- Systemanalyse -

Lastenheft für „Geheime Kommunikation mit Quantenkryptographie - eine Lernsoftware zum Verstehen der Grundlagen“

Version: 1.0

|  |  |  |
| --- | --- | --- |
| Projektbezeichnung | QuaKrypto | |
| Projektleiter | Simon Schisslbauer | |
| Verantwortlich | Team | |
| Erstellt am | 30.03.2023 | |
| Zuletzt geändert | 24.04.2023 20:38 | |
| Bearbeitungszustand |  | in Bearbeitung |
| X | vorgelegt |
|  | fertig gestellt |
| Dokumentablage | Main-Branch im Projekt | |

Änderungsverzeichnis

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Änderung | | | Geänderte Kapitel | Beschreibung der Änderung | Autor | Zustand |
| Nr. | Datum | Version |
| 1 |  | 1.0 | Alle | Initiale Produkterstellung |  |  |

Prüfverzeichnis

Die folgende Tabelle zeigt einen Überblick über alle Prüfungen – sowohl Eigenprüfungen wie auch Prüfungen durch eigenständige Qualitätssicherung – des vorliegenden Dokumentes.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Datum | Geprüfte Version | Anmerkungen | Prüfer | Neuer Produktzustand |
| 24.04.2023 | 1.0 | Überprüfung nach Prüfprotokoll | Jonas Hammer | 1.0 |

Inhalt

[1 Einleitung 4](#_Toc34239361)

[2 Ausgangssituation und Zielsetzung 4](#_Toc34239362)

[3 Funktionale Anforderungen 5](#_Toc34239363)

[3.1 Use-Case Übersicht 5](#_Toc34239364)

[3.2 Use-Beschreibungen 5](#_Toc34239365)

[3.3 (Sonstige) Funktionalität 7](#_Toc34239366)

[3.4 Modell des Problembereichs (Konzeptionelles Datenmodell) 7](#_Toc34239367)

[4 Nicht-Funktionale Anforderungen 7](#_Toc34239368)

[4.1 Benutzbarkeit (Usability) 7](#_Toc34239369)

[4.2 Zuverlässigkeit (Reliability) 8](#_Toc34239370)

[4.3 Leistung (Performance) 8](#_Toc34239371)

[4.4 Unterstützbarkeit (Supportability) 9](#_Toc34239372)

[4.5 Sonstige Einschränkungen 9](#_Toc34239373)

[5 Risikoakzeptanz 10](#_Toc34239374)

[6 Skizze der Gesamtsystemarchitektur 10](#_Toc34239375)

[7 Lieferumfang 11](#_Toc34239376)

[8 Abnahmekriterien 11](#_Toc34239377)

[9 Glossar 11](#_Toc34239378)

[10 Abkürzungsverzeichnis 12](#_Toc34239379)

[11 Literaturverzeichnis 12](#_Toc34239380)

[12 Abbildungsverzeichnis 12](#_Toc34239381)

# Einleitung

Dieses Dokument enthält alle an das zu entwickelnde System gestellten Anforderungen. Die Gliederung orientiert sich am Aufbau des V-Modell-XT®[[1]](#footnote-2)-Produkts „Anforderungen (Lastenheft)“, ist jedoch zur Verwendung für die Veranstaltung **„Software-Projekte“** in Informatik-Curricula der **OTH-Amberg-Weiden** angepasst worden (und nicht konform zum V-Modell-XT): Teilnehmer dieser Veranstaltung erhalten von ihrem „Auftraggeber“ lediglich einen Überblick über das gewünschte System, was ungefähr dem Thema „Ausgangssituation und Zielsetzung“ in diesem Dokument entspricht; die Anforderungen müssen die Teilnehmer dann in enger Abstimmung mit ihrem „Auftraggeber“ selbst erarbeiten und in diesem Dokument niederlegen. Dadurch sollen sie Gelegenheit erhalten, auch Tätigkeiten der System-Analyse intensiver zu üben. Die „Auftraggeberseite“ liefert also nicht – wie im V-Modell-XT vorgesehen - das komplette Lastenheft, aus dem die „Auftragnehmerseite“ ein separates Pflichtenheft ableitet; stattdessen wird das hier vorliegende Dokument vom studentischen Entwicklerteam zur Dokumentation der Analyse-Ergebnisse erstellt und zugleich als Ersatz für die im V-Modell-XT vorgesehenen Dokumente Lasten- und Pflichtenheft verwendet.

Kern dieses Dokuments sind die funktionalen und nicht-funktionalen Anforderungen an das System, sowie eine Skizze des Gesamtsystementwurfs. Der Entwurf berücksichtigt die zukünftige Umgebung und Infrastruktur, in der das System später betrieben wird, und gibt Richtlinien für Technologieentscheidungen. Ebenfalls Teil der Anforderungen ist die Festlegung von Lieferbedingungen und Abnahmekriterien.

Die funktionalen und nicht-funktionalen Anforderungen dienen nicht nur als Vorgaben für die Entwicklung, sondern sind zusätzlich Grundlage der Anforderungsverfolgung und des Änderungsmanagements. Die Anforderungen sollten so aufbereitet sein, dass die Verfolgbarkeit (Traceability) sowie ein geeignetes Änderungsmanagement für den gesamten Lebenszyklus eines Systems möglich sind.

Im Allgemeinen sollten keine technischen Lösungen vorgegeben werden, um Architekten und Entwickler bei der Suche nach optimalen technischen Lösungen nicht einzuschränken.

# Ausgangssituation und Zielsetzung

Das BB84-Protokoll ist ein Verschlüsselungsverfahren, das auf den Prinzipien der Quantenphysik basiert und in der modernen Kryptografie bekannt ist. Viele Menschen haben jedoch Schwierigkeiten, die grundlegenden Konzepte der Quantenphysik und ihre Anwendung auf das BB84-Protokoll zu verstehen. Hier kann eine Lern- und Experimentiersoftware helfen, das Verständnis zu fördern und ein solides Wissen aufzubauen.

Zielsetzung:

Ziel dieser Lern- und Experimentiersoftware ist es, den Benutzergruppen ein grundlegendes Verständnis der Quantenphysik und des BB84-Protokolls zu vermitteln. Durch ausgewählte Übungsszenarien soll die Benutzergruppe die grundlegenden Konzepte der Quantenphysik verstehen und lernen, wie diese in der Quantenkryptografie angewendet werden können. Am Ende des Lernprozesses soll die Benutzergruppe in der Lage sein, das BB84-Protokoll zu verstehen, seine Funktionsweise zu erklären und seine Anwendungen in der Praxis zu erkennen.

Folgende Elemente sollen in die Lern- und Experimentiersoftware integriert werden:

Frei konfigurierbares Wiki:

Die Software soll eine Einführung in die Quantenphysik und das BB84-Protokoll enthalten, um den Benutzergruppen eine Grundlage zu bieten, auf der sie aufbauen können. Dies kann mithilfe von Text, Diagrammen oder Videos erfolgen.

Interaktive Übungsszenarien:

Die Software soll interaktive Übungsszenarien enthalten, die den Benutzergruppen ermöglichen, die grundlegenden Konzepte der Quantenphysik und ihre Anwendung auf das BB84-Protokoll zu erleben und zu verstehen. Die Benutzergruppe kann auf Rollen verteilt (als Alice, Bob und/oder Eve) an den Übungsszenarien teilnehmen. Das Wissen jeder einzelnen Rolle soll dabei für die restlichen Teilnehmer gesperrt werden.

Feedback/Aufzeichnung:

Die Software soll die Abarbeitung der Übungsszenarien protokollieren, damit die Benutzergruppen ihre Fortschritte und ihr Verständnis des Konzeptes/Protokolls verfolgen/auswerten können. Dies geschieht nach der Vollendung des Übungsszenarios, da das System keine aktive Hilfestellung während der Abarbeitung geben soll. Es sind somit auch Fehler seitens der Benutzergruppe bei der Ausführung erlaubt, um einen Lerneffekt hervorzurufen.

Anpassungsfähigkeit:

Die Software sollte an die unterschiedlichen Quantenkryptographie-Protokolle (u.a. Ekert-Protokoll) anpassbar sein.

Netzwerkfähigkeit:

Die Software soll netzwerkfähig sein, sodass eine gemeinsame Durchführung der Übungsszenarien auf verschiedenen Rechnern im lokalen Netzwerk möglich ist.

# Funktionale Anforderungen

## Use-Case Übersicht



## Use-Beschreibungen

|  |  |  |
| --- | --- | --- |
| **Erstellen einer Lobby** | | |
| **Kennung** | | UC-1 |
| **Priorität** | | Hoch |
| **Kurzbeschreibung:** | | |
| Eine Benutzergruppe wählt:   * das Protokoll, das sie durch das System erlernen will * ob das Übungsszenario lokal oder netzwerkbasiert durchgeführt werden soll * die gewünschte Variante * die gewünschte(n) Phase(n) * den gewünschten Schwierigkeitsgrad   im Lobbykonfigurationsmenü aus. | | |
| **Vorbedingung(en):** | | |
| * Die Benutzergruppe befindet sich im Hauptmenü | | |
| **Nachbedingung(en):** | | |
| * Eine Lobby wurde erstellt * Das System öffnet die erstellte Lobby | | |
| **Normaler Ablauf:** | | |
|  | 1. Der Anwendungsfall beginnt, wenn die Benutzergruppe im Hauptmenü auswählt, dass sie eine Lobby erstellen will 2. Die Benutzergruppe wählt das Protokoll aus, welches sie durch das System erlernen will 3. Die Benutzergruppe wählt aus, ob das Übungsszenario lokal oder netzwerkbasiert bearbeitet werden soll 4. Die Benutzergruppe wählt die gewünschte Variante aus 5. Die Benutzergruppe wählt die gewünschte(n) Phase(n) des Protokollablaufs aus 6. Die Benutzergruppe wählt den gewünschten Schwierigkeitsgrad aus 7. Die Benutzergruppe bestätigt ihre Eingaben 8. Das System prüft, ob die Eingaben der Benutzergruppe gültig sind 9. Das System übernimmt die Eingabedaten und erstellt eine Lobby   **Ende**. | |
| **Ablauf-Varianten:** | | |
| 7a | Die Eingaben der Benutzergruppe sind ungültig | |
|  | 1. Das System weist die Benutzergruppe auf die ungültigen Eingaben hin   **Rückkehr nach:** 2 | |
| 8a | Die Benutzergruppe hat die netzwerkbasierte Bearbeitung für das Übungsszenario gewählt | |
|  | 1. Das System legt eine netzwerkbasierte Lobby an   **Ende.** | |
| 8b | Die Benutzergruppe hat die lokale Bearbeitung für das Übungsszenario gewählt | |
|  | 1. Das System legt eine lokale Lobby an   **Ende.** | |
| **Spezielle Anforderungen:** | | |
|  | | |
| **Zu klärende Punkte:** | | |
| Zu 7a: Alle Eingaben werden akzeptiert, allerdings Unvollständigkeit lässt „Lobby erstellen“ Button ausgegraut | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Beitritt zu einer lokalen Lobby** | | | |
| **Kennung** | | | UC-2 |
| **Priorität** | | | Hoch |
| **Kurzbeschreibung:** | | | |
| Die Benutzergruppe tritt einer vorhandenen, lokalen Lobby bei.  Dabei legt sie…   * ihre Rolle(n) * ihren Alias * ihr Passwort   fest.  Jede im Übungsszenario vorhandene Rolle (Alice, Bob, Eve) muss von genau einer Benutzergruppe repräsentiert werden. | | | |
| **Vorbedingung(en):** | | | |
| * Eine lokale Lobby wurde erstellt * Das System befindet sich in der Lobby | | | |
| **Nachbedingung(en):** | | | |
| * Die Benutzergruppe ist der Lobby beigetreten | | | |
| **Normaler Ablauf:** | | | |
|  | | 1. Der Anwendungsfall beginnt, wenn die Benutzergruppe die Aktion ausführt einer vorhandenen Lobby beizutreten 2. Die Benutzergruppe wählt mindestens eine der noch vorhandenen Rollen aus 3. Die Benutzergruppe legt ihren Alias fest 4. Die Benutzergruppe legt ihr Passwort fest 5. Das System prüft, ob die Eingaben gültig sind   **Ende**. | |
| **Ablauf-Varianten:** | | | |
| 5a | Die Eingaben der Benutzergruppe sind ungültig | | |
|  | 1. Das System weist die Benutzergruppe auf die ungültigen Eingaben hin   **Rückkehr nach:** 2 | | |
| 5b | Die Eingaben der Benutzergruppe sind gültig | | |
|  | 1. Das System sperrt die Auswahl der gewählten Rolle(n) für andere Benutzergruppen   **Ende.** | | |
| **Spezielle Anforderungen:** | | | |
|  | | | |
| **Zu klärende Punkte:** | | | |
|  | | | |

|  |  |  |
| --- | --- | --- |
| **Beitritt zu einer netzwerkbasierten Lobby** | | |
| **Kennung** | | UC-3 |
| **Priorität** | | Mittel |
| **Kurzbeschreibung:** | | |
| Die Benutzergruppe tritt einer vorhandenen, netzwerkbasierten Lobby bei.  Dabei legt sie…   * die gewünschte Lobby * ihre Rolle(n) * ihren Alias * ihr Passwort   fest.  Jede im Übungsszenario vorhandene Rolle (Alice, Bob, Eve) muss von genau einer Benutzergruppe repräsentiert werden. | | |
| **Vorbedingung(en):** | | |
| * Im selben Netzwerk wurde mindestens eine netzwerkbasierte Lobby erstellt * Die Benutzergruppe befindet sich im Lobbyauswahlmenü | | |
| **Nachbedingung(en):** | | |
| * Die Benutzergruppe ist der Lobby beigetreten | | |
| **Normaler Ablauf:** | | |
|  | 1. Der Anwendungsfall beginnt, wenn die Benutzergruppe die gewünschte Lobby im Lobbyauswahlmenü ausgewählt hat 2. Das System prüft, ob die Lobby weiterhin verfügbar ist 3. Die Benutzergruppe wird zur gewünschten Lobby hinzugefügt 4. Die Benutzergruppe wählt mindestens eine der noch vorhandenen Rollen aus 5. Das System sperrt die Auswahl der gewählten Rolle(n) für andere Benutzergruppen 6. Die Benutzergruppe legt ihren Alias fest 7. Die Benutzergruppe legt ihr Passwort fest 8. Das System prüft, ob die Eingaben gültig sind   **Ende**. | |
| **Ablauf-Varianten:** | | |
| 3a | Die ausgewählte Lobby ist nicht mehr existent | |
|  | 1. Das System weist die Benutzergruppe darauf hin, dass die angegebene Lobby nicht gefunden werden konnte   **Rückkehr nach**: 2 | |
| 8a | Die Eingaben sind ungültig | |
|  | 1. Das System weist die Benutzergruppe darauf hin, dass die Eingaben ungültig sind   **Rückkehr nach**: 6 | |
| **Spezielle Anforderungen:** | | |
| Das System lässt mehr Benutzergruppen als Rollen in dem Lobby Screen zu. Sobald das Übungsszenario aber gestartet wird, werden Benutzergruppen ohne Rolle ins Hauptmenü zurückbefördert | | |
| **Zu klärende Punkte:** | | |
|  | | |

|  |  |  |
| --- | --- | --- |
| **Bearbeitung eines Übungsszenarios** | | |
| **Kennung** | | UC-4 |
| **Priorität** | | Hoch |
| **Kurzbeschreibung:** | | |
| Alle vorhandenen Rollen durchlaufen die ihnen zugeordneten Handlungsschritte. | | |
| **Vorbedingung(en):** | | |
| * Eine Lobby wurde erstellt * Jede in der Lobby vorhandene Rolle ist von genau einer Benutzergruppe belegt | | |
| **Nachbedingung(en):** | | |
| * Eine Aufzeichnung der Bearbeitung des Übungsszenarios wurde erstellt | | |
| **Normaler Ablauf:** | | |
|  | 1. Der Anwendungsfall beginnt, wenn der Lobbyhost das Übungsszenario startet 2. Das System initialisiert das Übungsszenario und die Aufzeichnung des Übungsszenarios 3. Der aktiven Rolle werden dem Zug entsprechende Handlungsschritte angezeigt 4. Die aktive Rolle führt die gewünschten Handlungsschritte aus 5. Das System speichert die Bearbeitung des aktuellen Zuges in der Aufzeichnung ab 6. Die Rolle bestätigt das Ende ihres Zuges durch einen entsprechenden Handlungsschritt 7. Das System gibt die Steuerung für die nächste Rolle frei 8. Dieser Vorgang (Schritte 3 bis 8) wird so lange wiederholt, bis die aktuelle Phase abgeschlossen wurde 9. Dieser Vorgang (Schritte 3 bis 9) wird so lange wiederholt, bis die letzte durch den Lobbyhost ausgewählte Phase abgeschlossen wurde   **Ende**. | |
| **Ablauf-Varianten:** | | |
| 3a | Es handelt sich um ein lokales Übungsszenario, wobei mindestens zwei Benutzergruppen existieren | |
|  | 1. Die Rolle entsperrt vor ihrem Zug ihre Informationen und ihre Handlungsschritte mit ihrem Passwort   **Rückkehr nach**: 4 | |
| 6a | Es handelt sich um ein lokales Übungsszenario, wobei mindestens zwei Benutzergruppen existieren | |
|  | 1. Das System sperrt die Informationen und Handlungsschritte der jeweiligen Rolle   **Rückkehr nach**: 7 | |
| **Spezielle Anforderungen:** | | |
|  | | |
| **Zu klärende Punkte:** | | |
| Dieser Use-Case ist implementiert, aber in der Analysebeschreibung müssen die Ablaufvarianten gestrichen werden, da es hier keinen Unterschied zwischen lokaler und netzwerkbasierter Bearbeitung gibt | | |

|  |  |  |
| --- | --- | --- |
| **Einsicht in einen Wiki-Eintrag** | | |
| **Kennung** | | UC-5 |
| **Priorität** | | Gering |
| **Kurzbeschreibung:** | | |
| Um ihr Wissen und ihre Kenntnisse zu vertiefen, soll die Benutzergruppe ein Wiki mit Informationen über das Protokoll einsehen können. | | |
| **Vorbedingung(en):** | | |
| * Es existiert ein Wiki | | |
| **Nachbedingung(en):** | | |
| * Der Wiki-Eintrag wird der Benutzergruppe angezeigt | | |
| **Normaler Ablauf:** | | |
|  | 1. Der Anwendungsfall beginnt, wenn die Benutzergruppe die Aktion zum Öffnen des Wikis ausführt 2. Das System zeigt der Benutzergruppe das Wiki mit allen Wiki-Einträgen an 3. Die Benutzergruppe wählt einen Wiki-Eintrag der angezeigten Wiki-Einträge aus 4. Das System zeigt der Benutzergruppe ihren ausgewählten Wiki-Eintrag an   **Ende**. | |
| **Ablauf-Varianten:** | | |
|  |  | |
| **Spezielle Anforderungen:** | | |
| Die Benutzergruppe soll jederzeit Zugriff auf das Wiki haben | | |
| **Zu klärende Punkte:** | | |
|  | | |

|  |  |  |
| --- | --- | --- |
| **Bearbeitung des Wikis** | | |
| **Kennung** | | UC-6 |
| **Priorität** | | Gering |
| **Kurzbeschreibung:** | | |
| Die Benutzergruppe soll das vorhandene Wiki bearbeiten können. | | |
| **Vorbedingung(en):** | | |
| * Das Wiki ist geöffnet | | |
| **Nachbedingung(en):** | | |
| * Die Wiki-Einträge wurden gemäß der Benutzereingaben verändert * Die Änderungen am Wiki wurden abgespeichert | | |
| **Normaler Ablauf:** | | |
|  | 1. Der Anwendungsfall beginnt, wenn die Benutzergruppe die Aktion zum Bearbeiten des Wikis ausführt 2. Die Benutzergruppe wählt aus, ob sie einen Wiki-Eintrag bearbeiten, löschen oder hinzufügen will 3. Das System speichert die von der Benutzergruppe getätigten Änderungen am Wiki   **Ende**. | |
| **Ablauf-Varianten:** | | |
| 2a | Die Benutzergruppe will einen Wiki-Eintrag bearbeiten | |
|  | 1. Die Benutzergruppe wählt den zu bearbeitenden Wiki-Eintrag aus 2. Das System lädt den zu bearbeitenden Wiki-Eintrag 3. Die Benutzergruppe tätigt ihre Änderungen an dem gewählten Wiki-Eintrag 4. Die Benutzergruppe bestätigt die getätigten Änderungen am gewählten Wiki-Eintrag   **Rückkehr nach**: 3 | |
| 2b | Die Benutzergruppe will einen Wiki-Eintrag löschen | |
|  | 1. Die Benutzergruppe wählt den zu löschenden Wiki-Eintrag aus 2. Die Benutzergruppe bestätigt die Löschung des gewählten Wiki-Eintrags   **Rückkehr nach**: 3 | |
| 2c | Die Benutzergruppe will einen Wiki-Eintrag hinzufügen | |
|  | 1. Das System lädt einen neuen Wiki-Eintrag 2. Die Benutzergruppe fügt Informationen im neuen Wiki-Eintrag ein 3. Die Benutzergruppe bestätigt die Erstellung des neuen Wiki-Eintrags   **Rückkehr nach**: 3 | |
| **Spezielle Anforderungen:** | | |
| Die Benutzergruppe soll die Bearbeitung jederzeit abbrechen können | | |
| **Zu klärende Punkte:** | | |
|  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Anzeigen der Aufzeichnung** | | | |
| **Kennung** | | | UC-7 |
| **Priorität** | | | Mittel |
| **Kurzbeschreibung:** | | | |
| Das System soll die Aufzeichnung des Übungsszenarios anzeigen. | | | |
| **Vorbedingung(en):** | | | |
| * Die Bearbeitung eines Übungsszenarios ist beendet * Das System hat die Bearbeitung des Übungsszenarios aufgezeichnet | | | |
| **Nachbedingung(en):** | | | |
| * Der Benutzergruppe wurden die aufgezeichneten Handlungsschritte der Bearbeitung des Übungsszenarios angezeigt | | | |
| **Normaler Ablauf:** | | | |
|  | 1. Der Anwendungsfall beginnt, wenn das Übungsszenario beendet ist 2. Das System zeigt den Benutzergruppen die Aufzeichnung an 3. Die Benutzergruppe schließt die Aufzeichnung   **Ende**. | | |
| **Ablauf-Varianten:** | | | |
| 2a | | Es handelt sich um ein lokales Übungsszenario | |
|  | | 1. Allen Benutzergruppen wird abschließend zum Übungsszenario die Aufzeichnung an einem Rechner angezeigt   **Rückkehr nach**: 3 | |
| 2b | | Es handelt sich um ein netzwerkbasiertes Übungsszenario | |
|  | | 1. Allen Benutzergruppen wird abschließend zum Übungsszenario die Aufzeichnung am jeweiligen Rechner angezeigt   **Rückkehr nach**: 3 | |
| **Spezielle Anforderungen:** | | | |
|  | | | |
| **Zu klärende Punkte:** | | | |
| Bei diesem Use Case ist es möglich, eine Liste von ausgeführten Handlungsschritten anzuzeigen. Allerdings wird im aktuellen Stand (21.06.23) die Aufzeichnung am Ende eines Übungsszenarios noch nicht angezeigt, da das Ende eines Übungsszenarios in der Implementierung noch nicht definiert ist | | | |

|  |  |  |
| --- | --- | --- |
| **Nachricht senden** | | |
| **Kennung** | | UC-8 |
| **Priorität** | | Hoch |
| **Kurzbeschreibung:** | | |
| Die Rollen sollen Nachrichten in Form von Photonen oder Bitfolgen senden können. | | |
| **Vorbedingung(en):** | | |
| * Es wird ein Übungsszenario bearbeitet * Die Rolle, welche eine Nachricht senden möchte, ist am Zug | | |
| **Nachbedingung(en):** | | |
| * Die Nachricht wurde gesendet und ist auf dem entsprechenden Übertragungskanal gespeichert und kann ausgelesen werden | | |
| **Normaler Ablauf:** | | |
|  | 1. Der Anwendungsfall beginnt, wenn die Rolle den Handlungsschritt zum Senden einer Nachricht ausführt 2. Die Rolle wählt die zu sendende(n) Information(en) aus 3. Die Rolle wählt den Empfänger der Nachricht aus 4. Das System sendet die gewählte(n) Information(en) in Form einer Nachricht auf dem jeweiligen Übertragungskanal   **Ende**. | |
| **Ablauf-Varianten:** | | |
|  | | |
| **Spezielle Anforderungen:** | | |
|  | | |
| **Zu klärende Punkte:** | | |
| Dieser Use Case ist implementiert, allerdings unterscheidet der Ablauf in der Implementierung von der Analyse. Richtig im Testspezifikationsdokument beschrieben | | |

|  |  |  |
| --- | --- | --- |
| **Nachricht empfangen** | | |
| **Kennung** | | UC-9 |
| **Priorität** | | Hoch |
| **Kurzbeschreibung:** | | |
| Die Rollen sollen Nachrichten in Form von Photonen oder Bitfolgen empfangen können. | | |
| **Vorbedingung(en):** | | |
| * Es wird ein Übungsszenario bearbeitet * Die Rolle, welche eine Nachricht empfangen möchte, ist am Zug | | |
| **Nachbedingung(en):** | | |
| * Die Nachricht wurde empfangen und wird angezeigt * Die empfangene Nachricht wurde aus dem Übertragungskanal entfernt | | |
| **Normaler Ablauf:** | | |
|  | 1. Der Anwendungsfall beginnt, wenn die Rolle den Handlungsschritt zum Empfangen einer Nachricht ausführt 2. Das System zeigt an, auf welchem Übertragungskanal Informationen verfügbar sind 3. Die Rolle wählt aus, von welchem Übertragungskanal sie Informationen empfangen will 4. Die Nachricht wird gemäß der Benutzereingaben ausgelesen 5. Die Nachricht wird abgespeichert 6. Das System entfernt die empfangene Nachricht aus dem entsprechenden Übertragungskanal   **Ende**. | |
| **Ablauf-Varianten:** | | |
| 3a | Die Rolle möchte Informationen vom Photonenübertragungskanal empfangen | |
|  | 1. Die Rolle wählt vorhandene Polarisationsschemata als Detektor für die Photonenfolge aus   **Rückkehr nach**: 4 | |
| **Spezielle Anforderungen:** | | |
|  | | |
| **Zu klärende Punkte:** | | |
| Dieser Use Case ist implementiert, allerdings unterscheidet der Ablauf in der Implementierung von der Analyse. Richtig im Testspezifikationsdokument beschrieben | | |

|  |  |  |
| --- | --- | --- |
| **Nachricht abhören** | | |
| **Kennung** | | UC-10 |
| **Priorität** | | Hoch |
| **Kurzbeschreibung:** | | |
| Eve soll Nachrichten in Form von Photonen oder Bitfolgen abhören können. | | |
| **Vorbedingung(en):** | | |
| * Es wird ein Übungsszenario bearbeitet * Eve ist am Zug | | |
| **Nachbedingung(en):** | | |
| * Die Nachricht wurde abgehört und angezeigt * Die abgehörte Nachricht wurde an den ursprünglichen Empfänger weitergesendet | | |
| **Normaler Ablauf:** | | |
|  | 1. Der Anwendungsfall beginnt, wenn Eve den Handlungsschritt zum Abhören einer Nachricht ausführt 2. Das System zeigt an, auf welchem Übertragungskanal Informationen verfügbar sind 3. Eve wählt aus, auf welchem Übertragungskanal sie Informationen abhören will | |
| **Ablauf-Varianten:** | | |
| 3a | Eve möchte Informationen vom Photonenübertragungskanal abhören | |
|  | 1. Eve führt den Use-Case „Nachricht empfangen“ (UC-9) durch 2. Eve führt den Use-Case „Nachricht senden“ (UC-8) mit der empfangenen Bitfolge durch   **Ende.** | |
| 3b | Eve möchte Bitfolgen vom Bitübertragungskanal abhören | |
|  | 1. Die Nachrichten auf dem Bitübertragungskanal werden abgespeichert 2. Das System zeigt an, welche Bitfolgen abgehört wurden 3. Das System sendet die abgehörten Bitfolgen an den ursprünglichen Empfänger   **Ende.** | |
| **Spezielle Anforderungen:** | | |
|  | | |
| **Zu klärende Punkte:** | | |
| Dieser Use Case ist überflüssig, da „Abhören“ durch Eve eigentlich nur Empfangen und Senden von Informationen ist. Diese Funktionalitäten sind mit Use Case 8 und 9 abgedeckt | | |

|  |  |  |
| --- | --- | --- |
| **Generierung einer Information** | | |
| **Kennung** | | UC-11 |
| **Priorität** | | Hoch |
| **Kurzbeschreibung:** | | |
| Die Rolle soll Informationen generieren können. | | |
| **Vorbedingung(en):** | | |
| * Die Rolle, welche Informationen generieren möchte, ist am Zug * Die Rolle verfügt über die für die Generierung benötigten Informationen | | |
| **Nachbedingung(en):** | | |
| * Die generierten Informationen werden der Rolle angezeigt * Die generierten Informationen sind abgespeichert | | |
| **Normaler Ablauf:** | | |
|  | 1. Der Anwendungsfall beginnt, wenn die Rolle die Aktion zur Generierung der gewünschten Information ausführt 2. Das System generiert die gewünschte Information 3. Die Rolle benennt die generierte Information | |
| **Ablauf-Varianten:** | | |
| 2a | Die zu generierende Information ist eine Bitfolge | |
|  | 1. Die Rolle wählt eine beliebige Zahl aus, mit der eine zufällige Bitfolge generiert werden soll 2. Das System generiert eine zufällige Bitfolge   **Rückkehr nach**: 3 | |
| 2a1a | Die Rolle gibt die Bitfolge an | |
|  | 1. Die Rolle gibt die Bitfolge ein 2. Das System gibt der Rolle die Möglichkeit die eingegebene Bitfolge anzupassen   **Rückkehr nach**: 3 | |
| 2b | Die zu generierende Information sind Polarisationsschemata | |
|  | 1. Die Rolle wählt eine beliebige Zahl aus, mit der zufällige Polarisationsschemata generiert werden soll 2. Das System generiert zufällige Polarisationsschemata   **Rückkehr nach**: 3 | |
| 2b1a | Die Rolle gibt die Polarisationsschemata an | |
|  | 1. Die Rolle gibt die Polarisationsschemata ein 2. Das System gibt der Rolle die Möglichkeit die eingegebenen Polarisationsschemata anzupassen   **Rückkehr nach**: 3 | |
| 2c | Die zu generierende Information sind Photonen | |
|  | 1. Die Rolle wählt vorhandene Polarisationsschemata als Emitter für die Photonenfolge aus 2. Die Rolle wählt die Bitfolge, aus welcher die Photonen generiert werden sollen, aus 3. Das System berechnet anhand dieser beiden Eingaben die zu sendende Photonenfolge   **Rückkehr nach**: 3 | |
| 2d | Die zu generierende Information ist eine Bit-Maske | |
|  | 1. Die Rolle wählt die Länge der Bit-Maske und Anzahl der Einsen aus 2. Das System generiert die Bit-Maske   **Rückkehr nach**: 3 | |
| **Spezielle Anforderungen:** | | |
|  | | |
| **Zu klärende Punkte:** | | |
| Dieser Use Case ist implementiert, allerdings nicht vollständig, da in der Implementierung folgende weitere Funktionen hinzugekommen sind: Das System erzeugt einen eingegebenen Text; das System generiert eine Zahl; das System bestimmt die Textlänge | | |

|  |  |  |
| --- | --- | --- |
| **Vergleich von Informationen** | | |
| **Kennung** | | UC-12 |
| **Priorität** | | Hoch |
| **Kurzbeschreibung:** | | |
| Die Rolle soll Informationen vergleichen können. | | |
| **Vorbedingung(en):** | | |
| * Die Rolle, welche Informationen vergleichen möchte, ist am Zug * Die Rolle verfügt über die zu vergleichenden Informationen | | |
| **Nachbedingung(en):** | | |
| * Die Informationen wurden verglichen * Das System zeigt der Rolle das Ergebnis des Vergleichs an * Das Ergebnis des Vergleichs ist abgespeichert | | |
| **Normaler Ablauf:** | | |
|  | 1. Der Anwendungsfall beginnt, wenn die Rolle die Aktion zum Vergleich der gewünschten Information ausführt 2. Das System vergleicht die gewünschten Informationen 3. Die Rolle benennt das Ergebnis des Vergleichs | |
| **Ablauf-Varianten:** | | |
| 2a | Es sollen zwei Polarisationsschemata verglichen werden | |
|  | 1. Die Rolle gibt die zu vergleichenden Polarisationsschemata an 2. Das System vergleicht die beiden angegebenen Polarisationsschemata   **Rückkehr nach**: 3 | |
| 2b | Es sollen zwei Bitfolgen verglichen werden | |
|  | 1. Die Rolle gibt die zu vergleichenden Bitfolgen an 2. Das System vergleicht die beiden angegebenen Bitfolgen   **Rückkehr nach**: 3 | |
| **Spezielle Anforderungen:** | | |
|  | | |
| **Zu klärende Punkte:** | | |
| Hier fehlt die Ablaufvariante zum Vergleich zweier nicht vergleichbarer Informationen, ist aber implementiert. Siehe Testspezifikationsdokument | | |

|  |  |  |
| --- | --- | --- |
| **Umwandlung von Informationen** | | |
| **Kennung** | | UC-13 |
| **Priorität** | | Hoch |
| **Kurzbeschreibung:** | | |
| Die Rolle soll Informationen umwandeln können. | | |
| **Vorbedingung(en):** | | |
| * Die Rolle, welche Informationen umwandeln möchte, ist am Zug * Die Rolle verfügt über die umzuwandelnden Informationen | | |
| **Nachbedingung(en):** | | |
| * Die Informationen wurden umgewandelt * Das System zeigt der Rolle das Ergebnis der Umwandlung an * Das Ergebnis der Umwandlung ist abgespeichert | | |
| **Normaler Ablauf:** | | |
|  | 1. Der Anwendungsfall beginnt, wenn die Rolle die Aktion zum Umwandeln der gewünschten Informationen ausführt 2. Das System wandelt die gewünschten Informationen um 3. Die Rolle benennt die umgewandelte Information | |
| **Ablauf-Varianten:** | | |
| 2a | Umwandlung von Photonen zu einer Bitfolge | |
|  | 1. Die Rolle gibt die Photonenfolge an 2. Das System berechnet anhand dieser Eingabe die Bitfolge   **Rückkehr nach**: 3 | |
| 2b | Umwandlung eines Textes in eine verschlüsselte Nachricht | |
|  | 1. Die Rolle wählt einen vorhandenen Text, der verschlüsselt werden soll, aus 2. Die Rolle wählt die Bitfolge, mit der der Text verschlüsselt werden soll, aus 3. Das System berechnet anhand dieser beiden Eingaben den verschlüsselten Text   **Rückkehr nach**: 3 | |
| 2c | Umwandlung einer verschlüsselten Nachricht in einen Text | |
|  | 1. Die Rolle wählt einen vorhandenen Text, der entschlüsselt werden soll, aus 2. Die Rolle wählt die Bitfolge, mit der der Text entschlüsselt werden soll, aus 3. Das System berechnet anhand dieser beiden Eingaben den entschlüsselten Text   **Rückkehr nach**: 3 | |
| **Spezielle Anforderungen:** | | |
|  | | |
| **Zu klärende Punkte:** | | |
|  | | |

|  |  |  |
| --- | --- | --- |
| **Veränderung von Informationen** | | |
| **Kennung** | | UC-14 |
| **Priorität** | | Hoch |
| **Kurzbeschreibung:** | | |
| Die Rolle soll Informationen verändern können. | | |
| **Vorbedingung(en):** | | |
| * Die Rolle, welche Informationen verändern möchte, ist am Zug * Die Rolle verfügt über die zu verändernden Informationen | | |
| **Nachbedingung(en):** | | |
| * Die Informationen wurden verändert * Das System zeigt der Rolle das Ergebnis der Veränderung an * Das Ergebnis der Veränderung ist abgespeichert | | |
| **Normaler Ablauf:** | | |
|  | 1. Der Anwendungsfall beginnt, wenn die Rolle die Aktion zum Verändern der gewünschten Informationen ausführt 2. Das System verändert die gewünschten Informationen 3. Die Rolle benennt die veränderte Information | |
| **Ablauf-Varianten:** | | |
| 2a | Die Veränderung ist ein Streichen von Bits aus einer Bitfolge | |
|  | 1. Die Rolle gibt die Bit-Maske, nach der die Bitstellen aus der Bitfolge gestrichen werden sollen, an 2. Die Rolle gibt die Bitfolge an 3. Die Rolle gibt den zu streichenden Bit-Wert an 4. Das System streicht aus der Bitfolge die Bitstellen gemäß der Bit-Maske   **Rückkehr nach**: 3 | |
| 2b | Die Veränderung ist eine freie Bearbeitung von Information | |
|  | 1. Die Rolle verändert die Information in selbstherrlicher Manier   **Rückkehr nach**: 3 | |
| **Spezielle Anforderungen:** | | |
|  | | |
| **Zu klärende Punkte:** | | |
| Dieser Use Case ist implementiert, allerdings fehlen in den Ablaufvarianten die Negierung einer Bitfolge und das Neubennen einer Information | | |

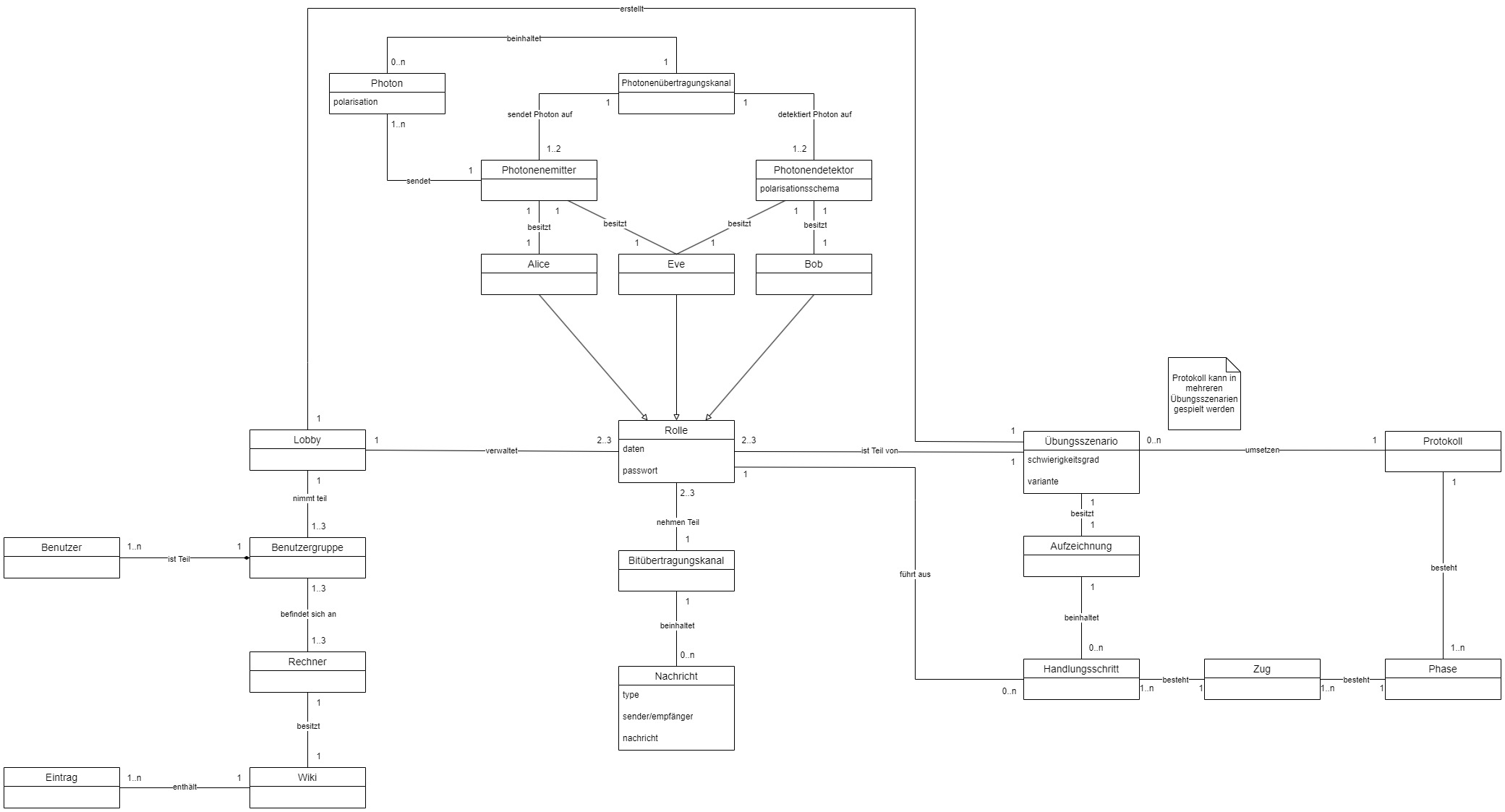
### Hinweise zu den Use-Cases

* Auf den Use-Case „One-Time-Pad vereinbaren“ wurde verzichtet!

## (Sonstige) Funktionalität

|  |  |  |
| --- | --- | --- |
| **ID** | **Beschreibung** | **Querverweise** |
| FR-001 | Das System soll jede Fehlersituation dauerhaft protokollieren. | - |
| FR-002 | Die Nutzung des Systems soll generell nur nach vorheriger Authentifizierung möglich sein. | - |
| FR-003 | Es soll einer Benutzergruppe ermöglicht werden, sich über Links/Beschreibungen in einem Verzeichnis selbst zu informieren. | - |
| FR-004 | Es soll einer Benutzergruppe ermöglicht werden, sich einer (oder mehrerer) beliebigen, noch vorhandenen Rolle(n) zuzuordnen. | - |
| FR-005 | Es soll einer Benutzergruppe möglich sein, gemeinsam Übungsszenarien zu bearbeiten. | - |
| FR-006 | Eine Benutzergruppe soll sich durch Handlungsschritte durch das Szenario hangeln können. | - |
| FR-007 | Die Benutzergruppen dürfen nicht gleichzeitig aktiv sein und müssen sich abwechseln. | - |
| FR-008 | Es soll möglich sein, Übungsszenarien in unterschiedlichen Schwierigkeitsgraden zu bearbeiten. | - |
| FR-009 | Das System soll den Zugriff auf die Informationen einer Rolle durch andere Rollen schützen. | - |
| FR-010 | Es soll einer Benutzergruppe auch ermöglicht werden, von unterschiedlichen Rechnern im lokalen Netzwerk aus mitzumachen. | - |
| FR-011 | Es soll einer Benutzergruppe ermöglicht werden, jederzeit ins Hauptmenü zurückzukommen. | - |
| FR-012 | Es soll einer Benutzergruppe ermöglicht werden, bei vorzeitiger Beendigung des Übungsszenarios das Protokoll mit den getätigten Schritten anzeigen zu lassen. | - |

## Modell des Problembereichs (Konzeptionelles Datenmodell)



# Nicht-Funktionale Anforderungen

## Benutzbarkeit (Usability)

|  |  |  |
| --- | --- | --- |
| **ID** | **Beschreibung** | **Querverweise** |
| UR-001 | Das System soll über eine grafische Benutzeroberfläche intuitiv bedienbar sein. |  |
| UR-002 | Die Benutzeroberfläche ist selbsterklärend gestaltet. |  |
| UR-003 | Die Benutzeroberfläche soll den Benutzer bei sich wiederholenden Eingaben unterstützen. |  |

## Zuverlässigkeit (Reliability)

|  |  |  |
| --- | --- | --- |
| **ID** | **Beschreibung** | **Querverweise** |
| RR-001 | Das System soll keine Eingaben verwerfen |  |
| RR-002 | Die Gefahr des Absturzes des Programms soll auf ein Minimum reduziert werden |  |
| RR-003 | Das System soll im Netzwerkbetrieb zuverlässig mit anderen Teilnehmern im lokalen Netzwerk kommunizieren können |  |
| RR-004 | Das System soll den Benutzer informieren, wenn die Verbindung instabil ist oder abgebrochen wird. |  |
| RR-005 | Das System soll bei einem Verbindungsabbruch eine Möglichkeit zum erneuten Verbindungsaufbau bieten. |  |

## Leistung (Performance)

|  |  |  |
| --- | --- | --- |
| **ID** | **Beschreibung** | **Querverweise** |
| PR-001 | Das System soll nicht länger als drei Sekunden benötigen, um auf Benutzereingaben zu reagieren |  |
| PR-002 | Nach Beendigung eines Zugs einer Rolle darf im netzwerkbasierten Betrieb eine andere Benutzergruppe maximal drei Sekunden auf die übertragenen Daten warten müssen. |  |

## Unterstützbarkeit (Supportability)

|  |  |  |
| --- | --- | --- |
| **ID** | **Beschreibung** | **Querverweise** |
| SR-001 | Das System soll mehrere Sprachen unterstützen. |  |
| SR-002 | Das System soll aus Komponenten zusammengesetzt sein, die eine geringe Kopplung untereinander aufweisen und auf eine Aufgabe spezialisiert sind. |  |
| SR-003 | Das System soll für weitere Protokolle offen sein. |  |

## Sonstige Einschränkungen

### Schnittstellen

* + Bandbreite der Netzwerkverbindung
  + Verfügbarkeit der Netzwerkverbindung

### Implementierung

* + Zielumgebung: Das Programm soll im Softwarelabor mit den vorgegebenen Softwareversionen ausführbar sein.
  + Die verwendeten Programmiersprachen sollen sich auf C# und Java beschränken. Intern wurde für C# gestimmt.

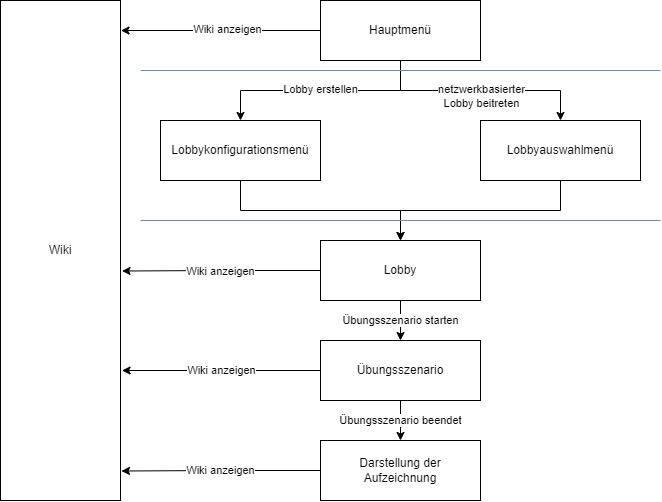
### Entwurf

Der Entwurf entfällt an dieser Stelle!

# Risikoakzeptanz

Hier nicht relevant, da kein sicherheitskritisches System.

# Skizze der Gesamtsystemarchitektur



# Lieferumfang

Die folgende Tabelle enthält alle Arbeitsergebnisse, die in der Veranstaltung „Software-Projekte“ zu dem vom Team zu liefernden „End-Produkt“ gehören – für die individuell von jedem Projektteilnehmer zu liefernden Ergebnissen lesen Sie bitte im Projektleitfaden bzw. im Projektkalender nach. Die Benotung erfolgt nicht nur auf Grundlage des lauffähigen Programms, sondern bezieht die Qualität der Analyse, des Entwurfs und des Systemtests mit ein.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lfd. Nr.** | **Was?** | **Art des Dokuments** | **Bemerkungen** |
| **Ergebnis der System-Analyse** | | | |
| 1 | Das Dokument „Systemanalyse\_TeamC\_V1.0“ (also dieses Dokument) mit funktionalen, nicht-funktionalen Anforderungen und konzeptionellem Datenmodell. | * Siehe Vorlage. * Wird bei Projektbeginn mit einem Überblick gebenden Systembeschreibung an das Team ausgegeben. Das Dokument ist vom Team weiterzuführen und wieder abzugeben. | * Bitte auf Abgabetermin während des Semesters achten (s. Projektkalender). * Rechtzeitig vor Abgabe auf Qualitätssicherung achten (Review) |
| **Dokumentation des Systementwurfs** | | | |
| 2 | Das Dokument „Systementwurf\_TeamC\_V1.0“. | * Siehe Vorlage. | * Bitte auf Abgabetermin während des Semesters achten (s. Projektkalender) * Rechtzeitig vor Abgabe auf Qualitätssicherung achten (Review) |
| **Implementierung** | | | |
| 3 | Lauffähiger und getesteter Quellcode |  | Abgabe am Semesterende |
| **Test** | | | |
| 4 | Testspezifikation Systemtest | * Siehe Vorlage | * Endgültige Abgabe am Semesterende; zur Vorbereitung des Abnahmetests ist die Aufstellung der in den Abnahmetest einbezogenen Testfälle früher vorzulegen (Termin im Projektkalender) |

# Abnahmekriterien

In der Veranstaltung „Software-Projekte“ werden vom „Auftraggeber“ (in Absprache mit den Teilnehmern) rechtzeitig vor Semesterende Systemtestfälle ausgewählt, die das System dann am Tag der Abnahme ohne Beanstandung „überstehen“ muss.

# Glossar

|  |  |
| --- | --- |
| Begriff | Erklärung |
| Aktion | Eine Handlung einer Benutzergruppe auf der Benutzeroberfläche |
| Alias | Der Anzeigename einer Rolle innerhalb eines Übungsszenarios |
| Aufzeichnung | Mitschnitt der Handlungsschritte eines Übungsszenarios |
| Benutzergruppe | Besteht aus einem oder mehreren Benutzern |
| Bitfolge | Aneinanderreihung von Bits. Stellt Information dar |
| Bitübertragungskanal | Ausprägung eines Übertragungskanals, welches ausschließlich Bitfolgen übertragen kann |
| Handlungsschritt | Elementare Einheit, welche eine Rolle während ihres Zuges ausführen kann |
| Hauptmenü | Das Menü, in welchem das System startet |
| Lobby | Besteht aus einem Übungsszenario und der Rollenzuteilung |
| Lobbyauswahlmenü | Das Menü, welches es Benutzergruppen erlaubt, netzwerkbasierten Lobbys in ihrem Netzwerk beizutreten |
| Lobbyhost | Die Benutzergruppe, welche die Lobby erstellt hat. Nur ihr ist es möglich, das Übungsszenario zu starten |
| Lobbykonfigurationsmenü | Das Menü, in welchem die Einstellungen für das Übungsszenarios einer Lobby getätigt werden können |
| Lokal | Eigenschaft einer Lobby. Bedeutet, dass diese ausschließlich auf einem System läuft |
| Menü | Bezeichnet eine Benutzeroberfläche, in welcher Änderungen vorgenommen werden können oder zu anderen Menüs gewechselt werden kann |
| Nachricht | Container für Information. Kann über einen Übertragungskanal gesendet werden |
| Netzwerkbasiert | Eigenschaft einer Lobby. Bedeutet, dass diese von anderen Systemen im selben Netzwerk gefunden werden und beigetreten kann |
| Phase | Besteht aus mehreren Zügen verschiedener Rollen. Fest definiert |
| Photon | Besitzt eindeutige Polarisation. Stellt Information dar |
| Photonenübertragungskanal | Ausprägung eines Übertragungskanals, welches ausschließlich Photonen übertragen kann |
| Polarisationsschema | Besitzt eindeutige Ausrichtung. Wird benutzt, um Photonen zu empfangen. Verändert je nach Umständen bei Empfang die Polarisation |
| Rolle | Alice, Bob und Eve. Handlungsträger in einem Übungsszenario. Wird von genau einer Benutzergruppe repräsentier |
| System | Beschreibt das gesamte Konstrukt |
| Übertragungskanal | Beschreibt das Konstrukt, über welches Nachrichten gesendet werden können |
| Übungsszenario | Ausprägung einer Variante mit ausgewählten Phasen und Schwierigkeitsgrad |
| Variante | Normaler Ablauf, Lauschangriff und Man-in-the-Middle |
| Wiki | Das Informationsverzeichnis, welches durch eine Benutzergruppe konfigurierbar ist |
| Wiki-Eintrag | Ein einzelner Eintrag des Informationsverzeichnisses |
| Zug | Besteht aus mindestens einem Handlungsschritt einer Rolle |

# Abkürzungsverzeichnis

|  |  |
| --- | --- |
| Abkürzung | Erklärung |
| Polscha (Sg.) | Polarisationsschema |
| Polschata/Polschas (Pl.) | Polarisationsschemata/Polarisationsschemas |

# Literaturverzeichnis

**[Lar]** Larman Craig, *Applying UML And Patterns. An Introduction to Object-Oriented Analysis And Design,* Prentice Hall, 2nd ed., 2002

# Abbildungsverzeichnis

1. V-Modell® ist eine geschützte Marke der Bundesrepublik Deutschland. [↑](#footnote-ref-2)