

## **3. Lösungsentwurf: Zielbild und Leitentscheidungen**

Aus den Ursachen ergibt sich ein klares Ziel: weniger Stau, kürzere Wartezeiten am Gate, mehr Sicherheit durch transparente Abläufe und weniger manuelle Fehler. Dazu kommt ein besseres Nutzererlebnis, mehr Durchblick bei Besucher- und Lieferströmen und insgesamt mehr Klarheit im Prozess. Um dieses Ziel zu erreichen, wurden im Entwurf einige zentrale Leitentscheidungen getroffen: eine zentrale Datenbasis statt Insellösungen, rollenbasierte Ansichten damit Security wirklich zügig arbeiten kann, eine definierte Statuslogik („in Prüfung“ zu „bestätigt“) und ein kontrollierter Umgang mit Ausnahmefällen Quick Booking statt informellem Durchwinken.

## **4. Alternativen und warum sie verworfen wurden**

**Alternative A:** Reines Quick-Booking ohne Anmeldung. Kurzfristig günstiger, weil weniger Freigabe-Logik und weniger Nutzer-Administration nötig wären. Fachlich würde diese Lösung aber das Grundproblem nicht lösen: Gate-Entscheidungen bleiben spontan, Planbarkeit ist gering, und Sicherheit lässt sich schwer nachweisen, weil Freigaben, Status und Audit nicht durchgängig erfasst sind. Genau die Engpässe (Rückfragen, Zeitdruck, manuelle Prüfungen) würden nur digital „verpackt“, aber nicht dauerhaft reduziert.

**Alternative B:** Nur Besucher/Lieferanten digitalisieren, Mitarbeitende/Security aus dem System raus. Dieses Vorgehen wirkt zwar klar, verschiebt das Problem in der Praxis aber nur: Security bleibt ohne Live-Status, ohne Scan-Screen und ohne klare Systementscheidung. Rückfragen, Medienbrüche und Zeitdruck bleiben bestehen, genau die Ursachen, die erkannt wurden.

**Alternative C:** Reine Public-Cloud ohne Hybrid-Absicherung. Oft leichter zu betreiben und gut skalierbar. Gleichzeitig wird die Internetabhängigkeit als kritisches Risiko genannt: Ohne stabile Verbindung könnte der Einlass ausfallen. Für einen Standortbetrieb ist dieses Risiko besonders teuer (Betriebsunterbrechung am Gate). Deshalb fiel die Entscheidung zugunsten von Hybrid als bewusstes Risikomanagement.

## **5. Kostenlogik (TCS):**

Bei der Wahl geht es nicht nur um Entwicklungskosten. Es zählt für uns der langfristige Gesamteffekt: Gate-Minuten sind teuer, weil Wartezeiten Staus erzeugen und Folgeprobleme nach sich ziehen (Verspätungen, Unzufriedenheit, mehr Personalaufwand, gestörte Abläufe). Daher können Minimalvarianten trotz niedriger Anfangskosten auf Dauer teurer sein, wenn sie die Prozesszeit nicht merklich senken. Umgekehrt kann eine zu starke Private-Only-Lösung überdimensioniert sein: Hohe Anschaffungs- und Betriebsaufwand, obwohl Teile der Vorteile (Skalierung, Self-Service) in der Cloud effizienter erreichbar wären. Diese Überlegung erklärt, warum wir eine ganzheitliche, organisatorisch

durchgängige Lösung gewählt haben, die technisch skalierbar und gleichzeitig robust ist, idealerweise im Hybrid-Modell.

## **6. Einfluss des Interviews auf die Entscheidung**

Für die Weiterentwicklung haben wir zusätzlich ein Interview geführt, um externe Perspektiven einzubringen. Interviewpartner war Arif Ulu, Mathe- und Politiklehrer am Hermann-Ehlers-Gymnasium in Berlin (das komplette Gespräch findet sich in Dokument: 26012026 TeamNr. 3 WiSe2526 Interview.pdf). Das Gespräch hat drei klare Design-Punkte gestärkt:

**Erstens:** Externe Nutzer brauchen vor allem einen reibungslosen Ablauf auch ohne Installationshürden, daher zählt Web/App-ähnlicher Zugriff als Standard.

**Zweitens:** Das Suchen nach E-Mails oder Papiernachweisen am Eingang führt realistisch zu Verzögerungen; deshalb gewinnt das Wallet/QR-Verfahren als Standard deutlich an Bedeutung.

**Drittens:** Die Akzeptanz hängt stark von Datenminimierung und Transparenz ab. Deshalb wurden Statuslogik, klare Rollenrechte und definierte Aufbewahrungs- bzw. Löschfristen als Teil der Lösung mitgedacht, damit Datenschutzfragen nicht erst später auftauchen. Diese Ansätze passen direkt zu unserer endgültigen Systemlogik (QR erst nach Freigabe, RBAC, Chat/Hilfe zur Reduktion von Rückfragen).

## **7. Ergebnis: Warum genau dieser Lösungsweg gewählt wurde**

Die finale Entscheidung fällt auf TCS als durchgängiges Besucher- und Liefermanagement mit zentraler Datenbasis, Statusworkflow, QR-Code, Security-Scan-Screen, Timeslots/Zonensteuerung und kontrollierten Ausnahmefällen. Diese Kombination ist gewählt, weil sie nicht nur Symptome „beschleunigt“, sondern Ursachen strukturell reduziert: Planbarkeit entsteht vor Ankunft, Gate-Arbeit wird zur Validierung statt zur Klärung, Lieferverkehr wird zeitlich/örtlich gesteuert, und Transparenz entsteht in Echtzeit.