TU Wien – Institut für Computertechnik

Projekttitel

Software Requirements Specification (SRS)

Gruppe	Autor(en)	MatrikelNr.
TRAD Gruppe X	NACHNAME Vorname	XXXXXXXX
	NACHNAME Vorname	XXXXXXXX
Ausgabe-Datum: 21.1.2021		Version: 2.5

0 INHALTSVERZEICHNIS

0.1 Versions-Historie

Version	Datum	Grund der Erstellung/Änderung
1.0	2020-11-20	Erstellen des Dokuments
1.1	2020-11-22	Hinzufügen der Use-Cases
1.2	2020-11-29	Review der Use-Cases
1.3	2020-12-03	Hinzufügen des Domänenmodells
1.4	2020-12-05	Hinzufügen der Kapitel 3.5, 4, 5 und 6
1.5	2020-12-06	Review des gesamten Dokuments
1.6	2020-12-13	Letzte Änderungen für die Zwischenabgabe
2.0	2020-12-19	Erweitern des Use-Case-Diagramms und der Sequenzdiagramme um den Akteur „Hardware“
2.1	2020-12-20	Einzeichnen der Systemgrenzen, im Domänenmodell
2.2	2020-12-21	Überarbeiten der funktionalen Anforderungen, der Use-Cases
2.3	2021-01-08	Review des gesamten Dokuments für die Endabgabe
2.4	2021-01-10	Letzte Änderungen für die Endabgabe
2.5	2021-01-16	Aktualisierung der Sequenzdiagramme

Tabelle 1: Versions-Historie

1 EINLEITUNG

Der Auftraggeber, im folgenden auch „Kunde“ genannt, ist ein Hersteller von Safes. In der Vergangenheit wurden wiederholt Beeinträchtigungen der Sicherheit des Systems gemeldet, die darauf zurückzuführen waren, dass der Schlüssel in unmittelbarer Nähe zum Safe gelagert wurde.
Durch die Umstellung des Verriegelungsmechanismus von traditionellen Schlüsseln auf RFID-Karten soll die Sicherheit des Systems gesteigert werden. Das Ziel ist, durch die Entriegelung per RFID-Karte, die Usability für den Endkunden zu verbessern. Dadurch soll die Anzahl der Fälle, in denen der Schlüssel in der Nähe des Safes gelagert wird, verringert werden.
Zusätzlich wird die Kontrolle für den Endkunden, durch diverse zusätzliche Funktionalitäten, wie einem eigenen Benutzer-Management System sowie einem Logging-Service, gesteigert.

Bei der Umsetzung ist besonders auf die Integrität des Systems zu achten.

Dieses Dokument befasst sich mit der allgemeinen Beschreibung des Auftrags und der Definition der konkreten Anforderungen an die zu entwickelnde Lösung. Weiters werden die Rahmenbedingungen für den Entwicklungsprozess bestimmt und ein Überblick über den Einsatz der Lösung, in der definierten Domäne, gegeben.

2 ALLGEMEINE BESCHREIBUNG DER AUFGABE

Der Entriegelungsmechanismus, des vom Kunden hergestellten Safes, soll von traditionellen Schlüsseln auf RFID-Karten umgestellt werden.

2.1 Übersicht der Problemstellung

Um die Umstellung des Entriegelungsmechanismus zu ermöglichen, muss eine eigens dafür optimierte Lösung entwickelt werden, die die durch das Entschlüsselungsmedium „Schlüssel“ gewährleistete Sicherheit beibehält, beziehungsweise verbessert. Weiters soll die Kontrolle über die Zutritte zum Safe, durch einige weitere Funktionalitäten erhöht werden.

2.2 Zweck der Software

Die zu entwickelnde Lösung soll die bisherige Entriegelung des Safes, per Schlüssel, ersetzen. Zusätzlich soll der Safe durch die Software überwacht werden. Die Überwachung erfolgt durch ein Logging-Service, das alle Zutrittsversuche der letzten Wochen aufzeichnet. Weiters soll es Systemadministratoren möglich sein, neue Benutzer anzulegen und bestehende Benutzer zu ändern, sowie den Zutrittscode zu ändern.
Das Aktivieren beziehungsweise Deaktivieren der elektronischen Verriegelung durch einen Systemadministrator soll jederzeit möglich sein.

Der Zutritt sowie das Abfragen beziehungsweise Ändern von Daten soll unautorisierten Benutzern unter keinen Umständen möglich sein.

Bei der zu entwickelnden Lösung handelt es sich um eine reine Software-Lösung.

2.3 Externe Beziehungen der Software

Um den bestmöglichen Einsatz der Software zu ermöglichen, wird von Seiten des Auftragnehmers die konkrete, vom Kunden einzusetzende, Hardware spezifiziert.
Die Ansteuerung der Hardware erfolgt über eine Hardware Abstraction Layer.

Von Seiten des Auftragnehmers wird folgende Hardware, für den Einsatz in Kombination mit „Safe RFID“, empfohlen:

- Ein Safe mit einer Safe-Türe, die elektronisch entriegelt und verriegelt werden kann.
- Ein integrierter Rechner, auf dem „Safe RFID“ ausgeführt werden kann. „Safe RFID“ wird in der Programmiersprache Java entwickelt. Die Hardware-Anforderungen des Rechners können daher den Anforderungen für Java JRE entnommen werden.
- Das Eingabepanel ist ein Touchscreen mit einer Bildschirmdiagonale von mindestens 8 Zoll. Es soll auf der Vorderseite des Safes montiert werden.
- Eine eingebaute unterbrechungsfreie Stromversorgung (USV), die im Falle eines Ausfalls der Stromversorgung das Zurücksetzen des Safes in den Werkszustand ermöglicht.
- Ein RFID-Lesegerät, das auf der Vorderseite des Safes verbaut wird.
- Fünf RGB LEDs, die auf der oberen Kante, der Vorderseite, verbaut werden.
- Ein Lautsprecher, der im Safe verbaut wird.
- Ein Sensor, der den aktuellen Zustand der Safe-Türe (offen / geschlossen) überwacht.
- Bei begehbaren Safes muss ein Notfall-Taster im Safe verbaut werden.

Zur Speicherung der Daten wird ein Datenbankmanagementsystem genutzt. Der Auftragnehmer ist zur Definition einer empfohlenen Konfiguration dessen, verpflichtet.

2.4 Einschränkungen und Nebenbedingungen

Die Entwicklung der Lösung erfolgt im Rahmen eines iterativ/inkrementellen Entwicklungs-Prozesses, bestehend aus mindestens zwei Iterationen. Der Abschluss einer jeweiligen Iteration wird durch einen Abstimmungs-Termin zwischen Auftraggeber und Auftragnehmer gekennzeichnet, bei dem Fragen geklärt beziehungsweise Feedback zur Umsetzung eingeholt wird. Im Laufe dieses Abstimmungs-Termins werden Punkte identifiziert, die im folgenden Inkrement berücksichtigt werden sollen.

Zu Beginn des Projektes werden von Seiten des Auftraggebers sowie von Seiten des Auftragnehmers jeweils eine Schlüsselperson definiert, die den Ablauf des Projektes aus der Sicht der jeweiligen Partei koordiniert und für eventuelle Fragen von Seiten des Vertragspartners zur Verfügung steht.

Die erste Entwicklungs-Phase findet vom 17.11.2020 bis zum 13.12.2020 statt. Der geplante Abstimmungs-Termin zwischen Auftragnehmer und Auftraggeber findet am 15.12.2020 um 14:00 Uhr statt. Das Ziel für die erste Entwicklungs-Phase ist die Fertigstellung der Software Requirements Specification (SRS).
Die zweite Entwicklungs-Phase findet vom 15.12.2020 bis zum 21.01.2021 statt und hat als Ziel die Fertigstellung der Software Design Description (SDD) und die Umsetzung des Feedbacks aus der ersten Entwicklungs-Phase.

Nach dem erfolgreichen Abschluss der zweiten Entwicklungs-Phase erfolgt die Übergabe der Software an den Auftraggeber. Die Übergabe erfolgt im Rahmen eines Einschulungs-Termins zwischen dem Auftraggeber und dem Auftragnehmer, bei dem der Quellcode sowie die Projekt-Dokumentation an den Auftraggeber übergeben werden.
Ein Nachweis über die Erfüllung der definierten Akzeptanzkriterien, ist in der Projekt-Dokumentation inbegriffen. Dieser besteht aus den Ergebnissen automatisierter Tests, die das System auf die Umsetzung der funktionalen Anforderungen prüfen.

Der Auftraggeber verpflichtet sich an den Abstimmungs-Terminen sowie dem Übergabe-Termin in Form von, entsprechend technisch geschulten und mit dem Projekt vertrauten Mitarbeitern, vertreten zu sein.

Die Umsetzung, der zu entwickelnden Lösung, erfolgt in der Programmiersprache Java.
Als Datenbankmanagementsystem kommt PostgreSQL zum Einsatz.

Gemäß dem österreichischen Verbraucherschutz verpflichtet sich der Auftragnehmer zu einer dreijährigen Gewährleistungs-Phase.
Der Auftragnehmer haftet für keinerlei Sicherheitsverstöße, die aufgrund fehlerhafter Bedienung oder auf, von der empfohlenen Hardware, abweichenden Systemen auftreten.

Der Auftraggeber ist, nach der erfolgten Übergabe, für die Wartung der Software verantwortlich.

Die Kalkulation der Kosten erfolgt nach Aufwand und basiert auf einem Stundensatz von 105€/Stunde. Die Abrechnung erfolgt nach der Übergabe.

3 AUSFÜHRLICHE BESCHREIBUNG DER ANFORDERUNGEN

Im folgenden Teil werden die Anforderungen, an die Umsetzung des Auftragnehmers, spezifiziert. Der erfolgreiche Abschluss des Projekts ist nur nach der Erfüllung aller spezifizierter Anforderungen möglich.

3.1 UML Use-Case-Diagramm

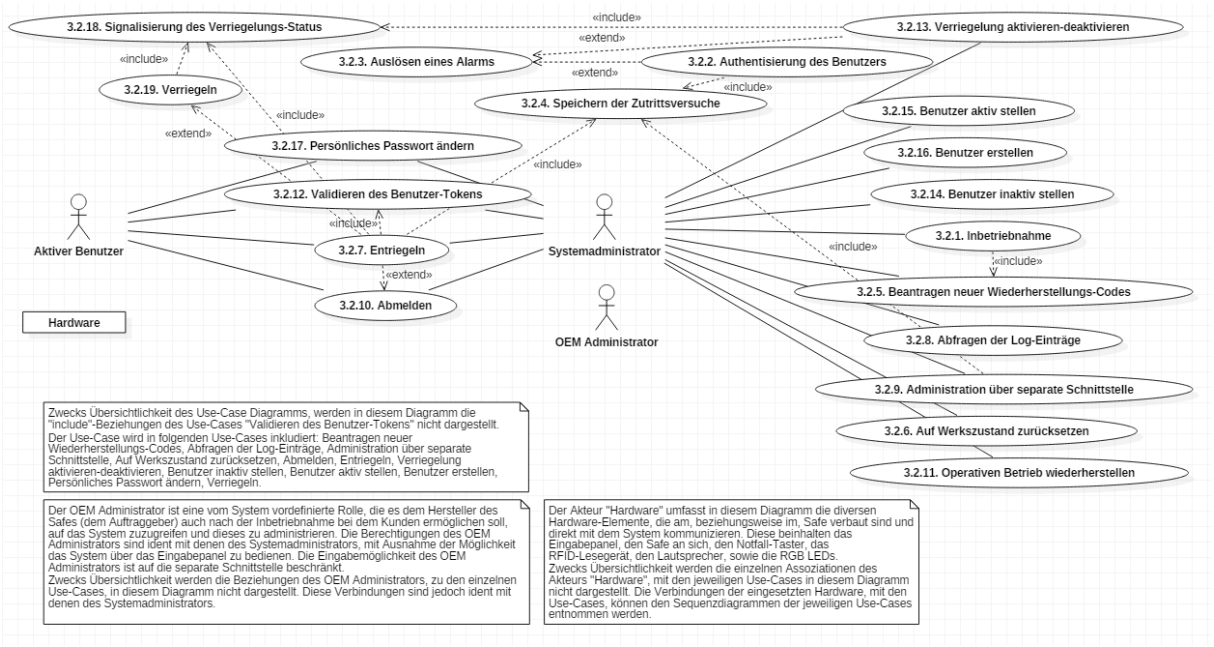

Abbildung 3-1: Use-Case-Diagramm

Im Use-Case-Diagramm sind alle Relationen, zwischen den einzelnen Use-Cases abgebildet. Eine Ausnahme bilden die Include-Beziehungen zwischen dem Use-Case „Validieren des Benutzer-Tokens“ und weiteren Use-Cases, da diese die Übersichtlichkeit des Diagramms beeinträchtigen würden.
Folgende Use-Cases inkludieren den Use-Case „Validieren des Benutzer-Tokens“:
Beantragen neuer Wiederherstellungs-Codes, Abfragen der Log-Einträge, Administration über separate Schnittstelle, Auf Werkszustand zurücksetzen, Abmelden, Entriegeln, Verriegelung aktivieren-deaktivieren, Benutzer inaktiv stellen, Benutzer aktiv stellen, Benutzer erstellen, Persönliches Passwort ändern, Verriegeln.
Weiters werden die Verbindungen von den Use-Cases zum Akteur Hardware, der als Zusammenfassung aller Komponenten die mit der Software interagieren zu sehen ist, aus Übersichtlichkeitsgründen nicht dargestellt.
Ebenso werden die Verbindungen der Use-Cases zum OEM Administrator nicht visualisiert um die Übersichtlichkeit nicht zu beeinträchtigen. Der OEM Administrator weist dieselben Berechtigungen auf wie ein Systemadministrator, jedoch kann dieser den Safe nicht mittels Touchscreen bedienen, sondern über die separate Schnittstelle. Daraus ergeben sich idente Verbindungen zu den Use-Cases.

3.2 Use Case Reports

3.2.1 INBETRIEBNAHME

Die Inbetriebnahme beschreibt den erstmaligen Start der Software, bei dem Endkunden. Bei der Inbetriebnahme werden die Sicherheitsrichtlinien für die Operation des Safes definiert.

Vorbedingungen: Der Safe muss beim Endkunden, an seiner endgültigen Position, installiert worden sein. Die Stromversorgung des Safes, inklusive aller Komponenten, muss vorbereitet worden sein. Die Inbetriebnahme muss von einem Systemadministrator durchgeführt werden.

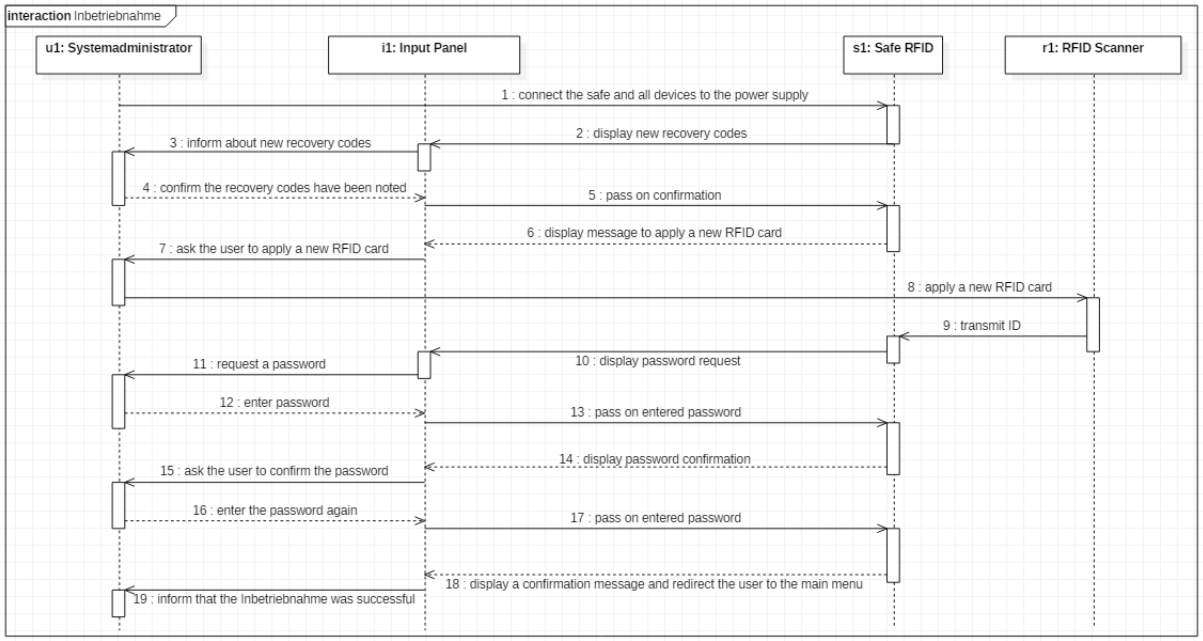

Abbildung 3-2: Sequenzdiagramm "Inbetriebnahme"

Normaler Ablauf: Ein Systemadministrator schließt den Safe an die Stromversorgung an. Beim erstmaligen Start der Software werden dem Benutzer auf dem Bedienfeld acht (8) zufällig generierte Wiederherstellungs-Codes angezeigt. Diese müssen vom Benutzer notiert werden. Nachdem der Benutzer bestätigt, dass die Wiederherstellungs-Codes notiert wurden, wird dieser aufgefordert einen Systemadministrator-Account zu erstellen.

Alternative Abläufe: Im Rahmen der Erstellung des Systemadministrator-Accounts, wird der Benutzer zur Eingabe eines persönlichen Passwortes aufgefordert. Entspricht dieses nicht den Vorgaben, muss ein anderes Passwort gewählt werden.

Nachbedingungen: Nach der erfolgreichen Inbetriebnahme geht der Safe in den operativen Betrieb über. In diesem Modus muss die Stromversorgung permanent gegeben sein.
Initial wird der Safe mit den Werkseinstellungen betrieben. Weitere Accounts können über das Eingabepanel und die REST-Schnittstelle angelegt werden.

Ziele: Nach der erfolgreichen Inbetriebnahme des Safes befindet sich dieser im operativen Betrieb und kann von allen aktiven Benutzern bedient werden.

Includes: Bei der Inbetriebnahme werden acht (8) Wiederherstellungs-Codes generiert und angezeigt. (siehe Use-Case „Beantragen neuer Wiederherstellungs-Codes“)

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.1. - Inbetriebnahme

3.2.2 AUTHENTISIERUNG DES BENUTZERS

Die Authentisierung beschreibt das Feststellen der Identität des aktuellen Benutzers. Nach der erfolgreichen Authentisierung erhält der Benutzer einen Benutzer-Token und wird ermächtigt den Safe, gemäß den zugewiesenen Berechtigungen, zu bedienen.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Es darf kein Benutzer aktiv am System angemeldet sein.

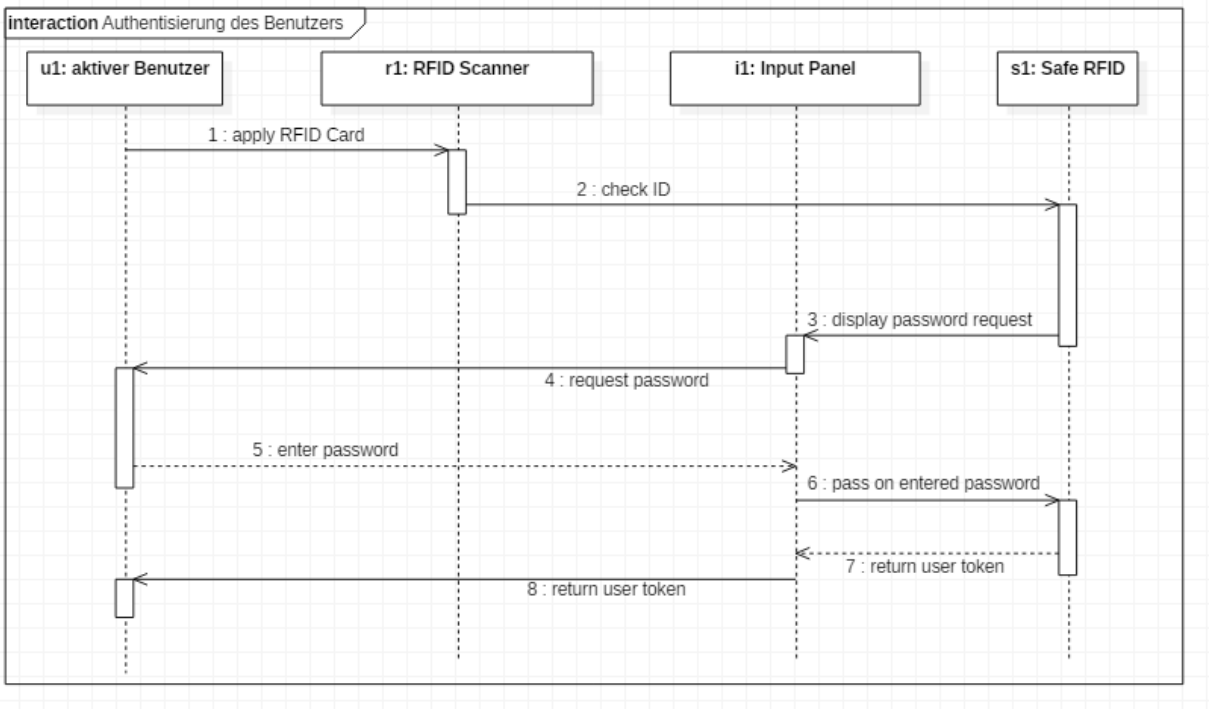

Abbildung 3-3: Sequenzdiagramm "Authentisierung des Benutzers"

Normaler Ablauf: Der Benutzer platziert seine RFID-Karte über dem RFID-Lesegerät. Dieser liest die eindeutige Benutzer-Kennung des aktuellen Benutzers aus. Sofern die Kennung in der Liste der aktiven Benutzer enthalten ist, wird der Benutzer nach seinem persönlichen Passwort gefragt. Stimmt das Passwort mit dem, für den Benutzer gespeicherten Passwort, überein, wird der Benutzer angemeldet.
Die Authentisierung ist ebenfalls über einen Endpunkt in der REST-Schnittstelle möglich.
Jeder Zutrittsversuch wird vom System entsprechend gespeichert.

Alternative Abläufe: Sollte die Benutzer-Kennung, der gescannten RFID-Karte, nicht in der Liste der aktiven Benutzer einhalten sein, wird der Anmeldeprozess abgebrochen und eine entsprechende Warnung in die Liste der gespeicherten Log-Einträge aufgenommen.
Sollte der Benutzer den persönlichen Zugangscode wiederholt (dreimal) falsch eingeben, wird ein Alarm ausgelöst. (siehe Use-Case „Auslösen eines Alarms“)

Nachbedingungen: Nach der erfolgreichen Authentisierung des Benutzers, wurde die Identität dieses eindeutig festgestellt. Der Benutzer kann den Safe nun über das Eingabepanel, gemäß den ihm zugewiesenen Berechtigungen, bedienen.

Ziele: Durch die Authentisierung des Benutzers soll sichergestellt werden, dass es sich bei dem aktuellen Benutzer um einen autorisierten Benutzer handelt. Ist dies der Fall, wird der Benutzer zur Bedienung des Safes ermächtigt.

Extension Points: Sollte der Benutzer den persönlichen Zugangscode wiederholt (dreimal) falsch eingeben, wird ein Alarm ausgelöst. (siehe Use-Case „Auslösen eines Alarms“)

Includes: Jede Authentisierung eines Benutzers wird durch einen entsprechenden Eintrag in der Liste der gespeicherten Log-Einträge vermerkt. Sollte die Authentisierung fehlschlagen, wird der Eintrag mit einer Warnung entsprechend gekennzeichnet. (siehe Use-Case „Speichern der Zutrittsversuche“)

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.2. – Authentisierung des Benutzers

3.2.3 AUSLÖSEN EINES ALARMS

Das Auslösen eines Alarms bedeutet die Abgabe visueller und auditiver Signale, des Safes, um auf einen möglicherweise sicherheitsbeeinträchtigenden Zustand hinzuweisen.

Vorbedingungen: Ein möglicherweise sicherheitsrelevanter Zustand muss ausgelöst werden.

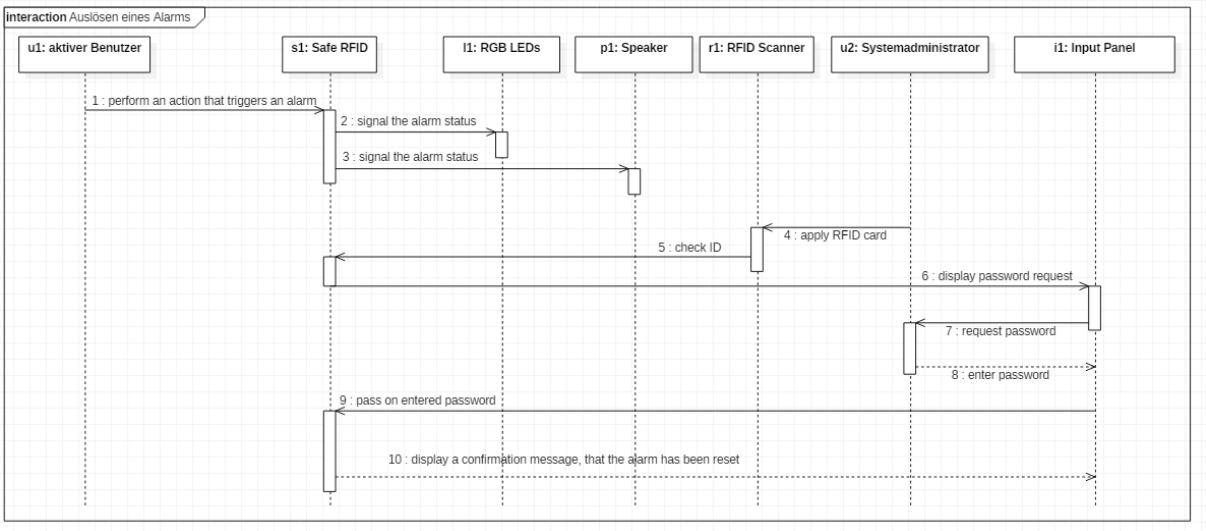

Abbildung 3-4: Sequenzdiagramm "Auslösen eines Alarms"

Normaler Ablauf: Die fünf (5) roten LEDs am oberen Rand des Safes beginnen zu blinken. Zusätzlich wird durch einen im Safe verbauten Lautsprecher ein Signalton abgegeben.
Durch die Authentisierung eines aktiven Systemadministrators kann der Alarm deaktiviert werden.
Das Auslösen des Alarms wird in der Liste der gespeicherten Log-Einträge vermerkt.

Nachbedingungen: Das Auslösen des Alarms soll in der Nähe befindliche Personen auf einen möglicherweise sicherheitsbeeinträchtigenden Zustand des Safes hinweisen. Nach der erfolgreichen Deaktivierung des Alarms geht der Safe in den operativen Betrieb über.

Ziele: Durch das Auslösen eines Alarms soll auf möglicherweise sicherheitsbeeinträchtigende Zustände hingewiesen werden. Das Deaktivieren des Alarms ist nur durch einen Systemadministrator möglich.

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.3. – Auslösen eines Alarms

3.2.4 SPEICHERN DER ZUTRITTSVERSUCHE

Um Zutritte zum Safe nachvollziehen zu können, werden alle Zutrittsversuche aufgezeichnet. Fehlgeschlagene Zutrittsversuche werden durch eine entsprechende Warnung gekennzeichnet.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Ein Zutrittsversuch muss stattfinden.

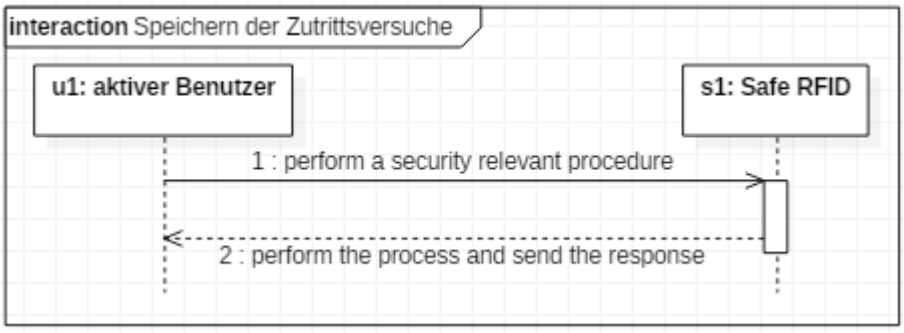

Abbildung 3-5: Sequenzdiagramm "Speichern der Zutrittsversuche"

Normaler Ablauf: Sicherheitsrelevante Vorgänge am System, werden in einer integren Liste vermerkt. Folgende Vorgänge werden vom System gespeichert:

- Die Authentisierung eines Benutzers.
- Das Entriegeln des Safes.
- Das Auslösen eines Alarms.
- Die Abfrage der gespeicherten Log-Einträge.
- Das Zurücksetzen des Safes auf den Werkszustand.
- Das Beantragen neuer Wiederherstellungs-Codes.

Ein gespeicherter Eintrag besteht aus dem Zeitstempel, wann der Vorgang stattgefunden hat, dem Benutzer, der den Vorgang durchgeführt hat und einer Beschreibung des Vorgangs. Fehlgeschlagene Vorgänge werden durch eine entsprechende Warnung und Fehlermeldung gekennzeichnet.

Nachbedingungen: Sobald es zu einem sicherheitsrelevanten Vorgang am System kommt, muss dieser in Form eines Log-Eintrags gespeichert werden. Die Integrität der gespeicherten Einträge muss zu jedem Zeitpunkt gewährleistet sein. Eine Änderung darf nur in Form des Speicherns eines weiteren Eintrags stattfinden. Die Änderung bereits gespeicherter Einträge darf nicht möglich sein.

Ziele: Durch das Speichern aller sicherheitsrelevanten Vorgänge am System, in einer integren Liste, soll die Nachvollziehbarkeit der Vorgänge gesteigert werden.

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.4. – Speichern der Zutrittsversuche

3.2.5 BEANTRAGEN NEUER WIEDERHERSTELLUNGS-CODES

Wiederherstellungs-Codes werden in Sets, bestehend aus acht (8) zufällig generierten Codes, gespeichert. Systemadministratoren sollen die Möglichkeit haben neue Wiederherstellungs-Codes zu beantragen.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Das Beantragen neuer Wiederherstellungs-Codes ist nur durch einen Systemadministrator möglich.

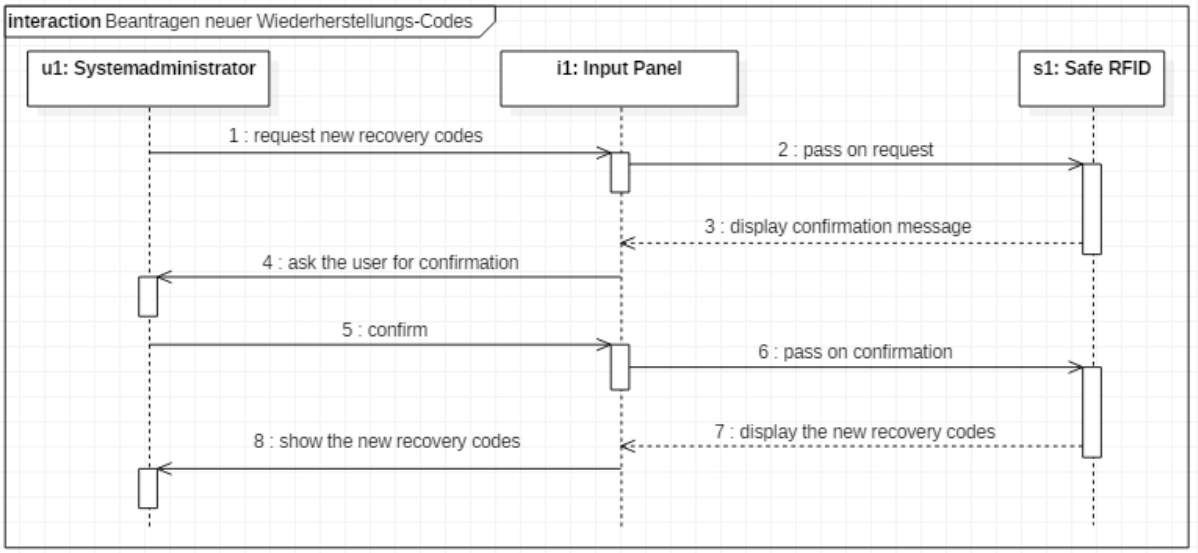

Abbildung 3-6: Sequenzdiagramm "Beantragen neuer Wiederherstellungs-Codes"

Normaler Ablauf: Ein Systemadministrator beantragt über das Eingabepanel, oder die REST-Schnittstelle, neue Wiederherstellungs-Codes. Diese werden von dem System nach dem Zufallsprinzip generiert und dem Benutzer angezeigt. Nachdem dieser die Wiederherstellungs-Codes notiert hat, werden sie vom System gespeichert. Bereits bestehende Wiederherstellungs-Codes werden dadurch invalidiert.

Alternativer Ablauf: Handelt es sich bei dem angemeldeten Benutzer um keinen Systemadministrator, wird der Prozess abgebrochen.

Nachbedingungen: Nach der erfolgreichen Beantragung neuer Wiederherstellungs-Codes, müssen diese vom Benutzer notiert worden sein und das System muss die Codes übernommen haben. Alte Wiederherstellungs-Codes müssen invalidiert worden sein.

Ziele: Der Benutzer soll die Möglichkeit haben jederzeit neue Wiederherstellungs-Codes zu beantragen, sollten die aktuellen Codes verloren gegangen sein oder nur noch eine geringe Anzahl an Wiederherstellungs-Codes gültig sein. Durch das Beantragen neuer Wiederherstellungs-Codes, werden die alten Codes invalidiert.

Includes: Das Beantragen neuer Wiederherstellungs-Codes ist nur für Systemadministratoren, mit einer gültigen Sitzung, möglich. (siehe Use-Case „Validieren des Benutzer-Tokens“)

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.5. – Beantragen neuer Wiederherstellungs-Codes

3.2.6 AUF WERKSZUSTAND ZURÜCKSETZEN

Systemadministratoren sollen die Möglichkeit haben den Safe auf den Werkszustand zurückzusetzen. Durch das Zurücksetzen werden alle gespeicherten Daten, mit Ausnahme der gespeicherten Log-Einträge, gelöscht.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Zum Zeitpunkt des Zurücksetzens müssen gültige Wiederherstellungs-Codes existieren.

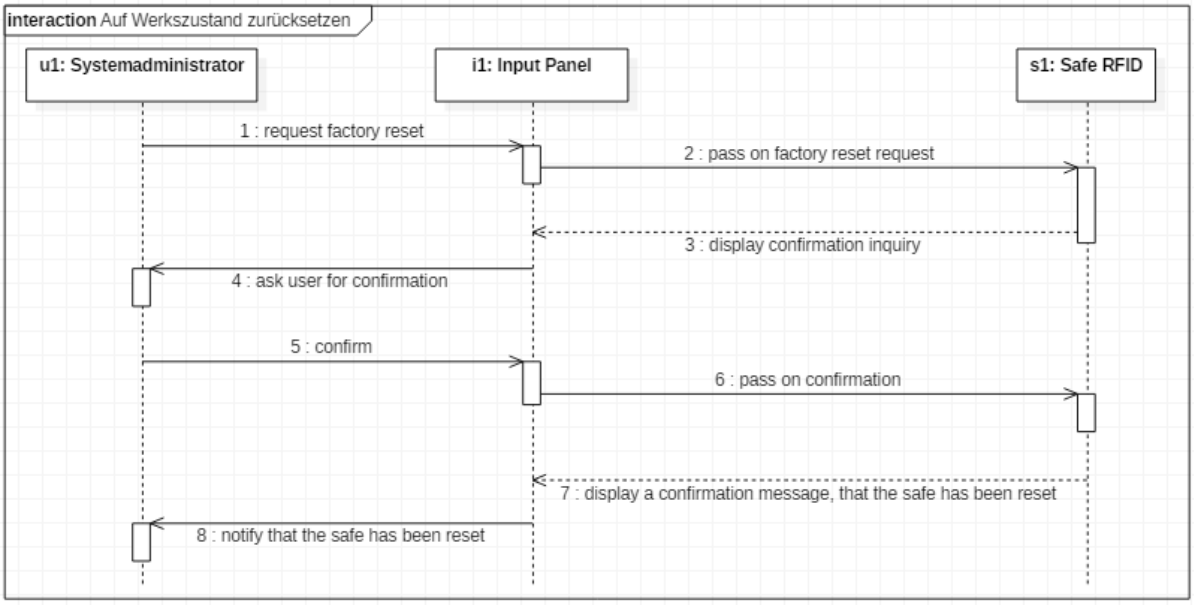

Abbildung 3-7: Sequenzdiagramm "Auf Werkszustand zurücksetzen"

Normaler Ablauf: Ein Systemadministrator leitet das Zurücksetzen des Safes, auf den Werkszustand, ein. Nach der Bestätigung des Vorgangs werden alle gespeicherten Daten, mit Ausnahme der gespeicherten Log-Einträge, unwiederbringlich gelöscht und der Safe, bis zur Eingabe eines gültigen Wiederherstellungs-Codes, gesperrt.
Kommt es im operativen Betrieb zu einer Unterbrechung der Stromversorgung, wird der Safe auf den Werkszustand zurückgesetzt.

Alternative Abläufe: Sollten zum Zeitpunkt des Zurücksetzens keine gültigen Wiederherstellungs-Codes vorhanden sein, wird der Vorgang abgebrochen.

Nachbedingungen: Nach dem Zurücksetzen des Safes, auf den Werkszustand, müssen alle zuvor gespeicherten Daten, mit Ausnahme der gespeicherten Log-Einträge, unwiederbringlich gelöscht worden sein. Zusätzlich muss der Safe, bis zur Eingabe eines gültigen Wiederherstellungs-Codes, gesperrt werden.
Im Falle einer Unterbrechung der Stromversorgung, muss der Safe automatisch auf den Werkszustand zurückgesetzt werden.

Ziele: Durch das Zurücksetzen des Safes auf den Werkszustand wird sichergestellt, dass alle zuvor gespeicherten Daten unwiederbringlich gelöscht werden und sich der Safe in einem

gesperrten Zustand befindet. Zusätzlich wird durch das automatische Zurücksetzen des Safes verhindert, dass durch Unterbrechungen in der Stromversorgung Sicherheitslücken entstehen.

Includes: Das Zurücksetzen des Safes, auf den Werkszustand, ist nur für Systemadministratoren, mit einer gültigen Sitzung, möglich. (siehe Use-Case „Validieren des Benutzer-Tokens“)

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.6. – Auf Werkszustand zurücksetzen

3.2.7 ENTRIEGELN

Aktive Benutzer sollen nach der erfolgreichen Authentisierung die Möglichkeit haben den Safe zu entriegeln.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Ein aktiver Benutzer, mit entsprechenden Berechtigungen, muss am System angemeldet sein.

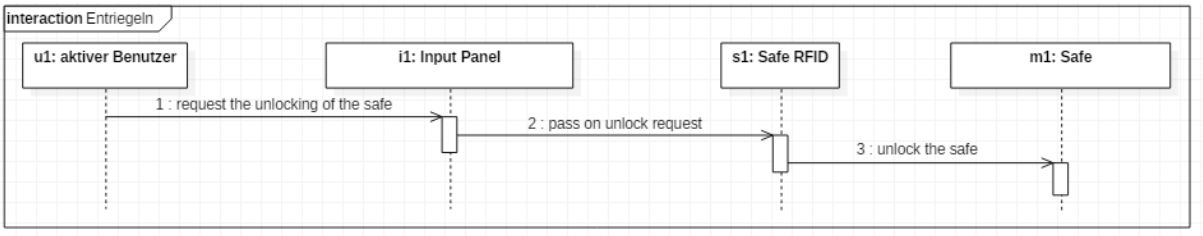

Abbildung 3-8: Sequenzdiagramm "Entriegeln"

Normaler Ablauf: Der angemeldete Benutzer fordert über das Eingabepanel, beziehungsweise die REST-Schnittstelle, die Entriegelung des Safes an. Der Safe entriegelt daraufhin die Türe und der Benutzer kann diese öffnen.
Ein entsprechender Eintrag in den gespeicherten Log-Einträgen wird hinzugefügt.
Wird der Notfall-Taster im Inneren eines begehbaren Safes betätigt, soll der Safe sofort entriegelt werden.

Alternative Abläufe: Wird die Türe des Safes, innerhalb von 30 Sekunden nach der Entriegelung, nicht geöffnet, so wird die Türe automatisch wieder verriegelt und der Benutzer abgemeldet.

Nachbedingungen: Nach der erfolgreichen Entriegelung, muss der Benutzer in der Lage sein die Türe des Safes zu öffnen. Geschieht dies innerhalb von 30 Sekunden nach der Entriegelung nicht, wird die Türe wieder verriegelt und der Benutzer automatisch abgemeldet.

Ziele: Durch das Entriegeln des Safes sollen aktive Benutzer in der Lage sein Zutritt zum Safe zu erhalten.

Extension Points: Findet innerhalb von 30 Sekunden, nach der Entriegelung, keine Öffnung des Safes statt, wird dieser verriegelt und der Benutzer automatisch abgemeldet. (siehe Use-Cases „Verriegeln“ und „Abmelden“)

Includes: Das Entriegeln des Safes ist nur mit einer gültigen Sitzung möglich. (siehe Use-Case „Validieren des Benutzer-Tokens“)

Nach der erfolgreichen Entriegelung des Safes, muss der Verriegelungs-Status entsprechend signalisiert werden. (siehe Use-Case „Signalisierung des Verriegelungs-Status“)
Zutritte zu dem Safe sollen entsprechend gespeichert werden. (siehe Use-Case „Speichern der Zutrittsversuche“)

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.7. - Entriegeln

3.2.8 ABFRAGEN DER LOG-EINTRÄGE

Gespeicherte Log-Einträge sollen von Systemadministratoren abgerufen werden können.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Ein Systemadministrator muss am System angemeldet sein.

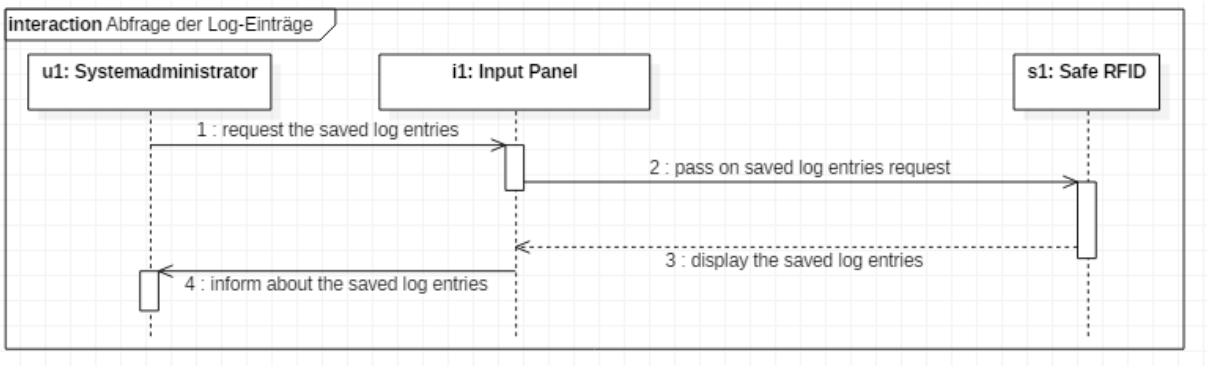

Abbildung 3-9: Sequenzdiagramm "Abfragen der Log-Einträge"

Normaler Ablauf: Ein Systemadministrator fragt über das Eingabepanel, oder die REST-Schnittstelle, die gespeicherten Log-Einträge ab. Die gespeicherten Einträge werden daraufhin in chronologischer Reihenfolge angezeigt.

Alternative Abläufe: Handelt es sich bei dem aktuell angemeldeten Benutzer um keinen Systemadministrator, steht die Option die gespeicherten Log-Einträge abzufragen, nicht zur Verfügung.

Nachbedingungen: Nach der Abfrage der Log-Einträge werden dem angemeldeten Systemadministrator alle gespeicherten Einträge angezeigt.
Die Abfrage der Log-Einträge selbst, soll ebenfalls als ein Log-Eintrag gespeichert werden.

Ziele: Durch die Abfrage der gespeicherten Log-Einträge, sollen Systemadministratoren die Möglichkeit haben sicherheitsrelevante Vorfälle nachvollziehen zu können und Anomalien zu erkennen.

Includes: Die Abfrage der gespeicherten Log-Einträge soll nur Systemadministratoren, mit einer gültigen Sitzung, möglich sein. (siehe Use-Case „Validieren des Benutzer-Tokens“)

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.8. – Abfragen der Log-Einträge

3.2.9 ADMINISTRATION ÜBER SEPARATE SCHNITTSTELLE

Dem Auftraggeber, sowie Systemadministratoren des Endkunden, soll über eine REST-Schnittstelle, die am Eingabepanel gegebene Funktionalität geboten werden.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Der Benutzer muss sich über die REST-Schnittstelle entsprechend authentisiert haben. (= der Benutzer muss einen Benutzer-Token angefordert haben.)

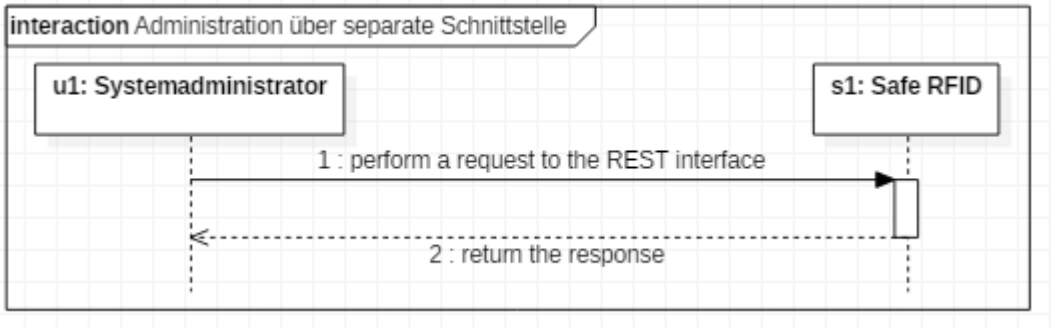

Abbildung 3-10: Sequenzdiagramm "Administration über separate Schnittstelle"

Normaler Ablauf: Das System bietet dem Auftraggeber, sowie Systemadministratoren des Endkunden, eine REST-Schnittstelle, zur Kommunikation mit dem System. Durch diese Schnittstelle werden dem Benutzer dieselben Funktionalitäten wie am Eingabepanel geboten. Der Zugriff ist nur durch das Mitsenden eines gültigen Benutzer-Tokens möglich.

Alternative Abläufe: Wird mit einer Anfrage an die REST-Schnittstelle kein gültiger Benutzer-Token mitgesendet, wird die Anfrage nicht verarbeitet und ein entsprechender Fehler wird geworfen. (Statuscode 401 – Unauthorized)
Findet die Anfrage an einem ungültigen Endpunkt der REST-Schnittstelle statt, wird diese nicht verarbeitet und ein entsprechender Fehler geworfen. (Statuscode 404 – Not found)
Tritt während der Verarbeitung der Anfrage ein Fehler auf, wird die Fehlermeldung zurückgegeben. (Statuscode 500 – Internal Server Error)

Nachbedingungen: Nach einer erfolgreichen Anfrage an die REST-Schnittstelle, sollen dem Benutzer die angefragten Daten zurückgegeben werden beziehungsweise der angefragte Vorgang durchgeführt werden.

Ziele: Durch den Zugriff auf die Funktionen des Systems über eine REST-Schnittstelle, soll dem Auftraggeber und den Systemadministratoren des Endkunden die Möglichkeit gegeben werden das System über alternative Anwendungen sowie remote steuern zu können.

Includes: Damit die Anfragen eines Benutzers, an die REST-Schnittstelle, verarbeitet werden, muss mit diesen ein gültiger Benutzer-Token mitgesendet werden. (siehe Use-Case „Validieren des Benutzer-Tokens“)
Anfragen an die REST-Schnittstelle werden als Log-Einträge gespeichert. (siehe Use-Case „Speichern der Zutrittsversuche“)

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.9. – Administration über separate Schnittstelle

3.2.10 ABMELDEN

Angemeldete Benutzer sollen die Möglichkeit haben sich über das Eingabepanel sowie über die REST-Schnittstelle manuell abzumelden.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Ein aktiver Benutzer muss am System angemeldet sein. Die Türe des Safes muss verriegelt sein.

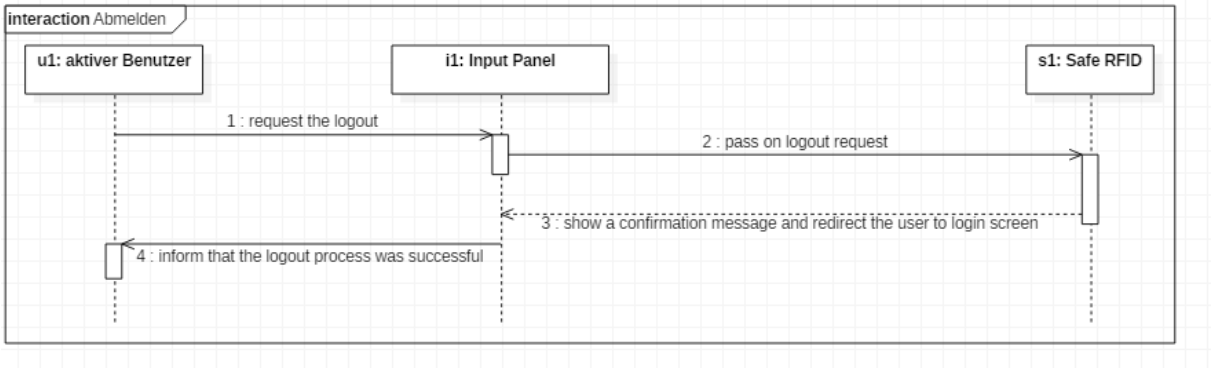

Abbildung 3-11: Sequenzdiagramm "Abmelden"

Normaler Ablauf: Der Benutzer meldet sich über das Eingabepanel manuell ab. Dadurch wird der Benutzer-Token invalidiert und der Benutzer muss sich, zur Interaktion mit dem System, erneut authentisieren.
Wird für eine Dauer von 30 Sekunden keine Interaktion mit dem System registriert, wird der Benutzer automatisch abgemeldet. (Sollte sich die Safe-Türe im geöffneten Zustand befinden, unterbricht dies den Mechanismus.)

Nachbedingungen: Durch das Abmelden soll der Benutzer-Token invalidiert werden und der Benutzer nicht mehr in der Lage sein mit dem System zu interagieren.

Ziele: Durch das manuelle sowie das automatische Abmelden sollen Zutritte durch unbefugte Dritte verhindert werden. Die Interaktion mit dem System ist, nach der Abmeldung, erst nach einer erneuten Anmeldung wieder möglich.

Includes: Das Abmelden vom System ist nur mit einer gültigen Sitzung möglich. (siehe Use-Case „Validieren des Benutzer-Tokens“)

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.10. - Abmelden

3.2.11 OPERATIVEN BETRIEB WIEDERHERSTELLEN

Nachdem der Safe manuell oder durch eine Unterbrechung der Stromversorgung auf den Werkszustand zurückgesetzt wurde, befindet sich dieser in einem gesperrten Zustand.
Der operative Betrieb kann erst nach der Eingabe eines gültigen Wiederherstellungs-Codes wieder aufgenommen werden.

Vorbedingungen: Der Safe muss sich im gesperrten Zustand befinden und mit Strom versorgt werden. Es müssen gültige Wiederherstellungs-Codes vorhanden sein.

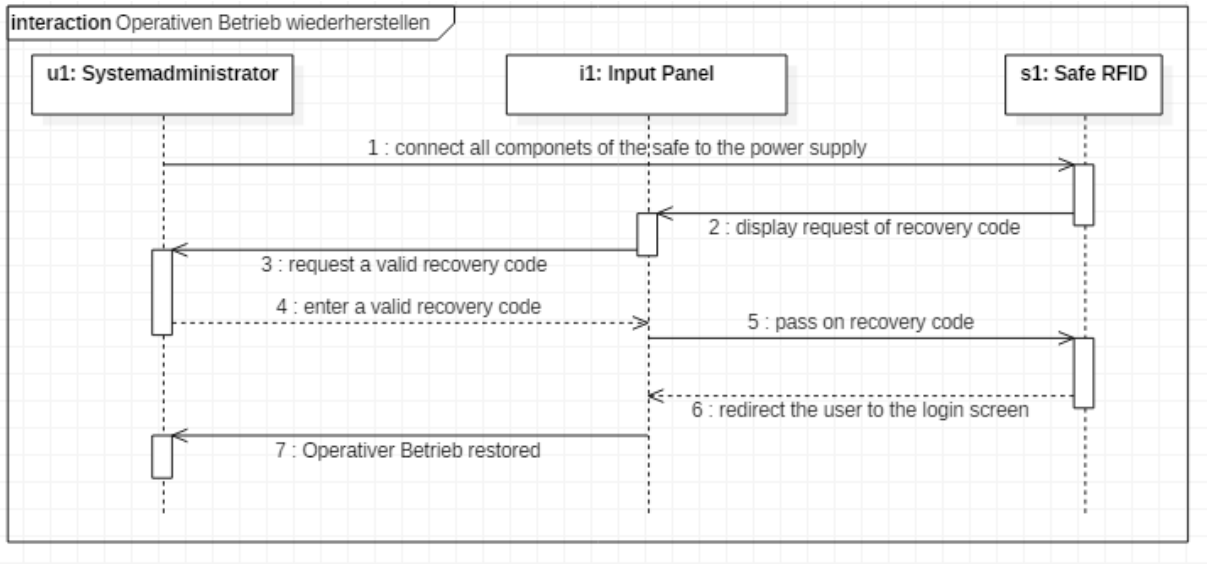

Abbildung 3-12: Sequenzdiagramm "Operativen Betrieb wiederherstellen"

Normaler Ablauf: Im gesperrten Zustand zeigt der Safe am Eingabepanel ein Feld für die Eingabe eines gültigen Wiederherstellungs-Codes an. Sobald der Wiederherstellungs-Code durch einen Systemadministrator eingegeben wurde, geht der Safe wieder in den operativen Betrieb über.

Alternative Abläufe: Handelt es sich bei dem eingegebenen Wiederherstellungs-Code um einen ungültigen Code, ist die Wiederherstellung des operativen Betriebs nicht möglich.

Nachbedingungen: Nach der Wiederherstellung des operativen Betriebs soll der Safe wieder entsperrt sein und bedient werden können. Der eingegebene Wiederherstellungs-Code soll invalidiert worden sein.

Ziele: Durch die Wiederherstellung des operativen Betriebs wird der manuell oder durch eine Unterbrechung der Stromversorgung verursachte gesperrte Zustand beendet und der Safe somit für aktive Benutzer wieder bedienbar.

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.11. – Operativen Betrieb wiederherstellen

3.2.12 VALIDIEREN DES BENUTZER-TOKENS

Bevor eine Operation vom System ausgeführt wird, muss die Gültigkeit der aktuellen Benutzer-Sitzung überprüft werden.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Ein aktiver Benutzer muss am System angemeldet sein. Eine Operation muss vom Benutzer ausgeführt werden.

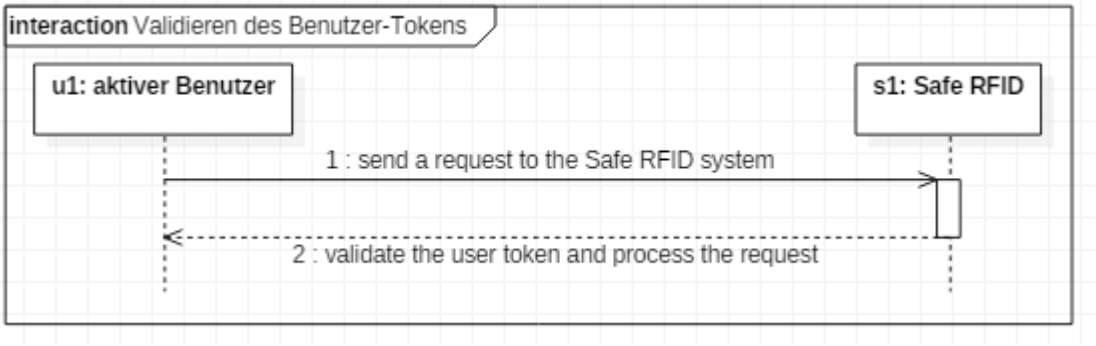

Abbildung 3-13: Sequenzdiagramm "Validieren des Benutzer-Tokens"

Normaler Ablauf: Beantragt ein angemeldeter Benutzer die Ausführung einer Operation, muss vor dem Starten des Vorgangs die Gültigkeit der aktuellen Sitzung, sowie die Berechtigungen des aktuellen Benutzers, überprüft werden. Die Überprüfung findet anhand des, der Anfrage mitgesendeten, Benutzer-Tokens statt.

Alternative Abläufe: Handelt es sich bei dem, mit der Anfrage mitgesendeten Benutzer-Token, um ein ungültiges Benutzer-Token, beziehungsweise besitzt der Benutzer nicht die benötigten Berechtigungen, wird die angeforderte Operation nicht ausgeführt und ein entsprechender Fehler geworfen. (Statuscode 401 – Unauthorized)
In diesem Fall wird eine entsprechende Warnung, in Form eines Log-Eintrags, gespeichert.

Nachbedingungen: Nach der Validierung des Benutzer-Tokens soll die Gültigkeit der aktuellen Sitzung überprüft worden sein. Handelt es sich um einen gültigen Benutzer-Token, wird die angefragte Operation ausgeführt.

Ziele: Durch die Validierung des Benutzer-Tokens soll der Zugriff auf Funktionen des Safes, durch unbefugte Dritte sowie unautorisierte Benutzer, verhindert werden.

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.12. – Validieren des Benutzer-Tokens

3.2.13 VERRIEGELUNG AKTIVIEREN-DEAKTIVIEREN

Systemadministratoren sollen in der Lage sein die elektronische Verriegelung zu aktivieren bzw. zu deaktivieren. Bei deaktivierter Verriegelung kann die Safe-Türe solange manuell, ohne weitere Schutzmechanismen, geöffnet werden, bis die elektronische Verriegelung reaktiviert wird.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Ein Systemadministrator muss am System angemeldet sein.

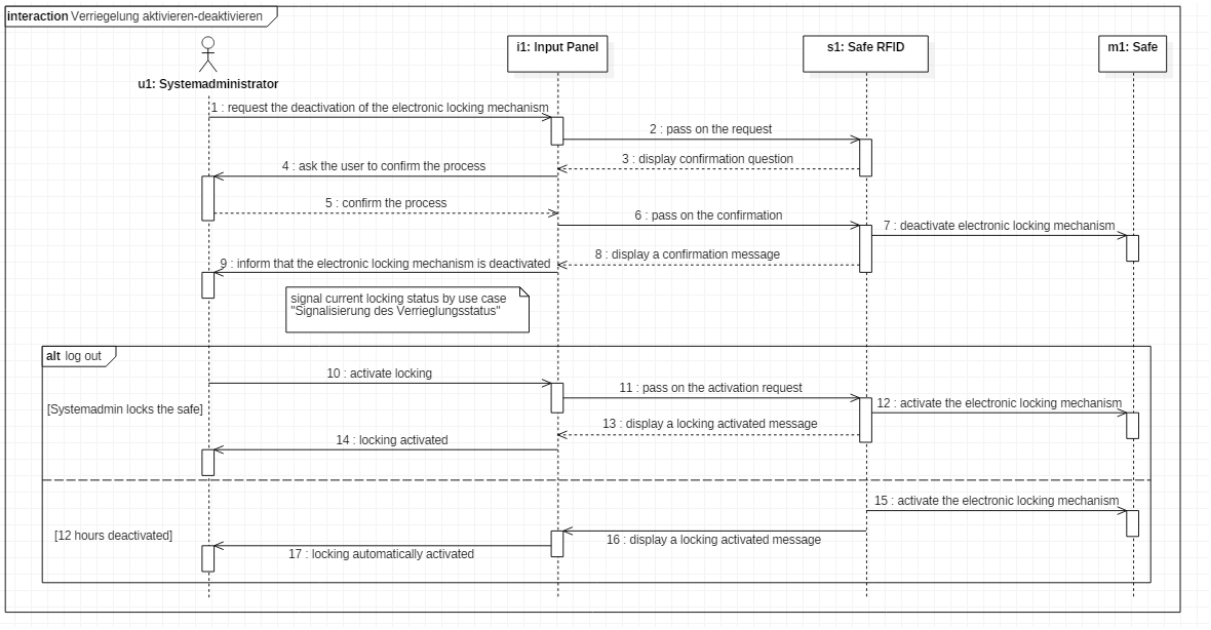

Abbildung 3-14: Sequenzdiagramm "Verriegelung aktivieren-deaktivieren"

Normaler Ablauf: Ein Systemadministrator beantragt die Deaktivierung der elektronischen Verriegelung. Nach der Bestätigung des Vorgangs, durch den Benutzer, wird die elektronische Verriegelung vom System deaktiviert.
Ist die Deaktivierung der elektronischen Verriegelung erfolgt, kann diese durch einen Systemadministrator wieder aktiviert werden. Dieser Vorgang ist nur möglich, wenn sich die Türe des Safes im geschlossenen Zustand befindet.
Um eine permanente Entriegelung zu vermeiden, wird die elektronische Verriegelung nach einer Dauer von 12 Stunden automatisch wieder aktiviert.

Alternative Abläufe: Ist die Safe-Türe geöffnet, was durch einen Sensor signalisiert wird, und wird versucht die elektronische Verriegelung wieder zu aktivieren, so muss eine Fehlermeldung am LCD-Screen erscheinen und die optische Signalisierung des Verriegelungsstatus durch die LEDs darf nicht auf Grün geändert werden. Wird die Safe-Türe geschlossen, so kann, wie im Normalen Ablauf beschrieben, die elektronische Verriegelung wieder aktiviert werden.

Für den Fall, dass die elektronische Verriegelung nach 12 Stunden nicht eingeschaltet werden kann, weil die Safe-Türe nicht geschlossen ist, wird ein Alarm ausgelöst.

Nachbedingungen: Die Safe-Türe befindet sich im geschlossenen Zustand und der Safe ist wieder elektronisch verriegelt. Um die Konsistenz der Zutrittsliste zu gewährleisten wird dieser Ablauf als Zutrittsversuch mit spezieller Kennzeichnung gespeichert.

Ziele: Das Ziel dabei ist, dass sich der Safe für die eine bestimmte Zeitdauer öffnen lässt, um zum Beispiel Umbauarbeiten in der Innenausstattung etc. vornehmen zu können. Nach diesen Tätigkeiten befindet sich die Safe-Türe wieder im geschlossenen Zustand und ist elektronisch verriegelt.

Extension Points: Befindet sich die Türe des Safes 12 Stunden nach der Deaktivierung der elektronischen Verriegelung im geöffneten Zustand, wird ein Alarm ausgelöst. (siehe Use-Case „Auslösen eines Alarms“)

Includes: Vor der Aktivierung beziehungsweise Deaktivierung der elektronischen Verriegelung müssen die Identität und die Berechtigungen des Benutzers validiert werden. (siehe Use-Case „Validieren des Benutzer-Tokens“)
Der geänderte Verriegelungsstatus soll jederzeit entsprechend signalisiert werden. (siehe Use-Case „Signalisieren des Verriegelungsstatus“)

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.13. – Verriegelung aktivieren-deaktivieren

3.2.14 BENUTZER INAKTIV STELLEN

Ein Systemadministrator muss die Möglichkeit haben einem bestehenden Nutzer die Zutrittsrechte zum Safe zu entziehen.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Ein Systemadministrator muss am System angemeldet sein.

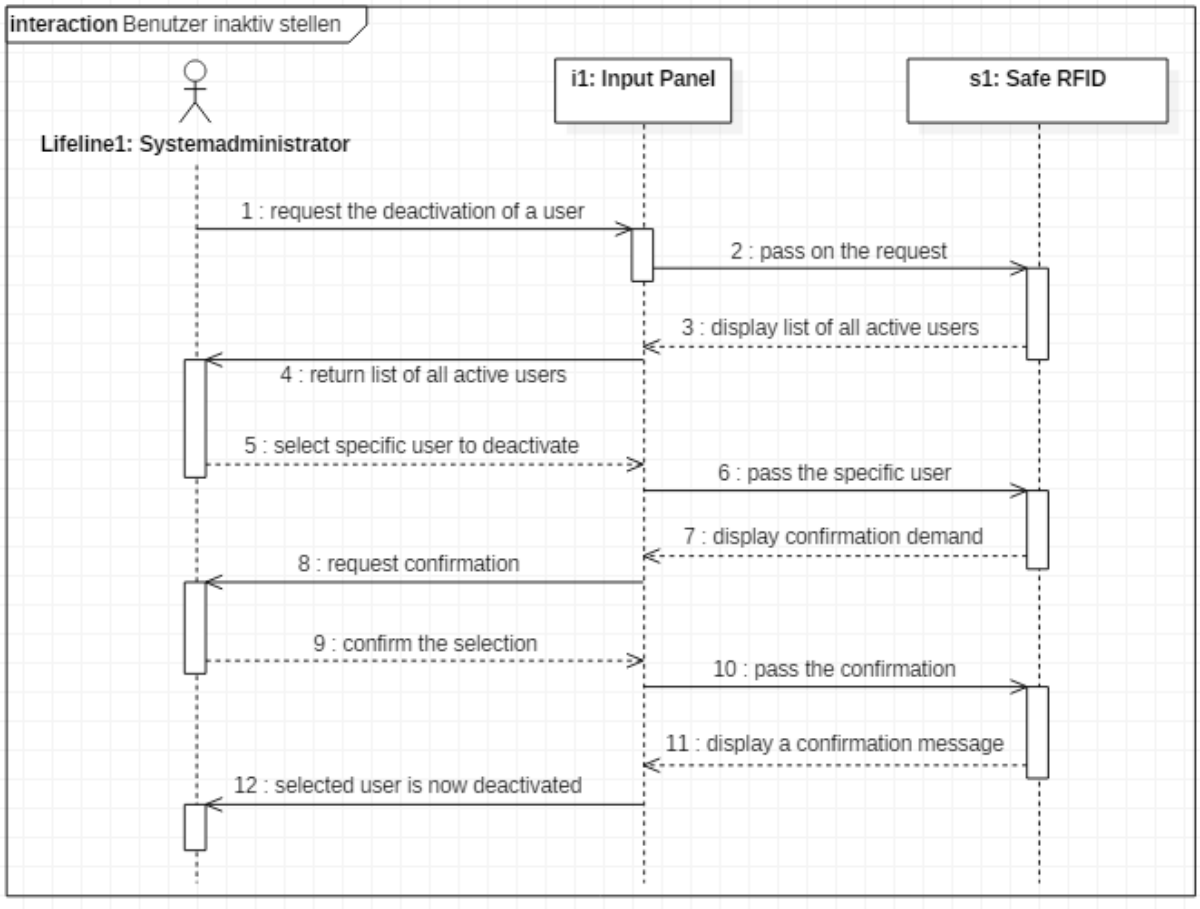

Abbildung 3-15: Sequenzdiagramm "Benutzer inaktiv stellen"

Normaler Ablauf: Der Systemadministrator wählt über das Eingabepanel beziehungsweise die REST-Schnittstelle die Funktion einen Benutzer zu deaktivieren. Daraufhin wird ihm eine Liste aller aktiven Benutzer angezeigt, die Zugang zu dem Safe haben. Durch Auswählen eines Nutzers und anschließendes Bestätigen der Auswahl wird derjenige Benutzer inaktiv gestellt. Existieren mehrere Systemadministratoren, so ist es jedem Systemadministrator erlaubt andere solche inaktiv zu stellen.

Alternative Abläufe: Handelt es sich bei dem angemeldeten Benutzer um keinen Systemadministrator, wird der Prozess abgebrochen.

Nachbedingungen: Der ausgewählte Benutzer soll inaktiv gestellt werden. Der Zugang zum System ist somit für den Benutzer nicht mehr möglich.

Ziele: Der Kreis der zutrittsberechtigten Personen soll so klein als möglich gehalten werden. Durch diese Funktion ist der Systemadministrator in der Lage Personen den Zutritt zu entziehen.

Includes: Vor der Deaktivierung eines Benutzers müssen die Identität und die Berechtigungen des angemeldeten Benutzers validiert werden. (siehe Use-Case „Validieren des Benutzer-Tokens“)

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.14. – Benutzer inaktiv stellen

3.2.15 BENUTZER AKTIV STELLEN

Der Systemadministrator muss die Möglichkeit haben einen inaktiven Nutzer aktiv zu stellen und ihm somit den Zutritt zum Safe wieder zu erlauben.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Ein Systemadministrator muss am System angemeldet sein.

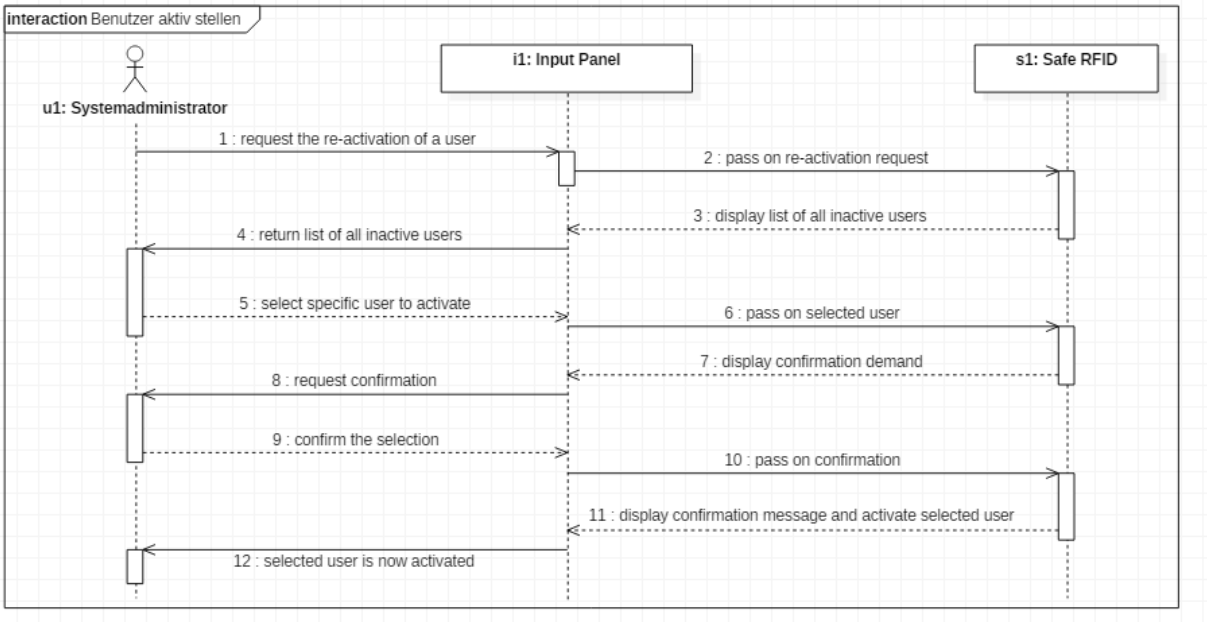

Abbildung 3-16: Sequenzdiagramm "Benutzer aktiv stellen"

Normaler Ablauf: Der Systemadministrator wählt mittels des Eingabepanels beziehungsweise der REST-Schnittstelle die Funktion einen Benutzer zu aktivieren. Daraufhin wird ihm eine Liste aller inaktiven Benutzer angezeigt. Durch Auswählen eines inaktiven Benutzers und erneutem Bestätigen wird der Aktivierungs-Prozess gestartet. Dieser hat nun, je nach Berechtigungsstatus, Zugriff auf die Funktionen des Safes.

Alternative Abläufe: Handelt es sich bei dem angemeldeten Benutzer um keinen Systemadministrator, wird der Prozess abgebrochen.

Nachbedingungen: Der ausgewählte Benutzer soll aktiv gestellt werden. Der Zugang zum System soll daraufhin für diesen Benutzer wieder möglich sein.

Ziele: Einem inaktiven Benutzer wurde wieder Zutritt zu dem Safe gewährt.

Includes: Vor der Aktivierung eines zuvor deaktivierten Benutzers müssen die Identität und die Berechtigungen des angemeldeten Benutzers validiert werden. (siehe Use-Case „Validieren des Benutzer-Tokens“)

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.15. – Benutzer aktiv stellen

3.2.16 BENUTZER ERSTELLEN

Systemadministratoren soll es möglich sein, neue Benutzer anzulegen, die wiederum mit der ihnen zugewiesenen RFID-Karte und einem persönlichen Zugangscode Zutritt zu dem Safe erhalten.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Ein Systemadministrator muss am System angemeldet sein.

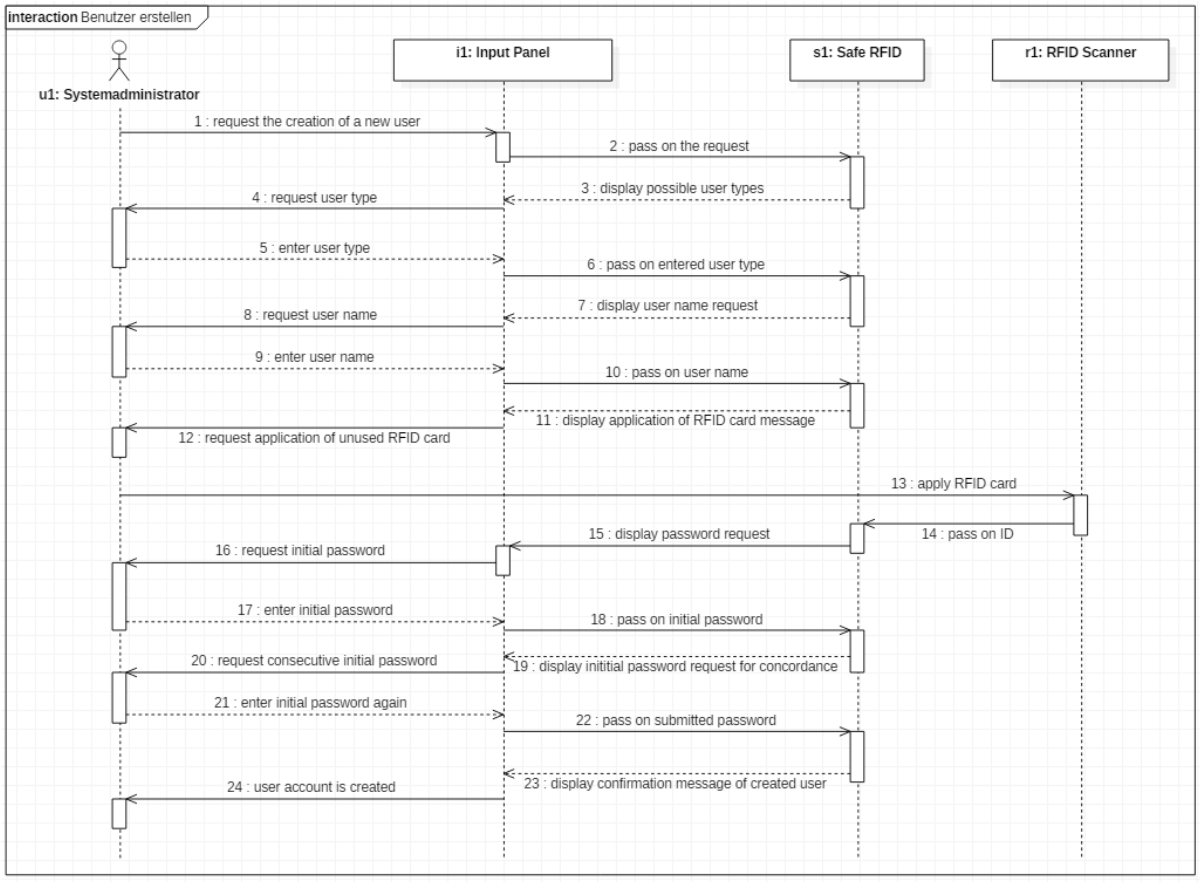

Abbildung 3-17: Sequenzdiagramm "Benutzer erstellen"

Normaler Ablauf: Nachdem der aktuell angemeldete Benutzer die Option einen neuen Benutzer anzulegen ausgewählt hat, wird dieser um die Eingabe des gewünschten Benutzer-Typen gebeten. Weiters muss der Name festgelegt werden, unter dem dieser Benutzer im Zutrittsspeicher-Verzeichnis angezeigt werden soll. Die Zuweisung der RFID-Karte erfolgt durch Anlegen einer noch nicht registrierten RFID-Karte an das RFID-Lesegerät. Dabei muss der

Systemadministrator ein initiales Passwort festlegen. Das Passwort muss sieben (7) Zeichen lang sein und Buchstaben sowie Zahlen enthalten. Es muss zweimal eingeben werden, um Fehler bei der Eingabe zu vermeiden. Der neu angelegte Benutzer kann seinen persönlichen Zugangscode, nach erfolgter Anmeldung am System, selbstständig ändern.

Alternative Abläufe: Wird eine bereits eine registrierte RFID-Karte an das RFID-Lesegerät gehalten, muss eine Fehlermeldung erscheinen.
Erfüllt das vom Systemadministrator eingegebene Passwort die formalen Bedingungen nicht, muss ein anderes Passwort gewählt werden.

Nachbedingungen: Der neu angelegte Benutzer hat mittels RFID-Karte und dem vom Systemadministrator festgelegten Passwort Zugang zu dem Safe. Neu angelegte Benutzer haben die Möglichkeit, nach erfolgter Anmeldung am System, das initial zugewiesene Passwort zu ändern. (siehe Use-Case „Persönliches Passwort ändern“)

Ziele: Ein neuer Benutzer wurde angelegt, der Zutritt zu dem Safe hat.

Includes: Vor der Deaktivierung eines Benutzers müssen die Identität und die Berechtigungen des angemeldeten Benutzers validiert werden. (siehe Use-Case „Validieren des Benutzer-Tokens“)

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.16. – Benutzer erstellen

3.2.17 PERSÖNLICHES PASSWORT ÄNDERN

Jeder Benutzer soll in der Lage sein, sein persönliches Passwort zu ändern.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Ein aktiver Benutzer muss am System angemeldet sein.

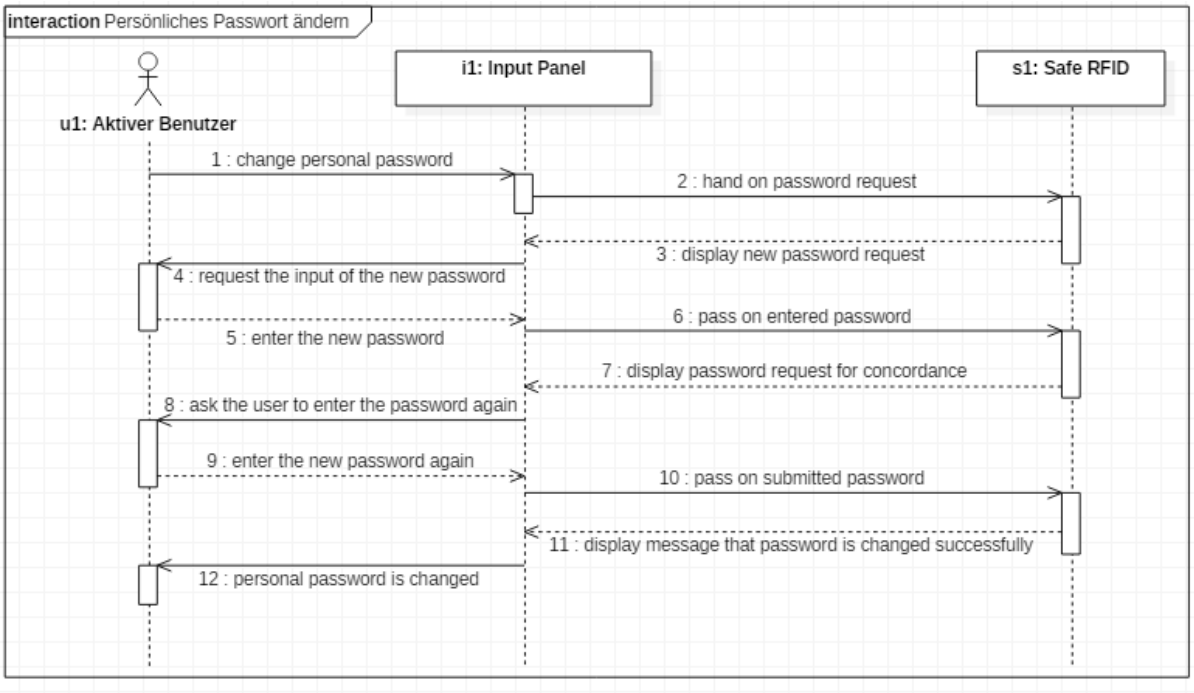

Abbildung 3-18: Sequenzdiagramm "Persönliches Passwort ändern"

Normaler Ablauf: Mithilfe des Eingabepanels beziehungsweise der REST-Schnittstelle wählt der Benutzer die Funktion zum Ändern des persönlichen Passwortes aus. Nach zweimaliger Eingabe des gewünschten Passwortes, wird dieses vom System übernommen. Das Passwort muss eine Länge von sieben (7) Zeichen haben und Buchstaben sowie Zahlen enthalten.
Aktive Benutzer dürfen nur in der Lage sein ihr eigenes Passwort zu ändern.
Systemadministratoren soll es möglich sein das Passwort anderer Benutzer zu ändern.

Alternative Abläufe: Bei Nichtübereinstimmen der beiden Passwörter wird eine Fehlermeldung angezeigt und der gewünschte Code muss erneut eingegeben werden.
Erfüllt das eingegebene Passwort die definierten Anforderungen an ein Passwort nicht, muss von dem Benutzer ein anderes Passwort gewählt werden.

Nachbedingungen: Nach der erfolgreichen Änderung des Passwortes ist der Benutzer in der Lage sich über dieses am System zu authentisieren.

Ziele: Durch die Änderung des persönlichen Passwortes soll der Benutzer in der Lage sein das bei der Authentisierung benötigte Passwort zu ändern.

Includes: Das Ändern des Passwortes darf nur nach der erfolgten Validierung der Identität sowie der Berechtigungen des angemeldeten Benutzers erfolgen. (siehe Use-Case „Validieren des Benutzer-Tokens“)

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.17. – Persönliches Passwort ändern

3.2.18 SIGNALISIEREN DES VERRIEGELUNGSSTATUS

Da der Verriegelungsstatus sicherheitsrelevant ist muss dieser eindeutig und gut sichtbar dargestellt werden. Zur Signalisierung werden fünf (5) LEDs am oberen Rand des Safes verwendet.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Es darf kein Alarm ausgelöst worden sein.

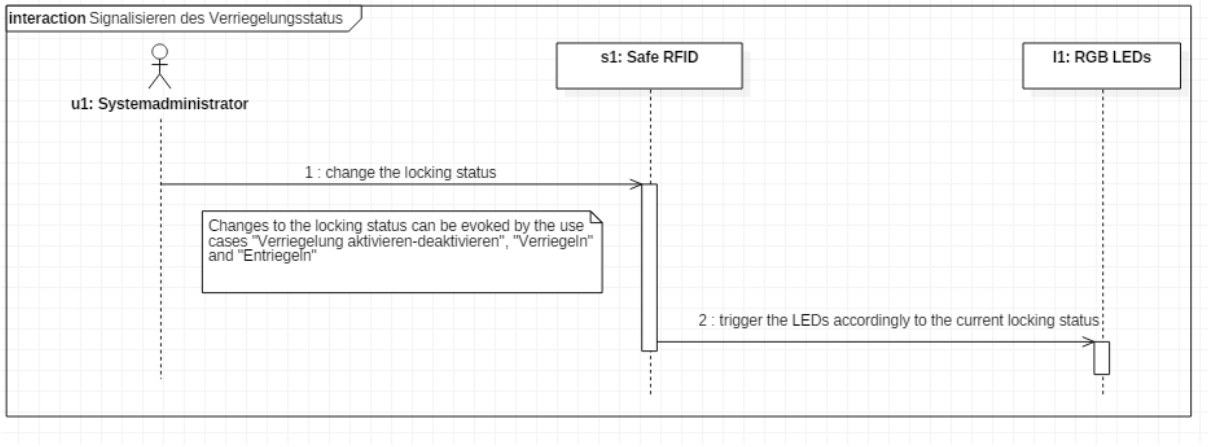

Abbildung 3-19: Sequenzdiagramm "Signalisieren des Verriegelungsstatus"

Normaler Ablauf: Da es sich um eine essenzielle Information handelt muss, sofern keine Unterbrechung der Stromversorgung auftritt, der Verriegelungsstatus jederzeit signalisiert

werden. Im entriegelten Zustand leuchten die am oberen Rand des Safes montierten LEDs grün. Im versperrten Zustand leuchten die LEDs rot.
Änderungen des Verriegelungs-Status können durch das Entriegeln beziehungsweise Verriegeln des Safes (siehe Use-Case „Entriegeln“ beziehungsweise „Verriegeln“) sowie dem Aktivieren beziehungsweise Deaktivieren der elektronischen Verriegelung hervorgerufen werden.

Nachbedingungen: Der aktuelle Verriegelungsstatus des Safes soll jederzeit entsprechend signalisiert werden.

Ziele: Eine eindeutige Anzeige signalisiert zu jeder Zeit den aktuellen Verriegelungs-Status des Safes.

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.18. – Signalisieren des Verriegelungsstatus

3.2.19 VERRIEGELN

Nach einer Entriegelung des Safes soll es dem Benutzer wieder möglich sein den Safe zu verriegeln.

Vorbedingungen: Der Safe muss sich im operativen Betrieb befinden. Ein aktiver Benutzer muss sich erfolgreich angemeldet haben und der Safe muss im entriegelten Zustand sein. Die Türe des Safes muss sich im geschlossenen Zustand befinden.

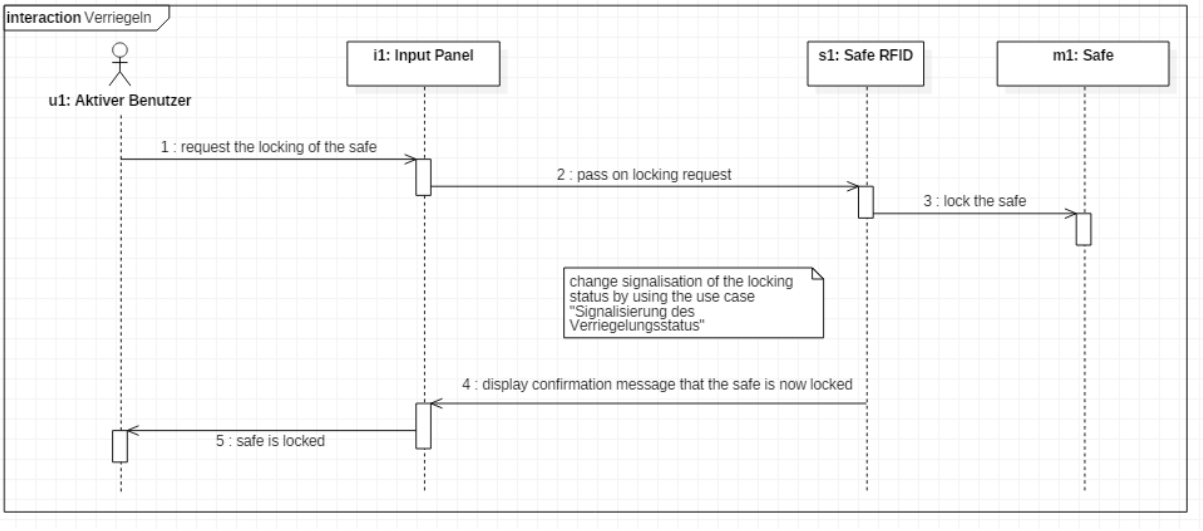

Abbildung 3-20: Sequenzdiagramm "Verriegeln"

Normaler Ablauf: Der angemeldete Benutzer wählt über das Eingabepanel beziehungsweise die REST-Schnittstelle die „Verriegeln“-Funktion aus. Der Safe wird daraufhin elektronisch verriegelt.

Alternative Abläufe: Befindet sich die Türe des Safes, zum Zeitpunkt der Verriegelung, in einem geöffneten Zustand, kann dieser nicht verriegelt werden. In diesem Fall muss der Benutzer durch eine Fehlermeldung auf den geöffneten Zustand der Türe hingewiesen werden.

Nachbedingungen: Nach der erfolgten Verriegelung des Safes, kann dieser erst nach einer erneuten Entriegelung wieder geöffnet werden.

Ziele: Mithilfe des Verriegelns soll das uneingeschränkte Öffnen der Safe Tür verhindert werden.

Includes: Nach der erfolgreichen Verriegelung des Safes, muss der Verriegelungs-Status entsprechend signalisiert werden. (siehe Use-Case „Signalisierung des Verriegelungs-Status“) Das Verriegeln des Safes soll nur aktiven Benutzern mit entsprechenden Berechtigungen gestattet sein. (siehe Use-Case „Validieren des Benutzer-Tokens“)

Hervorgehende funktionale Anforderungen: Siehe Punkt 3.4.19. – Verriegeln

3.3 Domänenmodell

Im folgenden Domänenmodell wird die zu entwickelnde Lösung in einem roten Rechteck dargestellt. Dies umfasst die eigentliche Software Safe RFID, das REST Interface sowie den Hardware Abstraction Layer. Jedem Benutzer, der physischen Zugang zum Safe hat, wird eine RFID Karte zugewiesen.
Die Administration des Safes, durch den Auftraggeber, erfolgt über die REST-Schnittstelle. Wie schon in Use-Case „Administration über separate Schnittstelle“ beschrieben haben auch die Systemadministratoren über die REST Schnittstelle Zugriff auf die Funktionen des Safes.

Eine weitere Einschränkung betrifft den Kommunikationsfluss. Die zentrale Steuereinheit ist die Software „Safe RFID“. Eine Kommunikation zwischen dem Eingabepanel und dem Hardware Abstraction Layer ist ohne Einbeziehen der zu entwickelnden Lösung nicht möglich.

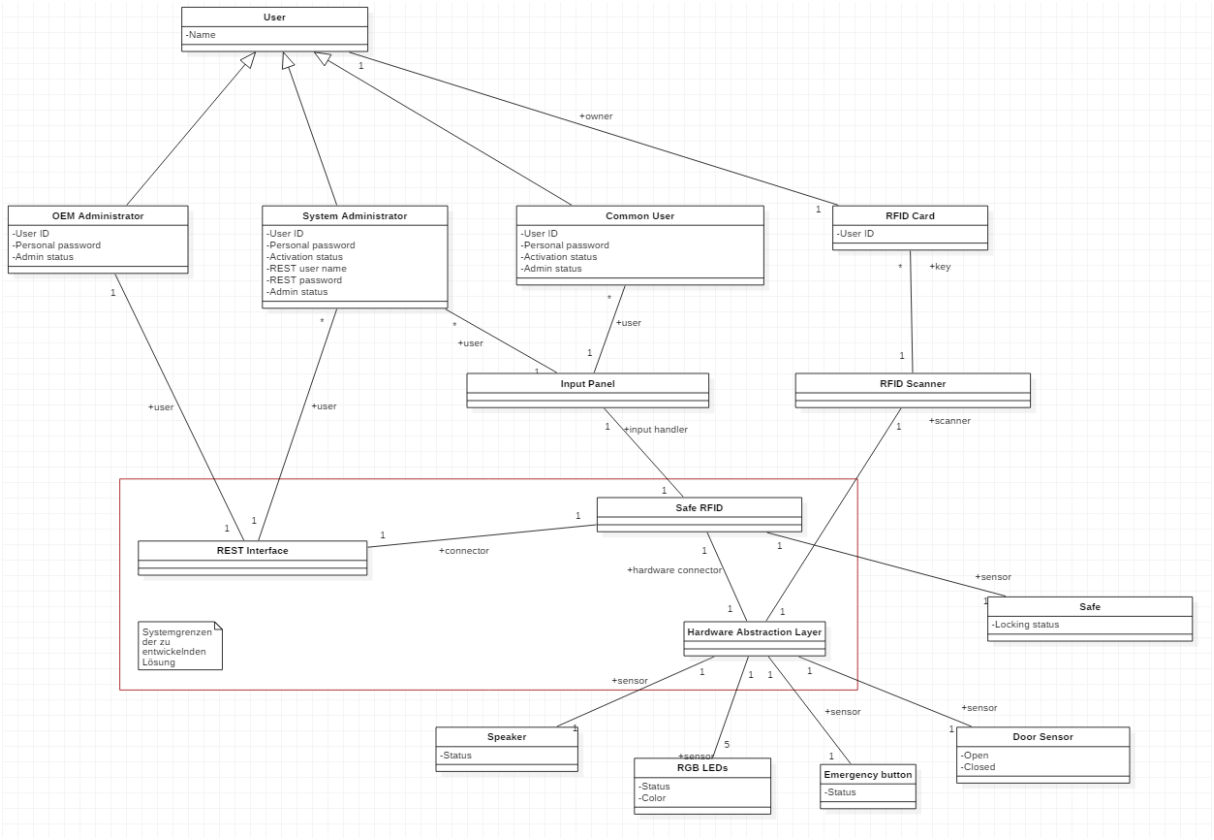

Abbildung 3-21: Domänenmodell

3.4 Funktionale Anforderungen

3.4.1 INBETRIEBNAHME

Der Safe muss einen Anschluss zur Stromversorgung bieten. Im Safe verbaut soll sich ein Rechner befinden, welcher automatisch startet, sobald die Stromversorgung angeschlossen wird.
Der Safe muss im Rahmen der Inbetriebnahme acht (8) unterschiedliche, zufällig generierte Codes anzeigen. Weiters muss der Benutzer aktiv aufgefordert werden einen Systemadministrator-Account zu erstellen. Der im Safe verbaute Rechner muss eine Speichereinheit haben und ein Datenbankmanagement-System zur Verfügung stellen. Die zu entwickelnde Lösung soll ein eigenes Benutzermanagement-System inkludieren.
Nach der Inbetriebnahme muss der Safe in den operativen Betrieb übergehen.

3.4.2 AUTHENTISIERUNG DES BENUTZERS

Ein RFID-Lesegerät muss am Safe verbaut sein. Der Safe muss über die Hardware Abstraction Layer mit dem RFID-Lesegerät kommunizieren können. Nach dem erfolgreichen Auslesen einer vor dem RFID-Lesegerät platzierten RFID-Karte, muss die ausgelesene Benutzerkennung mit denen der aktiven Benutzer verglichen werden. Existiert für die eingescannte Benutzer-Kennung ein gespeicherter Eintrag, wird der Benutzer zur Eingabe des persönlichen Passworts aufgefordert. Stimmt dieses, mit dem für den Benutzer gespeicherten Passwort überein, wird der Benutzer angemeldet. Ein entsprechender Log-Eintrag wird gespeichert. Zur Eingabe des Passwortes muss am Safe ein Eingabepanel verbaut sein, dass ein entsprechendes User-Interface bereitstellt.
Für den Fall, dass es sich bei der Kennung um keine bekannte Benutzer-Kennung handelt, muss der Anmeldeprozess abgebrochen werden. Zu der Überprüfung der Benutzer-Kennung sowie zu der Überprüfung des eingegebenen Passwortes muss die zu entwickelnde Lösung ein eigenes Benutzermanagement-System beinhalten.
Im Falle der mehrmaligen (dreimal) falschen Eingabe des persönlichen Passwortes, muss ein Alarm ausgelöst werden.
In beiden Fehlerfällen soll eine entsprechende Warnung in die Liste der gespeicherten Log-Einträge aufgenommen werden. Zum Speichern der Log-Einträge muss der im Safe verbaute Rechner eine Speichereinheit beinhalten und ein Datenbankmanagement-System zur Verfügung stellen.

3.4.3 AUSLÖSEN EINES ALARMS

Sicherheitsbeeinträchtigende Zustände sollen einen Alarm auslösen. Im Falle eines Alarms blinken die fünf (5) LEDs, am oberen Rand des Safes, rot und ein Signalton ertönt. Im Safe müssen dementsprechend fünf RGB LEDs sowie ein Lautsprecher verbaut sein. Um die Aktivierung und Deaktivierung der LEDs sowie des Lautsprechers zu ermöglichen, muss die zu entwickelnde Lösung eine Hardware Abstraction Layer inkludieren, über die die Kommunikation mit der verbundenen Hardware erfolgt.
Die Deaktivierung des Alarms soll durch die Authentisierung eines Systemadministrators erfolgen.

3.4.4 SPEICHERN DER ZUTRITTSVERSUCHE

Alle sicherheitsrelevanten Vorgänge am System müssen in Form eines Log-Eintrags gespeichert werden. Die Einträge sollen in einem von dem, im Safe verbauten Rechner, zur Verfügung gestellten Datenbankmanagement-System gespeichert werden. Fehlgeschlagene Vorgänge müssen durch eine entsprechende Warnung gekennzeichnet werden. Die Integrität der gespeicherten Log-Einträge muss zu jedem Zeitpunkt gewährleistet sein. Bereits gespeicherte Log-Einträge dürfen nicht verändert werden können.
Die Verwaltung der Log-Einträge soll über ein eigenes Logmanagement-System erfolgen.

3.4.5 BEANTRAGEN NEUER WIEDERHERSTELLUNGS-CODES

Systemadministratoren sollen die Möglichkeit haben neue Wiederherstellungs-Codes zu beantragen. Das System generiert infolgedessen acht (8) neue Wiederherstellungs-Codes, zeigt diese dem Benutzer an und speichert sie. Durch diesen Prozess werden alle alten Wiederherstellungs-Codes invalidiert. Die Wiederherstellung des operativen Betriebs ist nunmehr

durch einen der neuen Wiederherstellungs-Codes möglich.
Die Verwaltung der Wiederherstellungs-Codes soll durch ein eigenes Wiederstellungsmanagement-System erfolgen. Das Speichern der Wiederherstellungs-Codes setzt ein im System integriertes Datenbankmanagement-System, basierend auf einer entsprechenden Speichereinheit, voraus.

3.4.6 AUF WERKSZUSTAND ZURÜCKSETZEN

Alle gespeicherten Daten, mit Ausnahme der gespeicherten Log-Einträge, müssen durch das Zurücksetzen auf den Werkszustand gelöscht werden. Zusätzlich muss sich der Safe nach dem Zurücksetzen in einem gesperrten Zustand befinden. Die Reaktivierung des Safes darf nur durch die Eingabe eines gültigen Wiederherstellungs-Codes möglich sein.
Bei einer Unterbrechung der Stromversorgung, muss der Safe automatisch auf den Werkszustand zurückgesetzt werden. Die Stromversorgung des Safes muss für die Dauer des Zurücksetzens, mithilfe einer entsprechend dimensionierten USV, gegeben sein.

3.4.7 ENTRIEGELN

Aktive, autorisierte, Benutzer sollen die Möglichkeit haben die Entriegelung des Safes zu beantragen. Findet diese statt, hat der Benutzer 30 Sekunden lang die Möglichkeit die Safe-Türe zu öffnen. Passiert dies nicht, wird der Safe verriegelt und der Benutzer automatisch abgemeldet.
Die Kommunikation der zu entwickelnden Lösung, mit dem elektronischen Verriegelungsmechanismus, erfolgt über die integrierte Hardware Abstraction Layer.
Zutritte sollen in einer integren Liste gespeichert werden. (siehe Punkt 3.4.4.) Der aktuelle Verriegelungsstatus muss dem Benutzer jederzeit entsprechend signalisiert werden. (siehe Punkt 3.4.18.)
Begehbare Safes sollen im Inneren mit einem Notfall-Taster ausgestattet werden. Wird dieser betätigt, soll der Safe sofort entriegelt werden.

3.4.8 ABFRAGEN DER LOG-EINTRÄGE

Systemadministratoren sollen nach der erfolgreichen Authentisierung die Möglichkeit haben alle gespeicherten Log-Einträge abzufragen. Die Verwaltung der Log-Einträge erfolgt über ein eigenes Logmanagement-System.
Die Abfrage selbst soll in Form eines Log-Eintrags gespeichert werden. (siehe Punkt 3.4.4.)

3.4.9 ADMINISTRATION ÜBER SEPARATE SCHNITTSTELLE

Dem Auftraggeber, sowie Systemadministratoren des Endkunden, soll über eine REST-Schnittstelle die am Eingabepanel gegebene Funktionalität geboten werden. Anfragen dürfen nur unter Mitsenden eines gültigen Benutzer-Tokens verarbeitet werden. (siehe Punkt 3.4.12.)
Anfragen an die REST-Schnittstelle sollen als Log-Einträge gespeichert werden. (siehe Punkt 3.4.4.)

3.4.10 ABMELDEN

Ein angemeldeter Benutzer soll über das Eingabepanel, sowie die REST-Schnittstelle, die Möglichkeit haben sich abzumelden. Durch die Abmeldung muss der aktuelle Benutzer-Token invalidiert werden. Die Interaktion mit dem System darf nach der erfolgreichen Abmeldung nicht mehr möglich sein.

3.4.11 OPERATIVEN BETRIEB WIEDERHERSTELLEN

Sobald der Safe im gesperrten Zustand mit Strom versorgt wird, muss dieser am Eingabepanel ein Feld zur Eingabe eines Wiederherstellungs-Codes anzeigen. Wird in dieses Feld ein gültiger Wiederherstellungs-Code eingegeben, muss der Safe entsperrt und für aktive Benutzer wieder bedienbar werden.
Zur Eingabe des Wiederherstellungs-Codes muss an dem Safe ein Eingabepanel verbaut sein.
Die Validierung des eingegebenen Wiederherstellungs-Codes soll über ein eigenes Wiederherstellungsmanagement-System erfolgen. (siehe Punkt 3.4.5.)

3.4.12 VALIDIEREN DES BENUTZER-TOKENS

Meldet sich ein Benutzer an dem System an, soll dieser ein Benutzer-Token erhalten. Vor dem Ausführen einer, von dem Benutzer angeforderten, Operation, muss die Gültigkeit des mitgesendeten Tokens bestimmt werden. Handelt es sich um einen validen Benutzer-Token, wird die angeforderte Operation ausgeführt. Konnte die Gültigkeit nicht nachgewiesen werden, muss der Vorgang abgebrochen werden.
Die zu entwickelnde Lösung soll die Authentifizierung über ein Benutzer-Token unterstützen und in der Lage sein, Sitzungen über dieses zu validieren.

3.4.13 VERRIEGELUNG AKTIVIEREN-DEAKTIVIEREN

Die Verriegelung des Safes soll elektronisch erfolgen. Diese soll über das Eingabepanel sowie die REST-Schnittstelle aktiviert beziehungsweise deaktiviert werden können. Diese Funktion darf nur von einem Systemadministrator ausgeführt werden, es darf daher auf keinen Fall möglich sein, dass ein normaler Benutzer Zugriff auf dies Funktion hat. (siehe Punkt 3.2.12.)
Im Safe soll ein Sensor verbaut sein, der den Zustand der Türe bestimmt. Die Verriegelung soll nur im Falle der geschlossenen Safe-Türe deaktiviert werden können. Die Kommunikation der zu entwickelnden Lösung, mit dem elektronischen Verriegelungsmechanismus und dem Türsensor, soll über die Hardware Abstraction Layer erfolgen.
Das Speichern des Verriegelungsstatus erfordert ein Datenbankmanagementsystem.

3.4.14 BENUTZER INAKTIV STELLEN

Die Anzeige der zutrittsberechtigten Personen soll übersichtlich am Panel dargestellt werden (sortiert nach Berechtigungsstatus). Das inaktiv Stellen eines inaktiven Benutzers wird dadurch verhindert, dass in dieser Liste nur alle aktiv Zutrittsberechtigte angezeigt werden.
Die Abfrage der aktiven Benutzer, sowie das inaktiv stellen eines Benutzers, erfordert die Integration eines eigenen Benutzermanagement-Systems. Das Speichern von Benutzerdaten erfordert das Vorhandensein einer Speichereinheit in dem verbauten Rechner, sowie die Integration eines entsprechenden Datenbankmanagement-Systems.
Um die Benutzer-Referenzen der gespeicherten Daten konsistent zu halten, werden Benutzer nicht gelöscht, sondern inaktiv gestellt.

3.4.15 BENUTZER AKTIV STELLEN

Die Liste der nicht zutrittsberechtigten Personen soll übersichtlich am Panel dargestellt werden. Sobald der angemeldete Benutzer einen inaktiven Benutzer zur Reaktivierung ausgewählt hat, erhält dieser wieder Zugriff zu dem System. Das aktiv-stellen eines aktiven Benutzers wird dadurch verhindert, dass in dieser Liste nur alle inaktive Zutrittsberechtigte angezeigt werden. (siehe Punkt 3.4.14.)

3.4.16 BENUTZER ERSTELLEN

Systemadministratoren müssen die Möglichkeit haben neue Benutzer anzulegen. Das Erstellen von neuen Benutzern erfordert ein entsprechendes Benutzermanagement-System. Die Daten werden persistent in einem, auf dem integrierten Speicher des Rechners, laufendem Datenbankmanagement-System gespeichert.
Bereits zugewiesene RFID-Karten dürfen nicht erneut zugewiesen werden. Der neue Benutzer muss im System abgespeichert werden und je nach Berechtigungsstatus muss es ihm der Zugang zu dem Safe gestattet werden. (siehe Punkt 3.4.12.)

3.4.17 PERSÖNLICHES PASSWORT ÄNDERN

Jeder aktive, zutrittsberechtigte Benutzer sollte die Möglichkeit haben sein persönliches Passwort zu ändern. Vor dem Ändern des Passwortes muss die Gültigkeit der aktuellen Benutzer-Sitzung überprüft werden. Dabei ist zu beachten, dass das neue Passwort die formalen Anforderungen erfüllen muss. Das Ändern des persönlichen Passwortes soll über das integrierte Benutzermanagement-System erfolgen. Die Daten werden persistent in einem, auf dem integrierten Speicher des Rechners, laufendem Datenbankmanagement-System gespeichert.

3.4.18 SIGNALISIEREN DES VERRIEGELUNGSSTATUS

Auf der Vorderseite des Safes sollen fünf RGB LEDs verbaut sein. Die Ansteuerungen der, im Safe verbauten, LEDs muss im Rahmen dieses Use-Cases geschehen. Diese soll über eine integrierte Hardware Abstraction Layer erfolgen. Bei einer Änderung des Verriegelungszustandes muss dementsprechend auch die Farbe der verbauten LEDs angepasst werden.

3.4.19 VERRIEGELN

Befindet sich der Safe in einem entriegelten Zustand, soll ein angemeldeter Benutzer die Möglichkeit haben diesen zu verriegeln. (siehe Punkt 3.4.12.) Da die elektronische Verriegelung nur möglich ist, wenn die Türe des Safes geschlossen ist, soll der Zustand über einen entsprechenden Sensor überwacht werden. Dieser muss für diesen Use-Case berücksichtigt werden.
Die Kommunikation der zu entwickelnden Lösung mit dem Tür-Sensor sowie dem elektronischen Verriegelungsmechanismus, soll über eine integrierte Hardware Abstraction Layer erfolgen.
Der aktuelle Verriegelungsstatus muss jederzeit entsprechend signalisiert werden. (siehe Punkt 3.4.18.)

3.5 Einschränkungen

Anfragen, die über das Eingabepanel oder die REST-Schnittstelle an das System gesendet werden, sollen eine maximale Antwort-Zeit von einer Sekunde haben. Verzögerungen durch zusätzliche Netzwerkkomponenten, wie Gateways, Firewalls, etc. werden bei dieser Angabe nicht berücksichtigt.

Der Zugang zum System, soll nur autorisierten Benutzern erlaubt sein. Um dem Auftraggeber die Administration des Systems, auch nach der Inbetriebnahme bei dem Endkunden zu ermöglichen, existiert zu jeder Zeit ein vordefinierter Benutzer mit dem Status eines Systemadministrators. Die Benutzer-Kennung, dieses Benutzers, entspricht 64-mal der Zahl Null (0).
Bei der Umsetzung der zu entwickelnden Lösung ist besonders auf die Integrität des Systems zu achten.

Die Absicherung des physikalischen Zugangs zum System, sowie die Absicherung des jeweiligen Netzwerkes, über das auf die REST-Schnittstelle zugegriffen werden kann, liegt in der Verantwortung des Endkunden.

Die Kommunikation mit der bereitgestellten REST-Schnittstelle erfolgt über das Kommunikationsprotokoll HTTPS (Hypertext Transfer Protocol Secure), welches eine Transportverschlüsselung darstellt.

Das Speichern von betriebsrelevanten Daten erfolgt in einer Datenbank. Als Datenbankmanagementsystem kommt PostgreSQL zum Einsatz. Die Installation und Konfiguration dessen obliegt der Verantwortung des Auftraggebers. Von Seiten des Auftragnehmers wird eine empfohlene Konfiguration des Datenbankmanagementsystems definiert.

Die vom System gespeicherten Daten sollen zu jedem Zeitpunkt vor dem Zugriff durch unbefugte Dritte geschützt werden. Weiters sollen die gespeicherten Daten nur von aktiven Benutzern mit entsprechenden Berechtigungen eingesehen und verändert werden können. Spezielle Daten, wie die gespeicherten Log-Einträge, sollen unter keinen Umständen verändert werden können.

Die zu entwickelnde Lösung kann auf allen Hardware-Systemen, die den im Punkt 2.3. definierten Anforderungen entsprechen, bereitgestellt werden. Sicherheitsverstöße, die durch Fehler in der Hardware beziehungsweise dem Safe selbst auftreten, können durch die Lösung nicht verhindert werden. Die Verantwortung für derartige Vorfälle obliegt demnach nicht dem Auftragnehmer.
Der Auftragnehmer übernimmt keine Verantwortung für Sicherheitsverstöße sowie weitere Probleme, die auf Systemen, mit, der von dem Auftragnehmer empfohlener Hardware, abweichender Hardware, auftreten.

Die zu entwickelnde Lösung soll eine Verfügbarkeit von 99.9% bieten. Der Prozentsatz beschreibt hierbei die prozentuelle Dauer pro Jahr, für die sich der Safe im operativen Betrieb befindet. Ausfälle, die durch eine Unterbrechung der Stromversorgung, Fehler in der Bedienung oder eventuelle manuelle Abschaltungen verursacht werden, obliegen der Verantwortung des Endkunden und werden von der angegebenen Verfügbarkeit nicht berücksichtigt.

Damit das System keine Gefahr für die physische sowie psychische Gesundheit eines Benutzers darstellt, kann die Safe-Türe nur manuell geschlossen werden. Die Verriegelung kann erst stattfinden, sobald die Türe des Safes vollständig geschlossen ist.
Weiters ist bei begehbaren Safes ein Notfall-Taster im Inneren des Safes angebracht, bei dessen Betätigung der Safe sofort entriegelt wird. Durch diesen Mechanismus soll das Einschließen von Personen im Safe verhindert werden.

Das System bietet über das, auf der Vorderseite des Safes verbaute, Eingabepanel ein eigenes User Interface, um den Safe zu steuern. Außerdem bietet das System dem Auftraggeber sowie Systemadministratoren des Endkunden die Möglichkeit den Safe über eine REST-Schnittstelle zu steuern.
Eine Dokumentation zur Nutzung des User Interfaces sowie der REST-Schnittstelle, wird im Rahmen des Übergabe-Termins bereitgestellt.

Es liegt in der Verantwortung des Kunden beziehungsweise Endkunden, Benutzer des Systems auf die Speicherung personenbezogener Daten, durch das System, aufmerksam zu machen und diese entsprechend zu informieren.

4 VERPFLICHTUNGEN DES KUNDEN

Der Kunde verpflichtet sich, sowohl in der Phase der Konzeptionierung als auch während der Entwicklung, den Prozess mit entsprechend technisch geschulten und mit dem Projekt vertrauten Mitarbeitern zu betreuen.
Im Rahmen dessen verpflichtet sich der Kunde bei den, in Punkt 2.4. beschriebenen Abstimmungs-Terminen sowie dem Übergabe-Termin vertreten zu sein.

Weiters verpflichtet sich der Kunde dem Auftragnehmer, für des Projektes, ein realitätsnahes Test-System, inklusive der entsprechenden Dokumentation, zur Verfügung zu stellen. Das Test-System muss die Anforderungen, die im Rahmen des Projektes an die Hardware sowie Software gestellt werden, erfüllen. Dieses Test-System wird vom Auftragnehmer, bei Abschluss der Entwicklungsphase, zum Nachweis der vollständigen Erfüllung aller definierten funktionalen Anforderungen, genutzt.

5 VERWEISE AUF ANDERE DOKUMENTE

Die Definitionen, der Anforderungen des Auftraggebers, können in dem Dokument `Angabe_TRAD.pdf` gefunden werden.

Informationen zu dem Gesamtsystem, der Layer UI, der Layer BO und der Layer Data können dem Dokument `TRAD-Gruppe-2_Safe-RFID_SDD.pdf` entnommen werden.

6 ANNEX

Die originalen UML-Diagramme sind in der Datei `UML_Diagramm.mdj` enthalten.

Ein Export des Domänenmodells kann in der Datei `UML_Domaenenmodell.png` gefunden werden.

Weiters sind folgende Exporte der UML-Diagramme angehängt:

- Use-Case-Diagramm.png
- Inbetriebnahme_Sequenzdiagramm.png
- Authentisierung_des_Benutzers_Sequenzdiagramm.png
- Ausloesen_eines_Alarms_Sequenzdiagramm.png
- Speichern_der_Zutrittsversuche_Sequenzdiagramm.png
- Beantragen_neuer_Wiederherstellungs-Codes_Sequenzdiagramm.png
- Auf_Werkszustand_zuruecksetzen_Sequenzdiagramm.png
- Entriegeln_Sequenzdiagramm.png
- Abfragen_der_Log-Eintraege_Sequenzdiagramm.png
- Administration_ueber_separate_Schnittstelle_Sequenzdiagramm.png
- Abmelden_Sequenzdiagramm.png
- Operativen_Betrieb_wiederherstellen_Sequenzdiagramm.png
- Validieren_des_Benutzer-Tokens_Sequenzdiagramm.png
- Verriegelung_aktivieren-deaktivieren_Sequenzdiagramm.png
- Benutzer_inaktiv_stellen_Sequenzdiagramm.png
- Benutzer_aktiv_stellen_Sequenzdiagramm.png
- Benutzer_erstellen_Sequenzdiagramm.png
- Persoenliches_Passwort_aendern_Sequenzdiagramm.png
- Signalisieren_des_Verriegelungsstatus_Sequenzdiagramm.png
- Verriegeln_Sequenzdiagramm.png

7 DEFINITION VON BEGRIFFLICHKEITEN

Kunde	Der Begriff „Kunde“ beschreibt den Auftraggeber.
System	„System“ beschreibt die Kombination aus der verwendeten Hardware (= der Safe) und der zu entwickelnden Lösung (= Safe RFID).
Lösung	Der Begriff „Lösung“ beschreibt die, im Rahmen des Auftrags, zu entwickelnde Software, um einen Safe steuern zu können.