# **1. Introduction**

Resolving parking congestion, transportation inefficiencies, and commuting difficulties on university campuses is the goal of the Campus Ride-Sharing Platform with Parking System Integration. With digital ID verification for safe access and integration with parking availability data, the system enables staff and students to share rides in real time. The interactions, system boundaries, and external entities that influence the platform's operational environment are listed in this paper.

# **2. Step 1 - Identification of Potential Relevant Requirements Sources**

## 2.1 Context Objects Checklist

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Description | Role |
| Student | User | Students who use the platform to offer or request rides within campus. | Primary users; interact via mobile/web app |
| University Admin | User | University staff using the platform for commuting or parking information. | Secondary users |
| Campus Parking System | System | IoT-based system providing real-time parking lot availability data. | Supplies parking status to the platform |
| University Digital ID System | System | Identity verification system using student/staff digital credentials. | Authenticates users during registration |
| Security Personnel | User | |  | | --- | |  |  |  | | --- | | Campus authorities managing user verification and safety protocols. | | Monitor and approve new user access |
| Admin Interface | Interface | Management dashboard for system administrators. | Manage users, reports, and system settings |

## 2.1 Requirements Sources

|  |  |  |
| --- | --- | --- |
| **Requirements Sources** | **Type** | **Justification** |
| **Student** | Stakeholder | Direct stakeholders who define usability, security, and feature expectations |
| **University Admin** | Stakeholder | Define policy constraints, approve access control mechanisms |
| **Campus Parking System** | Existing System | Provides information about parking integration and APIs |
| **Digital ID System** | Existing System | Define technical constraints for integration (API, authentication) |
| **Security Personnel** | Stakeholder | Help define safety procedures, protocols, and emergency features |
| **System Documentation** | Document | Includes API manuals, compliance guidelines, and integration standards. |

# 3. Step 2 – Selection of Most Relevant Requirements Sources

## 3.1 Prioritization via 100 Dollar Test

A stakeholder workshop allocated a hypothetical $100 budget to rank requirements sources by relevance:

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirements Source** | **Allocated Budget ($)** | **Priority** | **Rationale** |
| **Students** | 35 | High | Direct end-users; critical for usability and adoption. |
| **University Admin** | 30 | High | Govern system policies and data access permissions. |
| **Campus Parking System** | 15 | Medium | Core technical dependency for parking integration. |
| **Digital ID System** | 10 | Medium | Essential for secure authentication but less dynamic than other sources. |
| **Security Personnel** | 7 | Low | Important for safety protocols but limited to edge cases. |
| **System Documentation** | 3 | Low | Supportive but secondary to stakeholder input. |

## 3.2 Final Selection

Primary Sources for Initial Elicitation:

* Students
* University Admin
* Campus Parking System

Secondary Sources for Later Phases:

* Digital ID System (validated during technical design)
* Security Personnel (consulted during risk assessment)

# 4. Conclusion

Through the methodical identification and prioritization of requirements sources, this procedure guarantees that the platform meets important technical, policy, and user needs. While secondary sources will subsequently improve safety and compliance, the priority sources will direct the first elicitation efforts.