ABUS | Pfaffenhain GmbH
abus.com

ABUS Pfaffenhain GmbH · Fabrikstraße 1 · 09387 Jahnsdorf 22.01.2026

Projektträger Jülich
Forschungszentrum Jülich GmbH
Postfach 61 02 47
10923 Berlin

Vorhabenbezeichnung „Chainlock - Blockchain-gestützte, smarte Schließanlagen“
Förderkennzeichen: 03WIR1321B
Abschlussbericht

Sehr geehrter Herr Dr. Engelhard,
sehr geehrte Frau Adelberger,

nachfolgend übersenden wir Ihnen den Projektabschlussbericht für das Förderprojekt 03WIR1321A.

1.) Aufzählung der wichtigsten wissenschaftlich-technischen Ergebnisse und anderer wesentlicher Ergebnisse

Projektmanagement / Organisation

Für die Organisation und Steuerung des Projekts sowie zur zentralen Ablage aller relevanten Dokumente, Konzepte, Arbeitsergebnisse, Ideen und des im Projekt generierten Wissens wurde die Projektmanagementplattform Confluence eingesetzt. Die Plattform diente als zentrales Arbeits- und Dokumentationssystem für alle Projektbeteiligten.

Das in Confluence integrierte Ticketsystem wurde genutzt, um den Projektverlauf strukturiert abzubilden. Hierüber konnten bereits durchgeführte Arbeitsschritte, der jeweils aktuelle Stand sowie anstehende Aufgaben nachvollziehbar dokumentiert werden. Darüber hinaus wurden Entwicklungsentscheidungen festgehalten und die Ressourcen geplant und koordiniert.

Der Zugriff auf die Projektplattform war auf einen klar definierten Nutzerkreis beschränkt. Dadurch wurde sowohl die Vertraulichkeit sensibler Projektinformationen als auch die Nachvollziehbarkeit aller Änderungen und Entscheidungen sichergestellt. Die vollständige Historie der Tickets und Inhalte erlaubt zudem eine revisionssichere Archivierung des Projektverlaufs.

Für den Austausch von Dateien wurde eine auf der Open-Source-Software Nextcloud basierende Lösung eingesetzt. Die Verwaltung von Programmquellen, Quellcode, Assets, Konfigurationen der Build-Umgebungen sowie Testdaten erfolgte über die Git-basierte Versionsverwaltungsplattform GitHub.

Zur inhaltlichen Abstimmung und Koordination wurden regelmäßige Meetings durchgeführt, sowohl in Präsenz als auch in digitaler Form. Für kurzfristige Abstimmungen und digitale Besprechungen wurde das Videokonferenzsystem Zoom genutzt.

Use Cases Definitionen

Die Use Cases des Projekts Chainlock wurden auf Grundlage einer detaillierten Analyse der Nutzung bestehender Schließsysteme entwickelt. Dabei wurden insbesondere die unterschiedlichen Kombinationen von Schließberechtigungen betrachtet, wie sie in realen Anwendungsszenarien auftreten (siehe Abbildung 1). Aus dieser Analyse konnten gezielt Optimierungspotenziale hinsichtlich Verwaltungsaufwand, Sicherheit und Flexibilität identifiziert werden.

Zur Reduzierung des administrativen Aufwands sowie zur konsistenten Durchsetzung und Kontrolle der Zugangsregeln wurde eine zentrale Konfiguration umgesetzt (siehe Abbildung 17). Diese Konfiguration regelt die Zuordnung von Personen zu sogenannten Schließgruppen sowie die Zuordnung dieser Schließgruppen zu einzelnen Schlössern. Ein Schloss kann ein Zylinder, ein Türbeschlag oder ein Einsteckschloss selbst sein. Alle Zuordnungen werden zentral verwaltet und autorisiert.

Die Art des Zugangs zu einem Schloss – beispielsweise normaler Nutzerzugang, Bereichs-Generalschlüssel oder Notfallzugang – wird über die jeweilige Schließgruppe definiert. Eine Person kann dabei mehreren Schließgruppen angehören. Die effektive Berechtigung zur Nutzung eines bestimmten Schlosses ergibt sich aus der Kombination der zugeordneten Schließgruppen.

Da Nutzer in der Praxis häufig nur zeitlich eingeschränkten Zugang benötigen, etwa Mitarbeitende nur an Arbeitstagen oder Reinigungspersonal nur außerhalb der regulären Arbeitszeiten, können entsprechende zeitliche Einschränkungen definiert werden. Diese zeitlichen Randbedingungen werden im System ähnlich wie Kalendereinträge behandelt und als zusätzlicher Faktor an die jeweiligen Schließberechtigungen angehängt. Auf diese Weise lässt sich die Sicherheit weiter erhöhen, da Zugriffe automatisch außerhalb der erlaubten Zeiträume verhindert werden.

Durch den Einsatz von Schließgruppen wird von einzelnen Nutzern abstrahiert. Änderungen, wie das Hinzufügen neuer Nutzer oder das Anpassen von Berechtigungen, beschränken sich dadurch in der Regel auf die Anpassung der Gruppenzuordnung. Dies vereinfacht die Verwaltung erheblich und reduziert potenzielle Fehlerquellen.

Die Zuordnung von Schließgruppen zu weiteren Schließgruppen bildet zudem die logische Organisationsstruktur der jeweiligen Einrichtung ab, beispielsweise die Struktur eines Unternehmens mit Abteilungen, Gebäuden, Räumen. Diese Struktur muss üblicherweise nur selten angepasst werden, erlaubt bei Bedarf jedoch auch sehr flexible Organisationsmodelle mit einer großen Anzahl von Gruppen. Dadurch ist die Verwaltung auch umfangreicher Schließsysteme effizient möglich.

Die endgültige Entscheidung, ob eine Schließaktion ausgeführt wird, trifft das jeweilige Schloss selbst. Hierzu kombiniert es die in den relevanten Schließgruppen definierten Berechtigungen und ermittelt daraus die für die anfragende Person wirksame Zugriffsberechtigung.

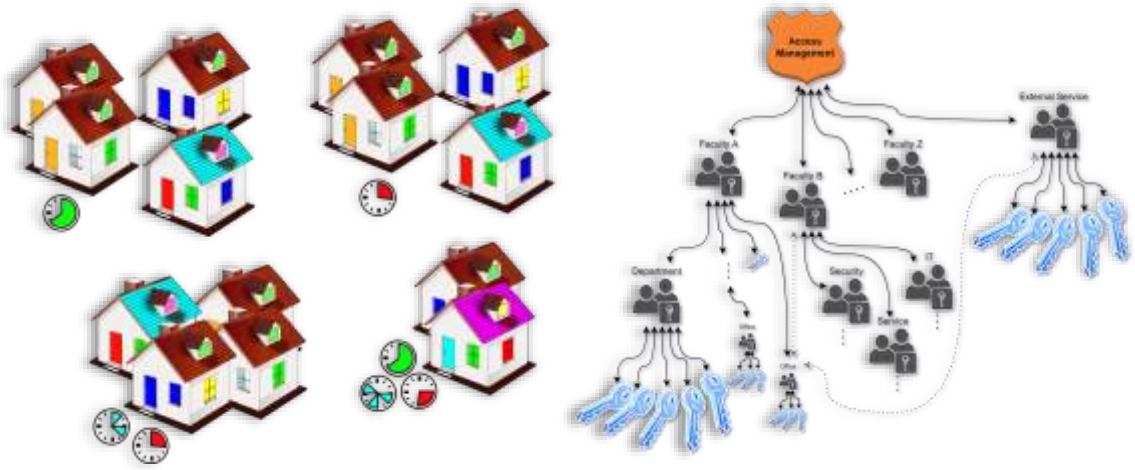


Abbildung 1: (Links) Beispielhafte Schließberechtigungen in einer Wohnanlage mit unterschiedlichen Kombinationen von Zugängen zu Türen und Fenstern sowie zeitlichen Einschränkungen. (Rechts) Komplexe Verwaltungshierarchie von Schließberechtigungen in größeren Einrichtungen mit Abteilungen und Fakultäten, einzelnen Generalschlüsseln sowie sich überschneidenden Berechtigungsbereichen.

Eine kosteneffiziente Verwaltung der Schließregeln bei gleichzeitiger Sicherstellung der Korrektheit, Integrität und Authentizität der Daten erfordert eine gezielte Aufteilung der gespeicherten Informationen. Im Projekt Chainlock wurde hierfür ein zweistufiges Speicherkonzept umgesetzt.

Die potenziell umfangreichen Schließregeln werden verschlüsselt in einem vom Betreiber der Schließanlage festgelegten Cloudspeicher abgelegt. Dieser sogenannte Off-Chain-Speicher ermöglicht eine wirtschaftliche Speicherung großer Datenmengen. Betreiber mit eigener IT-Infrastruktur können diese Daten lokal speichern und behalten so die volle Kontrolle über ihre Informationen. Alternativ können auch externe Speicherdienste wie Google Drive oder Nextcloud genutzt werden, diese sind meist kostenpflichtig.

Die für die Absicherung gegen Manipulation, zur Verifikation sowie zur Bestätigung der Authentizität erforderlichen Informationen werden hingegen als Bestandteil von Blöcken in einer öffentlichen Blockchain gespeichert. Im Projekt wurde hierfür die Blockchain Ethereum Classic verwendet. In der Blockchain werden nicht die Schließregeln selbst abgelegt, sondern ausschließlich kompakte, kryptographische Prüfinformationen. Diese sind unabhängig vom Umfang der eigentlichen Schließregeln und verursachen daher nur geringe Kosten.

Durch diese Aufteilung werden die Auswirkungen von Systemausfällen oder gezielten Angriffen deutlich reduziert. Gleichzeitig wird eine Unabhängigkeit von einem Hersteller der Schließanlage erreicht, da sowohl die Speicherlösung als auch die Blockchain-Technologie frei wählbar sind.

Autorisierte Nutzer verwalten ihre digitalen Identitäten innerhalb der Schließapp in Form von kryptographischen Schlüsseln. Diese können von den Nutzern selbst angelegt werden, beispielsweise getrennt nach Funktionen wie Büroarbeit oder technische Tätigkeiten. Gegenüber der Verwaltung der Schließanlage identifizieren sich die Nutzer mit einem ausgewählten Schlüssel, dem die entsprechenden Schließberechtigungen oder Berechtigungsgruppen zugeordnet sind.

Durch dieses Vorgehen wird die Person von ihren konkreten Funktionen abstrahiert. Dies ermöglicht eine effizientere Verwaltung und erlaubt im Bedarfsfall einen unterbrechungsfreien Ersatz von Nutzern oder Rollen. Gleichzeitig verbleiben alle für die Identitätsverifikation notwendigen Informationen lokal auf dem Endgerät des

Nutzers. Dadurch bleibt die Hoheit über die Daten beim Nutzer selbst, und insbesondere groß angelegte Angriffe werden erheblich erschwert.

Sobald ein Smartphone eine Internetverbindung herstellen kann – sowie zusätzlich in regelmäßigen Abständen – aktualisiert die Schließapp den bekannten Stand der Schließberechtigungen und der Blockchain (siehe Abbildung 17). Bewegt sich der Nutzer anschließend in die Nähe eines Schlosses, kann das Smartphone eine Verbindung herstellen und die aktuellen Daten an das Schloss übermitteln. Das Schloss selbst benötigt hierfür keine eigene Netzwerkinfrastruktur.

Nach Empfang der Daten aktualisiert das Schloss seinen internen Datenstand, einschließlich der Berechtigungen, des Blockchain-Status, der aktuellen Zeit sowie weiterer relevanter Parameter. Treffen andere Nutzer mit neueren Aktualisierungen ein, wird der Aktualisierungsvorgang entsprechend wiederholt. Veraltete oder fehlerhafte Datenstände werden vom Schloss erkannt und ignoriert. Auf diese Weise tragen auch Nutzer, die das Schloss nicht aktiv bedienen, zur Verteilung aktueller Daten bei. Diese Vielzahl unterschiedlicher und schwer beeinflussbarer Aktualisierungspfade erhöht die Gesamtsicherheit des Systems zusätzlich.

Möchte ein Nutzer eine Schließaktion durchführen, nutzt er die entsprechende Funktion der Schließapp. Das Smartphone kommuniziert dabei gezielt mit dem jeweiligen Schloss und weist die Identität des Nutzers nach. Das Schloss prüft anschließend, ob für diese Identität eine gültige Schließberechtigung vorliegt und ob der bekannte Datenstand ausreichend aktuell ist. Nur wenn alle Bedingungen erfüllt sind, wird die Schließaktion ausgeführt. Ist der Identitätsnachweis fehlerhaft, veraltet oder liegt keine passende Berechtigung vor, erfolgt keine Schließaktion.

Aus den beschriebenen Konzepten und Abläufen ergeben sich die in Abbildung 2 dargestellten Hauptkomponenten des im Projekt realisierten Schließsystems. Diese Komponenten sind jeweils durch die für ihre Umsetzung typischen Eigenschaften und eingesetzten Technologien gekennzeichnet.

Abbildung 2: Übersicht der vier Hauptkomponenten des Schließsystems und ihrer jeweils zentralen Eigenschaften und Aufgaben.

Das Zusammenspiel dieser Hauptkomponenten bei der Durchführung eines modernen, digital gestützten und blockchainbasierten Schließvorgangs erfolgt gemäß dem in Abbildung 3 dargestellten Ablauf. Dieser systematische Prozess trägt wesentlich zur Sicherheit, Nachvollziehbarkeit und Benutzerfreundlichkeit des entwickelten Schließsystems bei.

Abbildung 1: Ablauf mit der Verwaltung von Berechtigungen, der Blockchain (BC) und dem Speicher der verschlüsselten und gesicherten Berechtigungsdaten (Off-Chain-Storage). Mittels periodischen Downloads der Regeln auf das Smartphone des Benutzers und deren spätere Übermittlung zum Schloss erhält dieses zuverlässig Aktualisierungen der Regeln. Bei Anforderung einer Schließaktion prüft das Schloss die Identität des Nutzers und die Zulässigkeit der Aktion und führt die gewünschte Aktion gegebenenfalls aus.

Technologie & Hardware

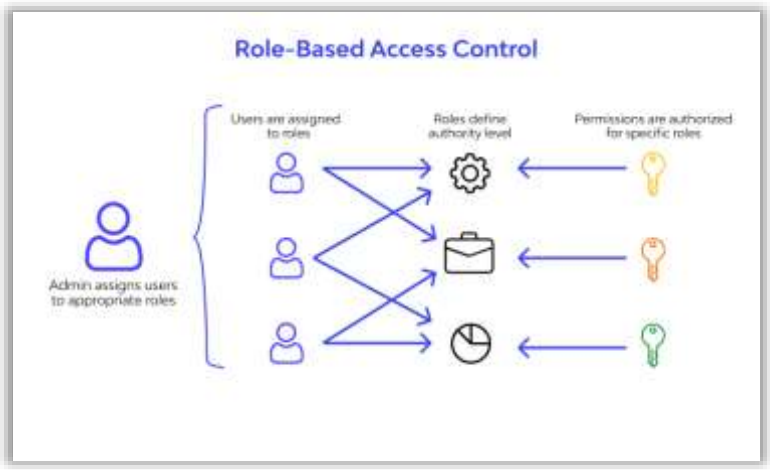


Abbildung 2: Beispiel einer Zuordnungsstruktur von Nutzern zu Rollen, um Zugriff zu bestimmten Objekten zu ermöglichen.

Im Berichtszeitraum wurden die zentralen Funktionsbereiche des Projekts bearbeitet. Diese umfassen die Verwaltung der Schließberechtigungen, die vom Anwender genutzte smartphonebasierte Schließapp sowie die im Schloss integrierte Steuerhardware.

Die Verwaltung der Schließanlage gliedert sich in mehrere Teilbereiche. Der erste Teilbereich betrifft die Erstellung und Registrierung neuer Benutzerkonten. Hierfür ist entweder eine zentrale Verwaltungsplattform vorgesehen oder eine Integration der Verwaltungsfunktionen in einen gesicherten Bereich der Schließapp (siehe Abbildung 17). Jeder Nutzer wird dabei eindeutig identifiziert. Zu den erfassten Basisdaten zählen unter anderem der Name, die E-Mail-Adresse sowie eine systemweit eindeutige Nutzer-ID.

Auf Seiten des Nutzers erfolgt die Erstellung eines digitalen kryptographischen Schlüsselpaares. Hierfür wird das international verbreitete, quelloffene und herstellerunabhängige Public-Key-Authentifizierungsverfahren Ed25519 gemäß RFC 7748 verwendet. Die dafür notwendige Funktionalität ist direkt in die Schließapp integriert. Sie ermöglicht die Erstellung einer beliebigen Anzahl von Schlüsselpaaren, beispielsweise zur Trennung unterschiedlicher Funktionen im Unternehmen, für verschiedene Einsatzbereiche oder für den unterbrechungsfreien Ersatz bestehender Schlüssel.

Der private Schlüsselteil verbleibt dabei stets geschützt beim Nutzer. Der öffentliche Schlüsselteil kann an die Verwaltung der Schließanlage übertragen werden. Dort wird er als Bestandteil der Nutzerdaten mit der entsprechenden Nutzer-ID verknüpft und dient fortan zur Authentifizierung des Nutzers gegenüber dem System.

Der zweite Teilbereich betrifft die Zuordnung der registrierten Nutzer zu den Schlössern, die sie verwenden dürfen (siehe Abbildung 4). Diese Zuordnung regelt den Zugang zu Standorten, Gebäuden, Abteilungen oder einzelnen Räumen. Um auch größere Schließanlagen mit vielen Organisationseinheiten effizient verwalten zu können, wurde dieser Verwaltungsbereich am Prinzip des gruppen- und rollenbasierten Zugriffsmanagements nach dem Modell der Role Based Access Control (RBAC) gemäß ANSI-Norm 359-2004 ausgerichtet. Dieses Modell ist seit vielen Jahren in Betriebssystemen und international verbreiteten Softwarelösungen etabliert.

Dabei erhalten einzelne Nutzer in der Regel keine direkten Berechtigungen, sondern werden Gruppen zugeordnet. Diese Gruppen fassen mehrere Nutzer mit vergleichbaren Anforderungen zusammen und abstrahieren vom einzelnen Nutzer. Dadurch werden die Organisation vereinfacht, die Übersichtlichkeit erhöht und die Durchsetzung von Sicherheitsrichtlinien erleichtert.

Die Gruppen wiederum werden festgelegten Rollen zugeordnet, beispielsweise Mitarbeiter Entwicklung, Buchhaltung, Personal, Instandhaltung oder externer Dienstleister. Diese Rollen bilden die organisatorischen Strukturen einer Einrichtung ab und bündeln Zugangsregelungen für mehrere Schlösser. Die konkreten Schließberechtigungen werden schließlich den jeweiligen Rollen zugewiesen.

Zusätzlich können zeitliche Einschränkungen definiert werden. Beispiele hierfür sind Zugänge an Werktagen zwischen 8 und 18 Uhr für Mitarbeitende einer Abteilung oder zeitlich befristete Zugangsrechte für externe Dienstleister, wie etwa für Reinigung im Zeitraum vom 1.03.2025 bis zum 26.04.2025 jeweils zwischen 6 und 22 Uhr, wie in Abbildung 17 dargestellt. Diese zeitlichen Randbedingungen werden im System ähnlich wie Kalendereinträge behandelt. Hierfür kommt ein an xCal (RFC 6321) angelehntes Format zum Einsatz.

In Teilbereich Drei wird das Hinzufügen neuer Schlösser zum Schließsystem umgesetzt. Zunächst werden die grundlegenden Informationen des neuen Schlosses, wie eine eindeutige Schloss-ID, ein Bezeichner sowie der Einbauort, durch die Schließanlagenverwaltung angelegt. Das noch nicht initialisierte Schloss wird anschließend über eine direkte Verbindung mit den grundlegenden Systemdaten versorgt. Dazu zählen unter anderem Informationen zur verwendeten Blockchain, die zugehörigen Identifikationsdaten, die eigene Schloss-ID, die aktuelle Uhrzeit sowie weitere betriebsrelevante Einstellungen. Nach dieser Initialisierung kann das Schloss am vorgesehenen Standort eingebaut und regulär genutzt werden. Weitere Änderungen oder Aktualisierungen am Schloss sind anschließend nur noch nach Autorisierung durch die Schließanlagenverwaltung möglich.

Teilbereich Vier umfasst die Änderung und Löschung von Schließberechtigungen. Entsprechend dem gewählten Ansatz der rollenbasierten Zugriffskontrolle (Role Based Access Control, RBAC) erfolgen Anpassungen der Zugangsrechte nicht auf Ebene einzelner Nutzer, sondern über die Zuordnung und Anpassung von Gruppen und Rollen. Wird ein Nutzer beispielsweise aus der Gruppe Eingang Gebäude A entfernt und wurde diese Gruppe gemäß den RBAC-Empfehlungen definiert, ist ein Zugang nicht mehr möglich, da alle entsprechenden Schlösser Schließanfragen dieses Nutzers ablehnen.

Ändert sich die Funktion eines Nutzers, etwa durch einen Abteilungswechsel, wird die bisherige Rolle entfernt und eine neue Rolle zugewiesen. Der Nutzer erhält dadurch automatisch die für seine neue Position passenden Zutrittsrechte. Ein manueller Abgleich einzelner Türen oder Zeiträume ist nicht erforderlich. Dies reduziert Fehlerquellen, erhöht die Sicherheit und vereinfacht die Verwaltung deutlich. Insgesamt verbessert diese Strukturierung die Übersichtlichkeit der Zugangsregelungen und erleichtert die Durchführung von Änderungen erheblich.

Änderungen an den Schließregeln werden in Form eines aktualisierten, xCal-artigen Eintrags dokumentiert. Aus diesen Daten wird ein digitaler Fingerabdruck erzeugt, der gesichert an das jeweilige Schloss übermittelt wird. Das Schloss überprüft die Korrektheit der Daten, wertet die Informationen aus und aktualisiert seine internen Speicher. Werden einem Nutzer alle Gruppenzugehörigkeiten entzogen, ist eine weitere Nutzung der Schließanlage nicht mehr möglich; der Nutzer ist damit faktisch aus dem System entfernt.

Ergeben sich Änderungen in der Organisationsstruktur, bei der Anzahl der Schlösser oder an Sicherheitsrichtlinien, können die den jeweiligen Rollen zugewiesenen Berechtigungen zentral angepasst werden. So kann beispielsweise für die Rolle Reinigungspersonal der Zugang zu bestimmten Bereichen eingeschränkt oder zeitlich begrenzt werden. Alle Gruppen und alle zugehörigen Nutzer übernehmen diese Änderungen automatisch, ohne dass individuelle Berechtigungen angepasst oder physische Schlüssel ausgetauscht werden müssen.

Im Teilbereich Fünf wurde für den Transfer der Schließberechtigungen und weiterer Systemdaten eine Anbindung an bestehende externe Speicherlösungen (Off-Chain-Storage) wie Google Drive und Nextcloud umgesetzt. Zusätzlich ist die Bereitstellung ausgewählter Informationen über QR-Codes gemäß ISO/IEC 18004:2006 realisiert.

Zur Sicherstellung der Integrität der Daten wird ein kryptographischer digitaler Fingerabdruck mithilfe des etablierten Verfahrens SHA-256 gemäß RFC 6234 erzeugt. Dieser Fingerabdruck wird als Bestandteil von Transaktionen in den Blöcken der Blockchain gespeichert (siehe Abbildung 5). Die dort öffentlich zugänglichen Informationen ermöglichen sowohl die Überprüfung der Aktualität der Schließberechtigungen als auch einen wirksamen Schutz gegen unbemerkte Manipulationen.

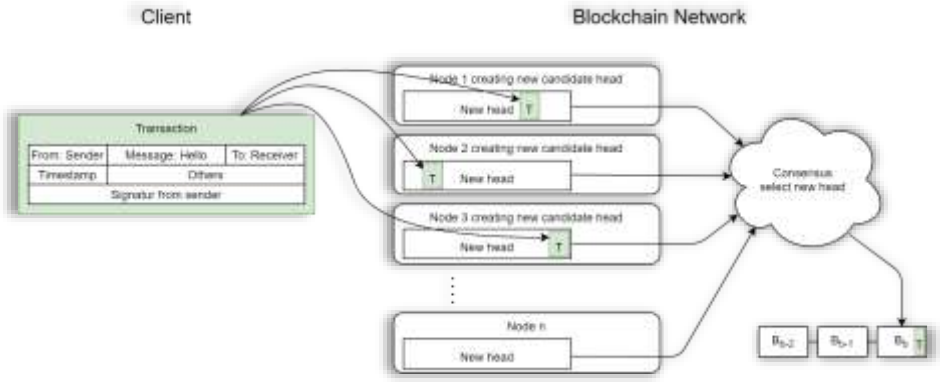


Abbildung 5: Prinzipieller Ablauf der Blockchain mit Erstellung von Transaktionen, Blockbildung, Auswahl eines Blockkandidaten und dem Anhängen eines neuen Kopfblocks an die bestehende Kette.

Die Verwendung einer externen Speicherlösung ermöglicht zum einen die kosteneffiziente Ablage der Schließregeln sowie weiterer Systemdaten, die aufgrund komplexer Organisationsstrukturen einen erheblichen Umfang annehmen können. Zum anderen erlaubt dieser Ansatz – sofern vom Betreiber der Schließanlage gewünscht – eine vollständige Kontrolle über die Daten und Systemkomponenten, etwa durch den Betrieb einer eigenen Speicherinfrastruktur.

Da in der Blockchain ausschließlich digitale Fingerabdrücke der Schließregeln gespeichert werden, deren Umfang im Wesentlichen konstant ist, bleiben die damit verbundenen Transaktionskosten gering. Gleichzeitig reduziert diese klare Trennung zwischen Nutzdaten und sicherheitsrelevanten Prüfinformationen die Angriffsfläche des Gesamtsystems und erschwert erfolgreiche Angriffe erheblich.

Die digitalen Fingerabdrücke der Schließberechtigungen werden als Bestandteil von Blockchain-Transaktionen gespeichert, denen zusätzliche Metadaten wie Zeitstempel, Absenderinformationen und digitale Signaturen beigefügt sind (siehe Abbildung 5). Jede Transaktion ist dabei einem Smart Contract zugeordnet, der die eindeutige Zuordnung zur jeweiligen Schließanlage sowie zur autorisierten Verwaltung sicherstellt.

Die Transaktionen werden über das Internet an mehrere zufällig ausgewählte Knoten des global verteilten Blockchain-Netzwerks übermittelt. Diese Knoten fassen mehrere Transaktionen zu Blöcken zusammen und ergänzen sie um blockspezifische Metadaten, wie beispielsweise den digitalen Fingerabdruck des vorherigen Blockchain-Kopfes. Jeder dieser Blöcke nimmt anschließend als Kandidat an dem Consensus-Verfahren teil, das einen Block als neuen Kopfblock auswählt und damit die Blockchain erweitert.

Durch die zufällige Verteilung der Transaktionen, die Eigenschaften des Consensus-Mechanismus sowie die kryptographische Verkettung der Blöcke ist eine unerkannte Manipulation der gespeicherten Informationen praktisch ausgeschlossen. Die weltweite Verteilung des Blockchain-Netzwerks erschwert darüber hinaus eine gezielte Behinderung der Datenübertragung erheblich. Für die prototypische Umsetzung wurde die öffentlich zugängliche und weltweit verteilte Ethereum Classic Blockchain (ETC) eingesetzt, da sie die für das Projekt erforderlichen Eigenschaften zuverlässig bereitstellt.

Die smartphonebasierte Schließapp (siehe Abbildung 17) basiert auf dem Open-Source-Framework Flutter, das die plattformunabhängige Entwicklung von Anwendungen in der Programmiersprache Dart ermöglicht. Dadurch kann die App ohne umfangreiche Anpassungen auf verschiedenen Zielplattformen wie Android, iOS, Linux oder als Webanwendung eingesetzt werden.

Die Schließapp dient den Nutzern zur Anforderung von Schließaktionen sowie zur Verwaltung ihrer digitalen Identitäten, der dafür notwendigen kryptographischen Schlüssel und der Konfigurationsdaten der verwendeten Blockchain sowie der externen Speicherlösung. Zur Abbildung unterschiedlicher Rollen – etwa regulärer Mitarbeiter, technischer Dienst oder Administrator – können mehrere kryptographische Schlüssel erzeugt und mit unterschiedlichen Rechten versehen werden.

In der prototypischen Umsetzung ist zudem ein gesonderter Administrationsbereich in die Schließapp integriert. Für die Registrierung eines Nutzers bei der Schließanlagenverwaltung ist die Erstellung eines digitalen Schlüsselpaares auf Basis eines asymmetrischen Public-Key-Authentifizierungsverfahrens erforderlich. Der private Schlüssel verbleibt dabei stets beim Nutzer und dient als digitaler Identitätsnachweis. Der öffentliche Schlüssel kann hingegen auf unterschiedlichen Wegen, beispielsweise als QR-Code, an die Verwaltung übermittelt werden. QR-Codes sind international standardisiert (ISO/IEC 18004:2006) und mit einer Vielzahl von Endgeräten zuverlässig lesbar, wodurch eine sichere und manipulationsresistente Übertragung gewährleistet wird.

Darüber hinaus realisiert die Schließapp die Zwischenspeicherung der Schließberechtigungen. Hierzu lädt sie automatisiert die Daten aus der externen Speicherlösung sowie den aktuellen Stand der Blockchain herunter. Diese Aktualisierungen erfolgen in regelmäßigen Intervallen, deren Dauer vom Nutzer in den Einstellungen der App angepasst werden kann. Eine manuelle Aktualisierung ist ebenfalls möglich, setzt jedoch – ebenso wie die automatische Aktualisierung – eine bestehende Internetverbindung voraus.

Unabhängig von einer Internetverbindung kontaktiert die Schließapp alle Schlösser der Schließanlage, die sich in Bluetooth-Reichweite befinden, und übermittelt ihnen die aktuellen Berechtigungsdaten. Da die App den zuletzt bekannten Datenstand kennt, werden jeweils nur die seitdem hinzugekommenen Änderungen übertragen. Dies ermöglicht einen ressourcenschonenden und effizienten Datentransfer, ohne andere Dienste zu beeinträchtigen. Eine zusätzliche Sicherung der Datenintegrität innerhalb der App ist nicht erforderlich, da ausschließlich das Schloss die Daten auswertet und die Entscheidung über eine Schließaktion trifft. Die geladenen Daten verbleiben auf dem Endgerät und werden bei späterer Gelegenheit an weitere Schlösser übermittelt.

Für die zuverlässige Kommunikation zwischen den Systemkomponenten wurden etablierte Protokolle und Werkzeuge eingesetzt. Die Anbindung an die Blockchain erfolgt über die Internetverbindung mithilfe der bewährten Open-Source-Software Geth. Die Kommunikation zwischen Schließapp und Schlössern erfolgt über Bluetooth Low Energy (BLE), welches eine energieeffiziente Verbindung bei gleichzeitig ausreichender Datenrate und Sicherheit bietet. Über definierte GATT-Profile werden Zugriffsbefehle, Statusinformationen und Rückmeldungen ausgetauscht. Dadurch wird eine hohe Kompatibilität mit gängigen Mobilgeräten sowie ein geringer Energieverbrauch sowohl auf Schloss- als auch auf App-Seite erreicht.

Das innerhalb dieser Kommunikation verwendete Authentifizierungsprotokoll zur Identifikation des Nutzers orientiert sich am seit Jahrzehnten erprobten und weltweit verbreiteten Secure Shell Authentication Protocol (RFC 4252). Dies unterstützt eine klare Trennung von Zustands- und Steuerinformationen, erleichtert die Fehlerbehandlung und fördert eine modulare und robuste Systemarchitektur.

Durch die konsequente Anlehnung an etablierte und international verbreitete Standards wie RBAC, xCal, QR-Code und die Ethereum-Blockchain wird ein grundsätzlich herstellerunabhängiger Datenaustausch ermöglicht. Gleichzeitig können bestehende, häufig Open-Source-basierte Softwarekomponenten genutzt werden. Dies erhöht die Zuverlässigkeit, Stabilität und Betriebssicherheit des Systems bei hoher Transparenz und Interoperabilität. Die Unabhängigkeit von kommerziellen Herstellern erleichtert zudem die Weiterentwicklung sowie die zeitnahe Umsetzung von Fehlerkorrekturen.

Die Integration der Verwaltungsfunktionen als gesonderter Bereich innerhalb der Schließapp erlaubt es berechtigten Personen, administrative Aufgaben ortsunabhängig durchzuführen, beispielsweise bei kurzfristigen Änderungen oder im Notfall. Dadurch entfällt die Notwendigkeit separater Verwaltungssoftware oder stationärer Zugriffspunkte. Dies reduziert sowohl den Schulungsaufwand als auch die benötigte IT-Infrastruktur. Die Verwaltungsfunktionen sind strukturell in Bereiche zur Verwaltung von Nutzern, Gruppen und Rollen, zur Zuweisung und zum Entzug von Schließberechtigungen sowie zum Einrichten neuer Schlösser unterteilt.

Die Entwicklung der Schlosselektronik erfolgte in mehreren Iterationen mit dem Ziel einer schrittweisen Miniaturisierung. In jeder Entwicklungsstufe wurden sowohl die technische Funktionalität weiter verfeinert als auch die physische Bauform verkleinert, um schließlich einen kompakten Prototypen zu realisieren, der sich direkt in marktübliche Türsysteme integrieren lässt.

Zu Beginn der Hardwareentwicklung wurde auf Basis der funktionalen Anforderungen ein erstes Systemkonzept erstellt (siehe Abbildung 6). Dieses Konzept stellt die wesentlichen Akteure und Komponenten des Chainlock-Schließsystems sowie deren Interaktionen dar. Die grundlegenden Bauteile, darunter Steuerungseinheit, Energieversorgung, Bluetooth-Modul, mechanische Aktoren und die smartphonebasierte Schließapp, lagen konzeptionell vor. Die detaillierte Ausgestaltung sowie mögliche Anpassungen oder Weiterentwicklungen bestehender Systeme – etwa durch Projektpartner – waren zu diesem Zeitpunkt noch Gegenstand weiterer Untersuchungen. Die frühen Planungen dienten primär dem Funktionsnachweis und dem Abgleich technischer Abhängigkeiten und orientierten sich noch nicht an der späteren finalen Bauform.

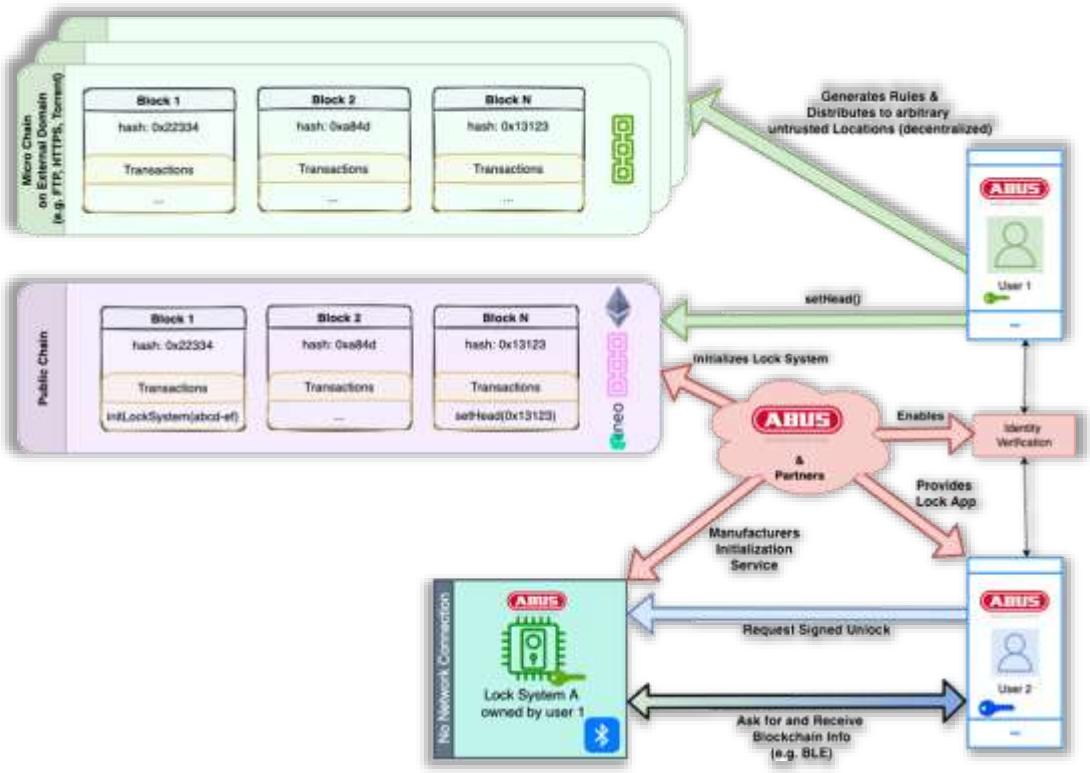


Abbildung 6: Schematische Darstellung des Chainlock-Systems. Das Schließsystem verfügt über keine eigene Netzwerkverbindung, während der Betreiber bzw. Administrator keinen physischen Zugang zur Wartung benötigt. Sämtliche für den Betrieb erforderlichen Informationen werden sicher über einen grundsätzlich nicht vertrauenswürdigen Übertragungskanal, nämlich das Smartphone des schließenden Nutzers, an das Schloss übermittelt.

Im Verlauf der ersten Komponentenprobungen zeigte sich, dass der ursprünglich präferierte und eingesetzte Arduino Nano 33 BLE Sense Rev1 durch einen leistungsfähigeren Mikrocontroller vom Typ Teensy 4.1 in Kombination mit einem zusätzlichen Bluetooth-Modul ersetzt werden musste. Dieser Schritt war erforderlich, da der Arduino Nano BLE Sense trotz seiner kompakten Bauform, der integrierten Bluetooth-Low-Energy-Funktionalität und weiterer Zusatzfunktionen in mehreren zentralen Bereichen – insbesondere hinsichtlich der Programmierbarkeit und der verfügbaren Systemressourcen – die geforderten technischen Anforderungen nicht vollständig erfüllte.

Die erste reale Umsetzung des Systems bestand daher neben diesem Komponentenwechsel aus einem prototypischen Hardwareaufbau mit handelsüblichen Bauteilen auf Steckbrettern und offenen Verdrahtungen. Diese Bauweise ermöglichte es, unterschiedliche Hardwarekonfigurationen effizient zu erproben und insbesondere auch komplexe Fehleranalysen und Diagnosen durchzuführen (siehe Abbildung 7).

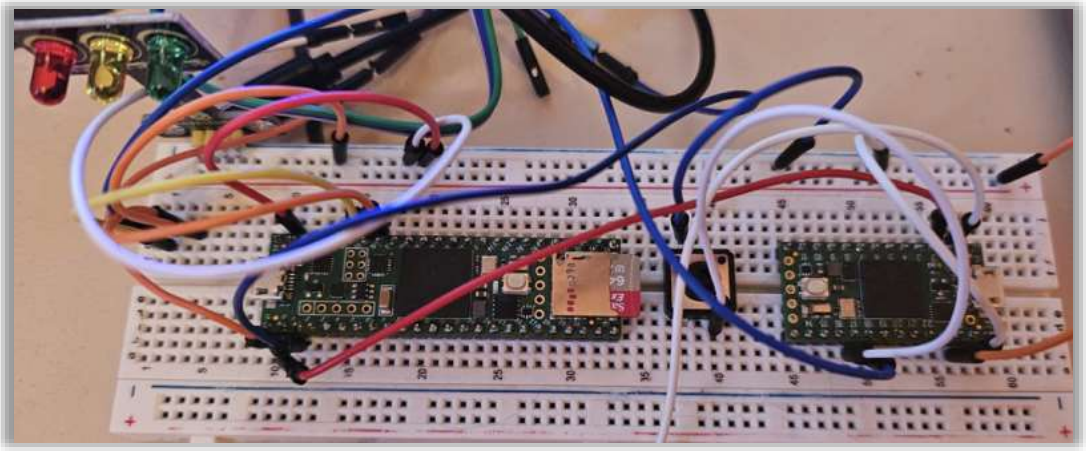


Abbildung 7: Erste Entwicklungsumsetzung der Hardware eines Chainlock-Schlosses auf einem Steckbrett. (Links) Hauptplatine mit Prozessor, internem Arbeitsspeicher, SD-Kartenslot sowie Verkabelung zum (rechts) Bluetooth-Modul. (Mitte) Buzzer zur akustischen Rückmeldung. (Oben links) farbige LED-Elemente zur visuellen Statusanzeige.

Der beschriebene Entwicklungsstand realisierte bereits die zentralen Grundfunktionen des Systems, darunter die Verarbeitung von Blockchain- und Berechtigungsdaten sowie das Öffnen des Schlosses über die Schließapp mittels Bluetooth. Mit Abmessungen von etwa 16 × 5 × 3 cm war dieser Prototyp jedoch noch deutlich größer als das angestrebte Zielprodukt. Er diente insbesondere der Validierung der Kommunikationswege, der Ansteuerung der Aktoren, der Analyse des Energieverbrauchs sowie der Untersuchung von Bearbeitungs- und Reaktionszeiten.

Die ursprünglich vorgesehene, auf zwei Komponenten verteilte Realisierung sah vor, den bei ABUS eingesetzten, erprobten und energieeffizienten Nordic NRF52832-Chip sowohl für die Bluetooth-Kommunikation als auch für die direkte Steuerung des Schließzylinders zu verwenden. Im Rahmen der Komponentenprobungen zeigte sich jedoch, dass sich die Programmierdetails dieses Chips in wesentlichen technischen Aspekten erheblich unterschieden. Eine Weiterverwendung hätte grundlegende Änderungen an der Hardwareprogrammierung, an der Schließapp sowie an der Blockchainanbindung erfordert und wurde daher verworfen.

Um diese umfangreichen Anpassungen zu vermeiden, wurde stattdessen das weit verbreitete und kostengünstige Bluetooth-Low-Energy-Modul Adafruit Bluefruit LE UART Friend eingesetzt. Dieser Austausch machte zwar zusätzliche Erprobungen notwendig, da einzelne Funktionen trotz vorhandener Dokumentation teilweise abweichend implementiert werden mussten, erlaubte jedoch eine stabilere und besser kontrollierbare Integration. Gleichzeitig ergab sich daraus die Notwendigkeit, die Ansteuerung des Schließzylindermotors vollständig durch den Teensy zu realisieren.

Die durchgeführten Erprobungen und die daraus resultierenden Zwischenstände lieferten wertvolle Erkenntnisse zur räumlichen Anordnung der Komponenten, zur Wärmeentwicklung sowie zum Energieverbrauch des Systems.

In weiteren Entwicklungsschritten wurden die Hardwareaufbauten schrittweise kompakter ausgeführt. Hierzu kamen Lochrasterplatinen, eine festere Verdrahtung sowie eine optimierte Anordnung der Bauteile zum Einsatz. Zusätzlich wurden ein Display zur Anzeige relevanter Verarbeitungs- und Diagnoseinformationen, zusätzlicher Arbeitsspeicher (RAM) sowie die Motoransteuerung integriert (siehe Abbildung 8).

Dieser wichtige Zwischenstand basiert auf dem Teensy 4.1 mit einem ARM Cortex-M7 Prozessor mit einer Taktfrequenz von 600 MHz, einer SD-Karte zur Datenspeicherung sowie zusätzlichen 128 MB NAND-Flash zur Zwischenspeicherung von Verarbeitungsergebnissen. Die Kommunikation mit

der Schließapp erfolgt weiterhin über das Bluetooth-Modul Adafruit Bluefruit LE UART Friend, während das integrierte Display Informationen zum aktuellen Schlossstatus bereitstellt.

Die von ABUS im Produkt Cylox (siehe Abbildung 9) bereits eingesetzten Motoren zur Schließzylindersteuerung konnten erfolgreich verwendet werden. Die Energieversorgung aller Komponenten erfolgt über eine CR2-3V-Batterie, die sich für den vorgesehenen Einsatzzweck als geeignet erwiesen hat. Die für die Hardware-Realisierung des Chainlock-Schlosses erforderlichen Komponenten sind damit in einer kompakten Bauform umgesetzt und konnten im Zusammenspiel mit der Schließapp, der Blockchain sowie den externen Speicherdiensten als Gesamtsystem erprobt und demonstriert werden.

Abbildung 8: Entwicklungsprototyp des Chainlock-Schlosses mit Teensy 4.1 inklusive SD-Karte und Flash-Speicher (unten), Bluetooth-Modul (rechts) sowie Display (links oben). Die Batterie und die zugehörige Verkabelung befinden sich auf der Unterseite der Trägerplatte.

Abbildung 9: ABUS Cylox One als Beispiel eines kommerziell vertriebenen elektronischen Schließsystems mit integrierter Elektronik

Mit Abmessungen von etwa 8 × 5 × 3 cm, einer Prüfzeit der Blockchaindaten von jeweils über 20 Sekunden sowie einem insgesamt noch hohen Energieverbrauch war dieser Entwicklungsstand zunächst auf prototypische Schlosstypen mit größerer Bauform beschränkt. Entsprechende Demonstratoren sind in Abbildung 10 dargestellt und wurden im Rahmen des Demonstratortags 2024 präsentiert.

Abbildung 10: Vergleich unterschiedlicher Schließlösungen und Prototypen.
(Links oben) Entwicklungsprototypen des Chainlock-Systems mit Teensy 4.1, Bluetooth-Modul und Display.
(Links unten) Beispielhafte Integration der Elektronik in die Schlosskomponente eines ABUS Fahrradbügelschlosses.
(Rechts) Darstellung eines kommerziell vertriebenen Fahrradbügelschlosses mit konventionellem Schließzylinder

Aufbauend auf dem beschriebenen Demonstrationsmuster konnten gezielte Weiterentwicklungs- und Optimierungsmaßnahmen sowohl auf technischer als auch auf funktionaler Ebene identifiziert und umgesetzt werden. Die zunächst eingesetzten handelsüblichen Komponenten sind grundsätzlich flexibel ausgelegt und für ein breites Spektrum an Einsatzszenarien geeignet. Für den im Projekt verfolgten Anwendungsfall – insbesondere die Verarbeitung von Blockchaindaten, die Bluetooth-Kommunikation mit der Schließapp sowie die Ansteuerung des Schließzylindermotors – wird jedoch nur eine klar abgegrenzte Teilmenge dieser Funktionen benötigt.

In diesem Zusammenhang konnten bestehende kabelbasierte Verbindungen durch speziell angepasste Leiterplattenlösungen ersetzt werden. Darüber hinaus war es möglich, nicht benötigte Schnittstellen und Komponenten, wie etwa Anschlüsse für CAN-Bus, Ethernet oder Audio sowie einzelne LED-Elemente, vollständig zu entfernen. Durch eine gezielte Neupositionierung der verbleibenden elektronischen Bauteile und die Entwicklung eines kompakteren, angepassten Platinenlayouts konnte eine mehrlagige Anordnung der Elektronik realisiert werden, wie sie in Abbildung 11 und Abbildung 12 dargestellt ist.

Diese Maßnahmen führten zu deutlichen Einsparungen beim Energieverbrauch sowie zu einer erheblichen Beschleunigung der Prüfung der Blockchaindaten auf etwa 3 Sekunden. Für eine material- und kostenoptimierte Fertigung wurden im Platinenlayout beide Lagen zunächst als eine gemeinsame Leiterplatte produziert. Die Trennung der einzelnen Lagen erfolgt erst nach dem Bestücken der Platine mit den mikroelektronischen Bauteilen, wie in Abbildung 12 (rechts) gezeigt.

Im Rahmen der Layoutentwicklung wurden gemäß den verfügbaren Herstellerangaben geeignete Speicherchips zur Zwischenspeicherung von Systemdaten beschafft und in das Design integriert. Während der Umsetzung traten jedoch erhebliche Schwierigkeiten auf. Die Ursachen konnten erst nach intensiver Analyse sowie nach dem Austausch mit Community- und Supportkanälen identifiziert werden und lagen in einer unzureichenden, unübersichtlich strukturierten oder teilweise eingeschränkten Dokumentation des verwendeten Bauteils. In der Folge musste der Speicherchip ersetzt werden, was zusätzliche Komplexität und Verzögerungen im Entwicklungsprozess verursachte.

Auch die Energieeffizienz des Gesamtsystems stellte im Verlauf der Entwicklung eine wiederkehrende Herausforderung dar. Insbesondere der während der Erprobungsphase notwendige Wechsel zwischen Netzbetrieb und Batteriebetrieb erforderte wiederholt technische Anpassungen und Optimierungen. Die dabei gewonnenen Erkenntnisse flossen in die weitere Auslegung der Hardware ein und bildeten eine wichtige Grundlage für die nachfolgenden Miniaturisierungs- und Effizienzmaßnahmen.

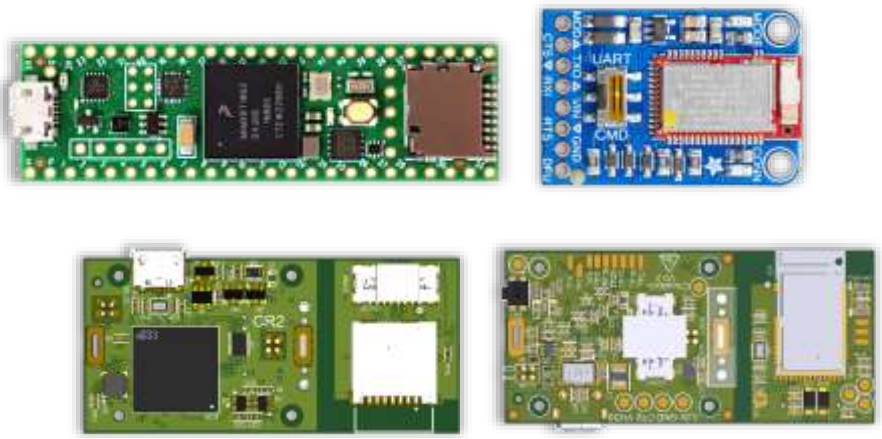


Abbildung 11: Darstellung der Elektronikkomponenten im gleichen Maßstab.
(Oben) Generische Versionen des Teensy 4.1 sowie des Adafruit Bluefruit LE UART Friend.
(Mitte und unten) Unter- und Oberseite der auf die für den Anwendungsfall notwendigen Komponenten reduzierten und teilweise neu angeordneten Versionen beider Ausgangsplatinen

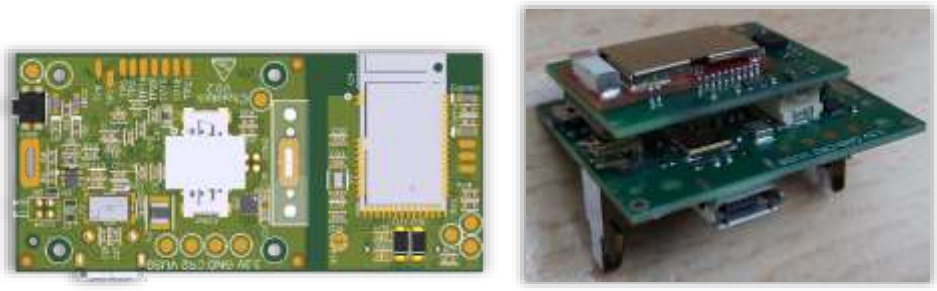


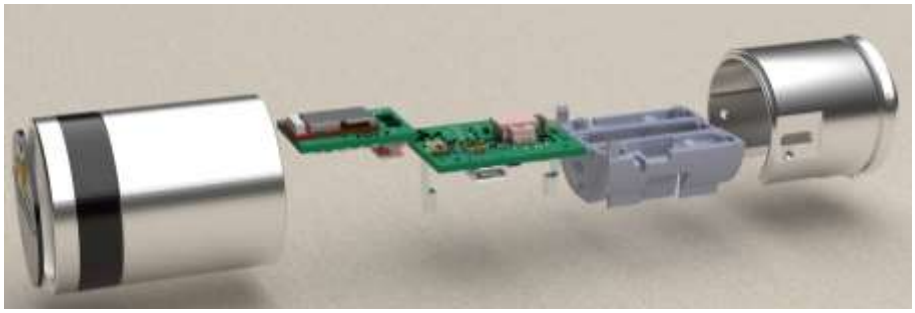
Abbildung 12: Umsetzung des optimierten Platinenlayouts.
(Links) Der senkrechte, dunkelgrün markierte Bereich im rechten Teil der Platine dient dem gezielten Auftrennen der Leiterplatte nach der Bestückung.
(Rechts) Die daraus entstehenden getrennten Platinenbereiche ermöglichen eine mehrlagige Anordnung der Elektronik und damit eine effizientere Ausnutzung des verfügbaren Bauraums im Zylinderknauf.

Nach der Ausstattung mit Batteriekontakten, mechanischen Trägerstrukturen, LED-Elementen sowie dem Anschluss des Schließmotors kann die entwickelte Elektronikeinheit in den inneren Metallorb des Zylinderknaufs integriert werden. Der Einbau ist innerhalb eines verfügbaren Innendurchmessers von 26 mm und einer Innenlänge von 36 mm realisierbar (siehe Abbildung 13).

Die äußere Knaufkappe schließt den Zylinder vollständig ab und sorgt für eine Versiegelung der Elektronik gegenüber äußeren Einflüssen. Dadurch wird der Knauf sowohl gegen Umwelteinwirkungen wie Staub und Feuchtigkeit als auch gegen mechanische Manipulations- und Aufbruchsversuche geschützt, wie schematisch in Abbildung 14 dargestellt.

Abbildung 13: Integration der Elektronik in den Zylinderknauf.
(Links) Mehrlagige Elektronikplatinen oberhalb des weißen Batteriefachs, mit LED-Elementen zur optischen Rückmeldung von Schließaktionen sowie der inneren Metallhülle des Knaufs.
(Rechts) Vollständig zusammengesetzter Zylinderknauf mit integrierter Elektronik.

Abbildung 14: 3D-Darstellung der Komponenten des Chainlock-Zylinderknaufs.



Durch die Ergänzung eines bei ABUS vorhandenen Schließzylinders sowie der erforderlichen Bauteile auf der Türinnenseite ergeben sich die in Abbildung 15 dargestellten Montageschritte, die in ihrer Gesamtheit das in Abbildung 16 gezeigte, in einen Türdemonstrator integrierte System bilden.

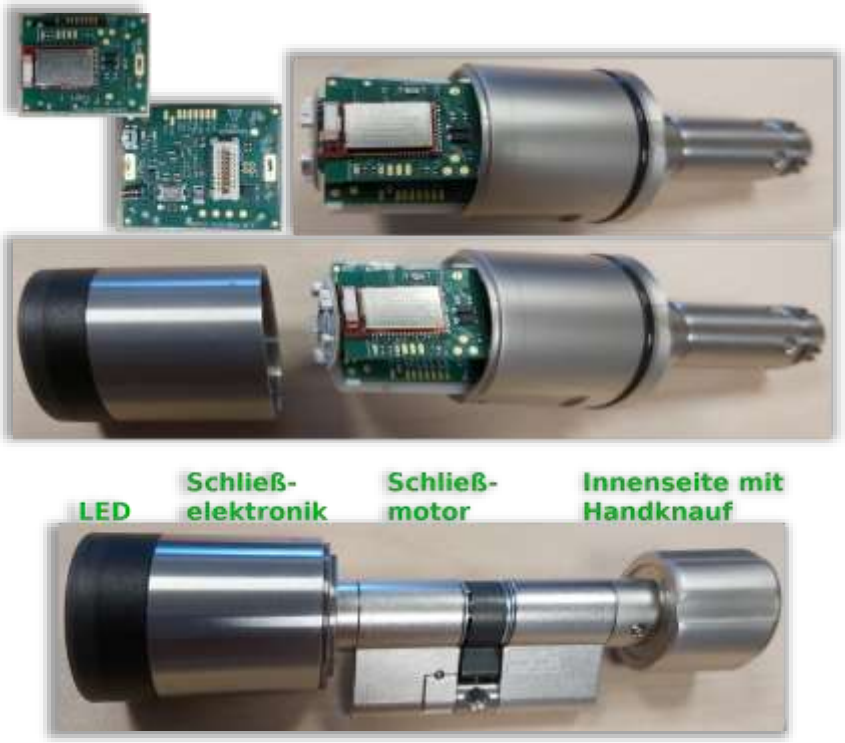


Abbildung 15: Komponenten und Montageschritte eines Chainlock-basierten Schließzylinders.
(Oben links) Einzelne elektronische Platinen.
(Oben rechts) Zusammengesetzte Steuereinheit mit mehreren Lagen und integriertem Batteriefach im Knaufkorb.
(Mitte) Einbau der Steuereinheit in das Schlossgehäuse mit aufgesetzter Knaufkappe.
(Unten) Fertig montierter Schließzylinder.

Abbildung 16: Transparente Demonstratortür mit einem Prototyp eines Chainlock-Schließzylinders, eingebaut in ein modernes Einsteckschloss

Die Analyse der aktuellen Lösung hinsichtlich des Nutzungsprofils der elektronischen Komponenten bei Datenübertragung, -verarbeitung und -speicherung zeigt deutliche Potenziale für den Einsatz von Hibernate- und Ruhezuständen. Durch das zeitweise Deaktivieren nicht benötigter Komponenten sowie eine dynamische Anpassung der Leistungsaufnahme an den aktuellen Arbeitsbedarf können weitere Einsparungen beim Energieverbrauch erzielt werden.

Nutzerinterface

Aus den definierten Use Cases wurden die unterschiedlichen funktionalen Anforderungen an die Interaktion mit der Chainlock-Schließanlage, den Nutzern sowie den Schlössern systematisch abgeleitet. Dabei wurden typische Anwendungsszenarien wie die Verwaltung von Schließberechtigungen, das Hinzufügen, Ändern und Entfernen von Nutzern und Schlössern sowie die Konfiguration der für den Betrieb notwendigen Systemeinstellungen erfasst, priorisiert und in konkrete Bedien- und Nutzungskonzepte überführt.

Diese strukturierte Herangehensweise ermöglichte eine klare Trennung der Funktionen, eine nachvollziehbare Benutzerführung sowie die Entwicklung rollenorientierter Benutzeroberflächen, beispielsweise für Administratoren und reguläre Nutzer. Gleichzeitig wurde darauf geachtet, den jeweiligen Nutzerrollen nur die tatsächlich benötigten Funktionen bereitzustellen, um die Bedienung übersichtlich und sicher zu gestalten.

Eine zentrale Anforderung an diese Nutzungs- und Verwaltungskomponente ist ihre Lauffähigkeit auf gängigen Systemplattformen, insbesondere auf mobilen Endgeräten mit Android, iOS sowie als Webanwendung. Ziel ist es, sowohl die Schließanlage als auch die zugehörige Anwendung möglichst unabhängig von spezifischen Betriebssystemen, herstellergebundenen Steuergeräten oder proprietären Frameworks zu gestalten. Eine feste Bindung an einzelne Anbieter (Vendor-Lock-in) sollte ausdrücklich vermieden werden, um die Zukunftssicherheit, Wartbarkeit, Erweiterbarkeit, Kosteneffizienz und Flexibilität des Systems zu gewährleisten.

Entsprechend wurden bevorzugt Technologien auf Basis offener Standards eingesetzt. Dazu zählen unter anderem die RFCs 4252, 6234, 6321 und 7748, die ISO/IEC 18004:2006, die ANSI-Norm 359-2004 sowie Blockchain-Technologien der Ethereum-Klasse mit internationaler Verbreitung. Weitere Auswahlkriterien waren eine lange Verwendungsdauer, eine große Nutzer- und Entwicklergemeinschaft sowie die Erwartung regelmäßiger Updates, Fehlerbehebungen und funktionaler Weiterentwicklungen.

Auf Grundlage dieser Anforderungen und Kriterien wurde für die Umsetzung des Nutzerinterfaces das Open-Source-Framework Flutter ausgewählt. Flutter ermöglicht die Entwicklung von Android-, iOS- und Webanwendungen auf Basis einer gemeinsamen Codebasis. Die gute Portierbarkeit auf unterschiedliche Endgeräte sowie die konsistente, moderne und performante Benutzeroberfläche unterstützen eine effiziente Bereitstellung der Anwendung. Gleichzeitig bietet Flutter eine hohe Entwicklungsgeschwindigkeit, eine große Community und umfangreiche Bibliotheken, ohne eine Bindung an einen einzelnen Plattformanbieter zu erzwingen.

Die korrekte Konfiguration von Flutter im Zusammenspiel mit weiteren Plugins und spezifischen Einstellungen stellte dabei teilweise eine technische Herausforderung dar. Durch eine konsequente Trennung von Frontend und Backend mittels standardisierter APIs konnte jedoch eine hohe Robustheit gegenüber Fehlern und Manipulationsversuchen erreicht werden. Gleichzeitig wird dadurch die Austauschbarkeit einzelner Systembestandteile ermöglicht, etwa bei funktionalen Erweiterungen oder zukünftigen Weiterentwicklungen. Der modulare Aufbau der Benutzeroberfläche erlaubt eine unabhängige Weiterentwicklung, Erweiterung oder Ersetzung einzelner Funktionsbereiche. Klar definierte Zustandsmodelle sorgen für nachvollziehbare Aktionen und konsistente Anzeigen auf Basis der jeweils aktuellen Daten und standardisierten Backend-Nachrichten. Dies erleichtert sowohl die Wartung als auch die Internationalisierung und die Anpassung an spezifische Anforderungen einzelner Betreiber von Schließanlagen.

Das Nutzerinterface der Schließapp (siehe Abbildung 17) besteht aus einer Hauptseite zur Anforderung von Schließaktionen sowie aus mehreren Verwaltungs- und Einstellungsseiten, die über ein Menü erreichbar sind. Eine eigene Seite dient dem Anlegen und Verwalten digitaler Schlüsselpaare zur Identitätsnachweisung sowie dem Einlesen öffentlicher Schlüssel anderer Nutzer. Weitere Seiten ermöglichen die Verwaltung der in der Schließanlage eingesetzten Schlösser, die Konfiguration der Blockchainanbindung, die Einstellung der externen Speicherverbindung sowie individuelle Darstellungs- und Nutzungseinstellungen. Aufgrund inhaltlicher Überschneidungen wurden die administrativen Funktionen direkt in die Oberfläche integriert und sind über eine entsprechende Autorisierung freischaltbar.

Die Kalenderseite stellt den zentralen Verwaltungsbereich der Schließanlage dar. Sie ermöglicht die übersichtliche Konfiguration, Zuweisung und Anpassung von Schließberechtigungen. Hierzu können beliebig viele Kalendereinträge erstellt und mit unterschiedlichen Datums-, Zeit- und Wochentags Einstellungen versehen werden, beispielsweise einmalige Termine, tägliche Berechtigungen, bestimmte Wochentage oder zeitlich begrenzte Zeiträume. Anschließend werden diesen Einträgen die relevanten Nutzer, Gruppen und Rollen zugeordnet, wodurch die Verbindung zwischen berechtigten Personen und der zugehörigen Hardware hergestellt wird.

Bei Änderungen, etwa an den gültigen Wochentagen, müssen lediglich die zeitlichen Parameter der betroffenen Kalendereinträge angepasst werden. Die anschließend von der Verwaltung ausgelöste Aktualisierungsaktion ermittelt automatisch alle Änderungen, aktualisiert die Datensätze im externen Speicher und erzeugt den entsprechenden Hash dieser Daten als Transaktionsinhalt für die Blockchain. Bei bestehender Internetverbindung werden sowohl der externe Speicher als auch die Blockchain aktualisiert, wodurch die Änderungen zuverlässig im gesamten Schließsystem verteilt werden. Alle Anpassungen werden dabei protokolliert und sind jederzeit nachvollziehbar. Dies erhöht sowohl die Transparenz der Verwaltung als auch die Sicherheit im operativen Betrieb.

Zur Beurteilung der Benutzerfreundlichkeit und Funktionalität wurden erste Untersuchungen mit ausgewählten Personen durchgeführt. Diese umfassten typische Use Cases wie das Öffnen eines Schlosses mit der Schließapp auf dem Smartphone sowie das Anlegen und Verwalten von Nutzern und deren Schließberechtigungen. Zentrale technische Abläufe, insbesondere der Datentransfer zum externen Speicher und zur Blockchain, der Download dieser Daten auf das Smartphone sowie deren spätere Übertragung an die Schlösser, wurden wiederholt und detailliert untersucht.

Die Tests lieferten wertvolles qualitatives Feedback zu Navigation, Reaktionszeiten und Verständlichkeit der Benutzeroberfläche, beispielsweise hinsichtlich eindeutiger Bezeichner bei der Schlüsselgenerierung oder verbesserter visueller Rückmeldungen bei Schließaktionen.

Weitere systematische Usability-Tests mit größerer Nutzerbasis sind vorgesehen, um die Benutzeroberfläche iterativ weiter zu optimieren. Insgesamt bildet die Umsetzung der Chainlock-Schließapp auf Basis von Flutter, in Kombination mit offenen Schnittstellen und einem modularen Design, eine tragfähige Grundlage für eine skalierbare, benutzerfreundliche und zukunftssichere Anwendung, die unabhängig von einzelnen Plattformanbietern betrieben und weiterentwickelt werden kann.

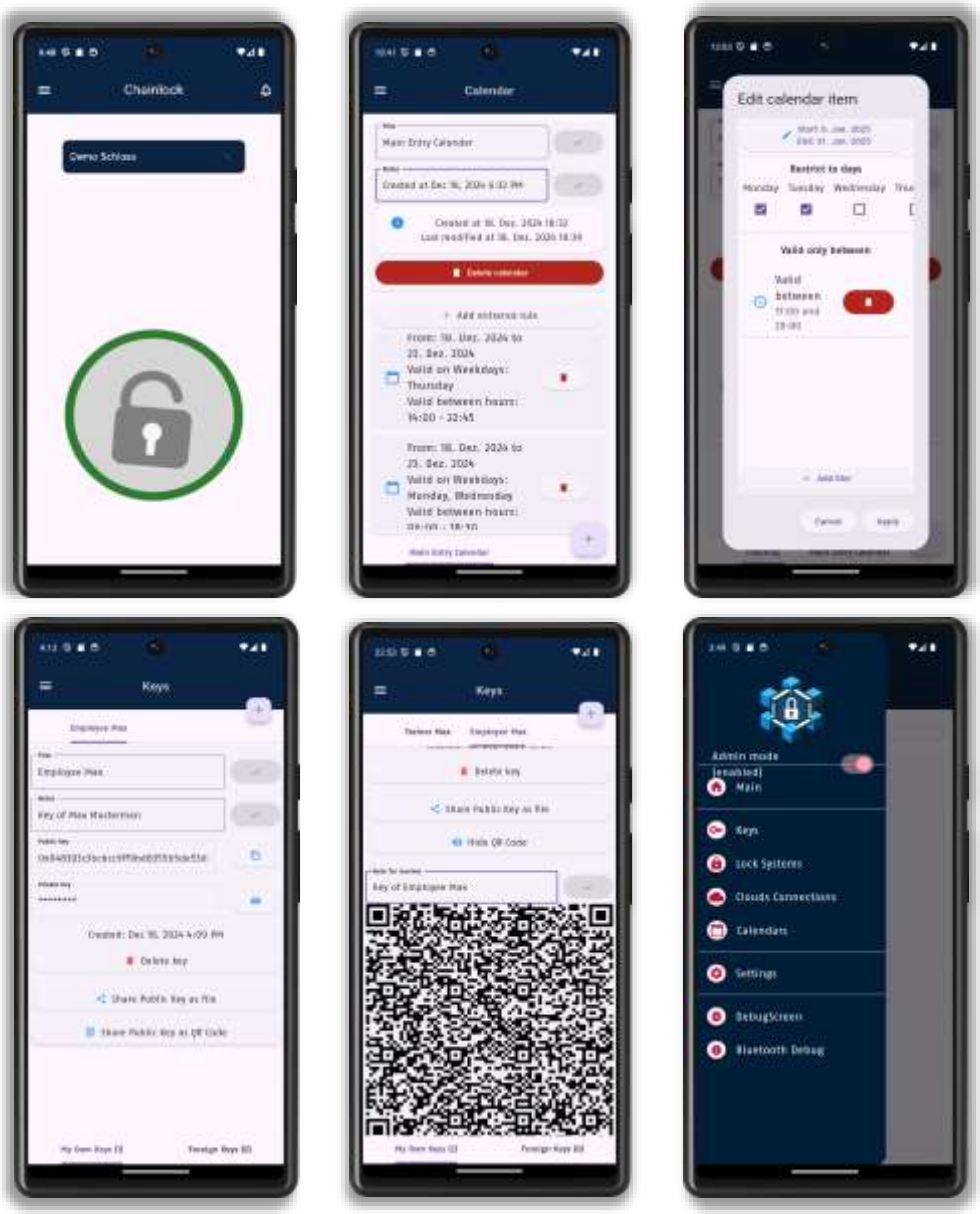


Abbildung 17: Screenshots der aktuellen Version der Steuerungs- und Verwaltungsapp.
(Oben) Ansicht mit Schlossauswahl, Anforderung von Schließaktionen, Übersicht der Schließzeiten einer Gruppe von Schlössern sowie dem Menü zur zeitlichen Festlegung von Berechtigungen.
(Unten) Menü zur Erstellung eines neuen digitalen Schlüssels für einen Nutzer oder eine Rolle sowie dessen Übertragung mittels QR-Code. Das Hauptmenü fasst die funktionalen Einheiten der Anwendung übersichtlich zusammen.

Arbeitspakete

AP 1 – 1.5: Technologierecherche, Blockchain-, Hardware- und Sicherheitsanalyse sowie Use-Case-Definition

Mit Beginn des Projekts Chainlock und dem damit verbundenen Entwicklungsprozess wurden mehrere zentrale Arbeitsschwerpunkte parallel bearbeitet. Ein wesentlicher Fokus lag zunächst auf einer systematischen Technologierecherche zu bestehenden Lösungen, Standards und etablierten Verfahren im Bereich elektronischer Zutrittskontroll- und Schließsysteme. Diese umfasste unter anderem die Analyse von Blockchain-Technologien, Kommunikationsmöglichkeiten moderner Smartphones, kryptographischer Verfahren zur Schlüsselverwaltung sowie Konzepte zur plattformunabhängigen Entwicklung mobiler Anwendungen, insbesondere für Smartphones.

Ein weiterer Schwerpunkt bildete die Analyse existierender Hardwaresysteme, die für den Einsatz in elektronischen Schließsystemen geeignet sind. Dabei wurden unterschiedliche Bauformen, Größen und Formfaktoren betrachtet sowie die damit verbundenen technischen Möglichkeiten, Einschränkungen, Sicherheitsanforderungen und potenziellen Risiken untersucht. Ergänzend dazu wurden relevante Anwendungsfälle (Use Cases) für das angestrebte Schließsystem definiert, die sich an typischen Einsatzszenarien orientieren. Diese drei Arbeitsschwerpunkte bildeten die konzeptionelle Grundlage für Architekturentscheidungen, Schnittstellendesigns sowie die Auswahl geeigneter Hardware- und Softwarekomponenten.

Im Rahmen der Recherchen lag der Fokus auf der Identifikation von offenen, sicheren, erprobten, erweiterbaren und standardisierten Technologien, die sich gut in ein modulares Gesamtsystem integrieren lassen. Besondere Beachtung fanden dabei Aspekte wie Interoperabilität, langfristige Wartbarkeit, Energieeffizienz und Miniaturisierbarkeit. Darüber hinaus wurde gezielt nach Technologien mit verfügbaren Open-Source-Implementierungen und einer aktiven Nutzer- und Entwicklergemeinschaft gesucht, um Vendor-Lock-in-Effekte zu vermeiden und eine unabhängige Weiterentwicklung zu ermöglichen. Als Ergebnis dieser Recherche wurden unter anderem Technologien auf Basis der RFCs 4252, 6234, 6321 und 7748, der ISO/IEC 18004:2006, der ANSI-Norm 359-2004 sowie Blockchain-Technologien der Ethereum-Klasse identifiziert und priorisiert.

Die Recherche zu geeigneten Hardwaresystemen erwies sich als besonders anspruchsvoll. Trotz nahezu identischer Spezifikationen und Dokumentationen existieren bei vielen Komponenten zahlreiche unterschiedliche Realisierungen mit teils erheblichen Detailabweichungen. Einzelne Funktionen sind zwar spezifiziert, erweisen sich jedoch erst bei der praktischen Erprobung als eingeschränkt nutzbar oder inkompatibel. Dies führte im Projektverlauf mehrfach zu Anpassungen und zum Austausch von Hardwarekomponenten, wie am in Abbildung 14 dargestellten Prototypaufbau nachvollzogen werden kann.

Parallel zur Technologierecherche wurden die zentralen Use Cases des Schließsystems entwickelt und dokumentiert. Diese umfassen typische Anwendungsszenarien wie die Anforderung von Schließaktionen per Smartphone, die Verwaltung von Nutzern und Schließberechtigungen sowie das Hinzufügen neuer Schlösser. Die Use Cases wurden in enger Abstimmung mit ABUS erarbeitet und dienten als Leitfaden für die Systemarchitektur, die Gestaltung der Benutzeroberflächen, die Sicherheits- und Kommunikationskonzepte sowie die Definition der Hardwareeigenschaften. Ausgehend von den in Abbildung 1 dargestellten realen Anforderungsszenarien ergaben sich die in Abbildung 2 gezeigte Systemstruktur sowie der in Abbildung 3 dargestellte Anwendungsablauf.

AP 2 – 3.4: Implementierung von Frontend, Backend, Schloss, Kommunikation, Schnittstellen und Proof of Concept

Im weiteren Projektverlauf wurden die definierten Systemfunktionen in mehreren iterativen Entwicklungszyklen umgesetzt. Der Fokus lag dabei auf der schrittweisen Realisierung eines funktionsfähigen Gesamtsystems, das sowohl die Frontend- und Backend-Komponenten als auch die Schlosshardware umfasst. Durch diesen Ansatz konnten wiederholt Untersuchungen, Tests und Demonstrationen einzelner Entwicklungsstände durchgeführt werden.

Das Frontend wurde zunächst als Lösung mit zwei getrennten Anwendungen konzipiert: einer App für reguläre Nutzer und einer separaten Administrationsanwendung. Aufgrund der erheblichen funktionalen Überschneidungen erfolgte jedoch frühzeitig eine Umstellung auf eine einheitliche App, die einen gesonderten, über entsprechende Einstellungen aktivierbaren Administrationsbereich enthält (siehe Abbildung 17). Nach der vorangegangenen Technologierecherche wurde hierfür das Framework Flutter eingesetzt. In der prototypischen Umsetzung wurden zentrale Use Cases realisiert, darunter die Anforderung von Schließaktionen, die Zuweisung zeitlich begrenzter Berechtigungen sowie die Verwaltung von Nutzern.

Das Backend umfasst zum einen die im Hintergrund der Schließapp bereitgestellten Funktionen zur Verwaltung von Schlössern, Nutzern, Gruppen, Rollen und Schließberechtigungen sowie die Anbindung an den externen Speicher und die Blockchain. Zum anderen übernimmt es die automatisierte Kommunikation mit dem externen Speicher, der Blockchain und den in Reichweite befindlichen Schlössern, um die Berechtigungsdaten innerhalb der Schließanlage aktuell zu halten. Der Ablauf orientiert sich dabei an der in Abbildung 3 dargestellten Systemlogik.

Parallel zur Softwareentwicklung wurde ein funktionaler Hardwareprototyp entwickelt, der ein physisches Schloss mit integrierter Elektronik zur Steuerung der Nutzung kombiniert. Der ursprünglich vorgesehene Arduino Nano 33 BLE Sense Rev1 musste dabei frühzeitig durch den leistungsfähigeren Teensy 4.1 in Kombination mit dem Adafruit Bluefruit BLE-Modul ersetzt werden, um die Bluetooth-Kommunikation mit der Schließapp, die Datenspeicherung sowie die erforderlichen kryptographischen Berechnungen zuverlässig umzusetzen. Die entsprechenden Entwicklungsstände sind in Abbildung 7, Abbildung 8 und Abbildung 10 dargestellt.

Für die Interaktion zwischen Schließapp, externem Speicher und Blockchain wurden bestehende Flutter-Plugins genutzt, die die Kommunikationsprotokolle der jeweiligen Speicheranbieter, beispielsweise Google Drive und Nextcloud, implementieren. Aufgrund der Vielzahl möglicher Nutzungsszenarien und Konfigurationsoptionen stellte deren Einbindung eine technische Herausforderung dar. Für die Kommunikation zwischen Schließapp und Schloss wurden zusätzliche Plugins eingesetzt und das darin enthaltene rudimentäre Protokoll um ein eigens definiertes Kommunikationsprotokoll erweitert. Dieses ermöglicht sowohl den Austausch größerer Teile der Blockchain als auch die Übertragung einzelner, noch fehlender Blöcke sowie von Differenzen bei der Aktualisierung der Schließberechtigungen.

Durch die jeweils partielle Funktionsfähigkeit einzelner Zwischenstände konnten die zu diesem Zeitpunkt implementierten Features gezielt untersucht, Schwachstellen frühzeitig identifiziert und entsprechende Anpassungen vorgenommen werden. Dies betraf sowohl softwareseitige Komponenten als auch mikroelektronische Bauteile. Auf diese Weise konnten einzelne Teile der Funktionskette – etwa die Nutzerverwaltung, die Blockchain-Kommunikation oder konkrete Schließaktionen – nachvollziehbar demonstriert werden, unter anderem im Rahmen von Demonstratortagen. Der abschließende Nachweis der Gesamtfunktionalität bestätigt die technische Umsetzbarkeit des Systems und bildet die Grundlage für mögliche Tests im realen Einsatzumfeld.

AP 4 – 4.2: Ergebniskonsolidierung und Dokumentation

Die im Projektverlauf erarbeiteten Entwürfe, Konzepte, Teilergebnisse und Beschreibungen wurden systematisch in der eingesetzten Projektmanagementplattform Confluence zusammengeführt. In Verbindung mit dem integrierten Ticketsystem lassen sich sowohl der Projektverlauf als auch einzelne Arbeitsschritte, aktuelle Entwicklungsstände und getroffene Entscheidungen nachvollziehen.

Die Programmquellen, einschließlich Source Code, Assets, Konfigurationen der Buildumgebungen und Testdaten, wurden in der Quellenverwaltungsplattform GitHub versioniert und gesichert. Dadurch steht für mögliche Folgeprojekte sowie für externe Projektpartner eine strukturierte, belastbare und nachvollziehbare Wissensbasis zur Verfügung, die eine Weiterentwicklung oder Überführung der Projektergebnisse in andere Kontexte unterstützt.

Meilensteine

Meilenstein M1 wurde erfolgreich erreicht.

Im Rahmen dieses Meilensteins wurden die zentralen Use Cases des Projekts sowie die zugehörigen technischen Konzepte für alle beteiligten Systemkomponenten – insbesondere Schließapp, Schloss, Datenspeicher und Blockchain – systematisch erarbeitet und dokumentiert. Die Verarbeitungsprozesse der eingesetzten Blockchain-Technologie wurden umfassend analysiert. Dabei wurden relevante Eckdaten, unter anderem zu Kommunikationsschnittstellen, Speicherbedarf und Ressourcenverbrauch, ermittelt und bewertet.

In enger Zusammenarbeit mit einem extern beauftragten Sicherheitsexperten wurden einschlägige Sicherheitsrichtlinien recherchiert und auf die spezifischen Anforderungen des Projekts angewendet. Potenzielle Angriffsvektoren und Angriffsmethoden wurden identifiziert, bewertet und dokumentiert. Die daraus gewonnenen Erkenntnisse führten zu gezielten Anpassungen der Systemarchitektur und der Programmierung, ebenso wie zu Maßnahmen, die im Zusammenhang mit der angestrebten Miniaturisierung der Hardware erforderlich waren. Auf dieser Grundlage konnte eine kompakte und konsistente Umsetzung der vorgesehenen Systemlösung realisiert werden.

Die Meilensteine M2 und M3 wurden ebenfalls erreicht.

Es wurde ein lauffähiger Prototyp des administrativen Frontends zur Verwaltung der Schließanlage entwickelt, der die Verwaltung von Schlössern, Nutzern und Schließberechtigungen ermöglicht. Parallel dazu wurden die backendseitigen Anbindungen an den externen Speicher sowie an die verwendete Blockchain umgesetzt. Darüber hinaus stehen mehrere prototypische Demonstratoren mit angepasster Embedded-Hardware in unterschiedlichen Entwicklungsständen zur Verfügung.

Diese Demonstratoren wurden auf mehreren Demonstratortagen der Blockchain-Schaufensterregion Mittweida präsentiert und deren Zusammenspiel erfolgreich sowohl interessierten Besuchern als auch einem Fachpublikum demonstriert. Erste Untersuchungen zur Nutzbarkeit, Funktionseffizienz, Usability und Bedienbarkeit des Systems wurden durchgeführt und die gewonnenen Ergebnisse systematisch erfasst.

Die im Projekt entwickelten Konzepte sowie verschiedene Zwischenstände der Hard- und Software wurden im Jahr 2023 auf der internationalen Konferenz Pervasive Technologies Related to Assistive Environments (PETRA) am 05.07.2023, auf der Blockchain Autumn School (BAS) am 14.09.2023 sowie auf dem Demonstratortag der Blockchain-Schaufensterregion Mittweida am 15.09.2023 durch unser Projektpartner vorgestellt.

Im Jahr 2024 folgten weitere Beiträge und Präsentationen auf der International Conference on Computing, Networking and Communications (ICNC) am 19.02.2024, auf dem Demonstratortag der Blockchain-Schaufensterregion Mittweida am 18.09.2024, einschließlich eines Beitrags im MDR Sachsenspiegel, sowie

auf der internationalen 3rd Blockchain and Cryptocurrency Conference (B2C) am 17.10.2024.

Weitere Präsentationen und Demonstrationen der entwickelten Prototypen für ein breites Publikum wurden im Rahmen der Nacht der Wissenschaften der Hochschule Mittweida am 20.06.2025 sowie auf dem Demonstratortag 2025 geplant.

2. Vergleich des Stands des Vorhabens mit der ursprünglichen (bzw. mit Zustimmung des Zuwendungsgebers geänderten) Arbeits-, Zeit- und Ausgabenplanung.

Der Vorhabenstand entspricht der geplanten Verteilung.

3. Haben sich die Aussichten für die Erreichung der Ziele des Vorhabens innerhalb des angegebenen Berichtszeitraums gegenüber dem ursprünglichen Antrag geändert (Begründung)?

Nein.

4. Sind inzwischen von dritter Seite Ergebnisse bekannt geworden, die für die Durchführung des Vorhabens relevant sind? (Darstellung der aktuellen Informationsrecherchen nach Nr. 2.1 BNBest-BMBF 98).

Nein.

5. Sind oder werden Änderungen in der Zielsetzung notwendig?

Nein.

6. Erfindungen/Schutzrechtsanmeldungen und erteilte Schutzrechte, die vom ZE oder von am Vorhaben Beteiligten gemacht oder in Anspruch genommen wurden, sowie deren standortbezogene Verwertung (Lizenzen u.a.) und erkennbare weitere Verwertungsmöglichkeiten

Keine.

7. Fortschreibung des Verwertungsplans. Diese soll, soweit im Einzelfall zutreffend, Angaben zu folgenden Punkten enthalten.

Die grundlegenden Systemfunktionen wurden implementiert und im Rahmen der Prototypenentwicklungsphase erfolgreich nachgewiesen. Das im Projekt entwickelte System kann weiterentwickelt werden.

Für die weitere Entwicklung sind mehrere Maßnahmen vorgesehen. Dazu zählen insbesondere die für die Vermarktung notwendige Erhöhung der möglichen Schließzyklen des Schlossprototyps sowie dessen weitere energetische und elektronische Optimierung unter Berücksichtigung der Anforderungen einer industriellen Fertigung.

Mit freundlichen Grüßen,

Sebastian Müller
Bereichsleitung Entwicklung