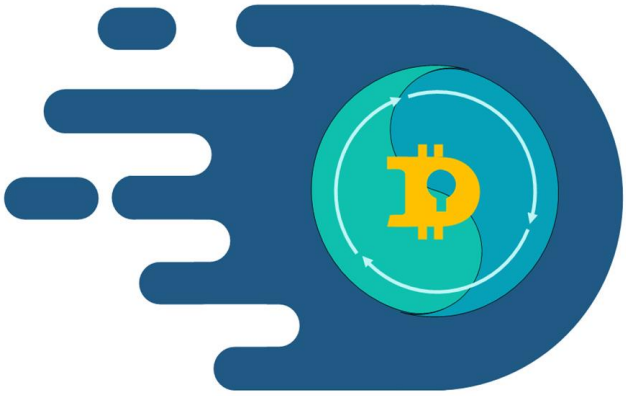
Verbundprojekt: TRustworthy Autonmous Driving by DEzentralized Authentication and Authorization - TRADE

Teilvorhaben: In-Car-DLT-Lösung

FKZ 16KIS1408

KIS – Kommunikationssysteme; IT-Sicherheit (VDI/VDE)
im Rahmen der Bekanntmachung
"KMU-innovativ: Informations- und Kommunikationstechnologien" des BMBF



Schlussbericht

Zuwendungsempfänger:
ETO GRUPPE TECHNOLOGIES GmbH

Laufzeit des Vorhabens: 01.07.2021 bis 30.06.2024

Inhalt

1 Projektübersicht ... 3
1.1 Projektbeschreibung und Zielsetzung ... 3
1.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde ... 5
1.3 Planung und Ablauf des Vorhabens ... 6
1.4 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde ... 7
1.5 Aktueller Stand der Wissenschaft und Technik ... 8
2 Verwendung der Zuwendung, Durchführung und Ergebnis des Vorhabens ... 9
2.1 Übersicht des Projektverlaufs ... 9
2.1.1 Erzielte Ergebnisse ... 9
2.1.2 Gegenüberstellung mit den vorgegebenen Zielen ... 18
2.1.3 Abweichungen in der Arbeits-, Zeit- und Ausgabenplanung ... 18
2.2 Wichtigste Positionen des zahlenmäßigen Nachweises ... 19
2.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit ... 19
2.4 Nutzen und Verwertbarkeit der Ergebnisse ... 19
2.4.1 Wirtschaftliche Verwertung ... 19
2.4.2 Wissenschaftliche/technische Verwertung ... 19
2.5 Erfolgte oder geplante Veröffentlichungen ... 20

Abbildungsverzeichnis

Abbildung 1 Projektphasenmodell des Gesamtvorhabens TRADE ... 6
Abbildung 2 Arbeitsschema ... 6
Abbildung 3 Schametisches Modell der Authentifizierung mit Tangle ... 9
Abbildung 4 Gesamtkonzept ... 10
Abbildung 5 Validierungsprozess ... 12
Abbildung 6 Lebensphasen eines ACS ... 13
Abbildung 7 Übersicht elektronische Kommunikation im Gesamtsystem ... 13
Abbildung 8 Konzept der Schlüsselratifizierung ... 14
Abbildung 9 Prozess der Validierung eines DID ... 15
Abbildung 10 Nucleo F446ZE zur Demonstration ... 16
Abbildung 11 Testfahrzeug und Demonstratoren ... 16
Abbildung 12 Anzeige im Testfahrzeug bei Anschluss des Plagiats ... 17
Abbildung 13 Anzeige im Display vergrößert ... 17

Dieser Bericht wurde erstellt unter Mitwirkung der Projekt-Mitarbeiter der ETO GRUPPE und der Projektpartner des Verbundvorhabens. Die ETO GRUPPE bedankt sich bei allen Mitwirkenden für die hervorragende Zusammenarbeit und die guten Ergebnisse.

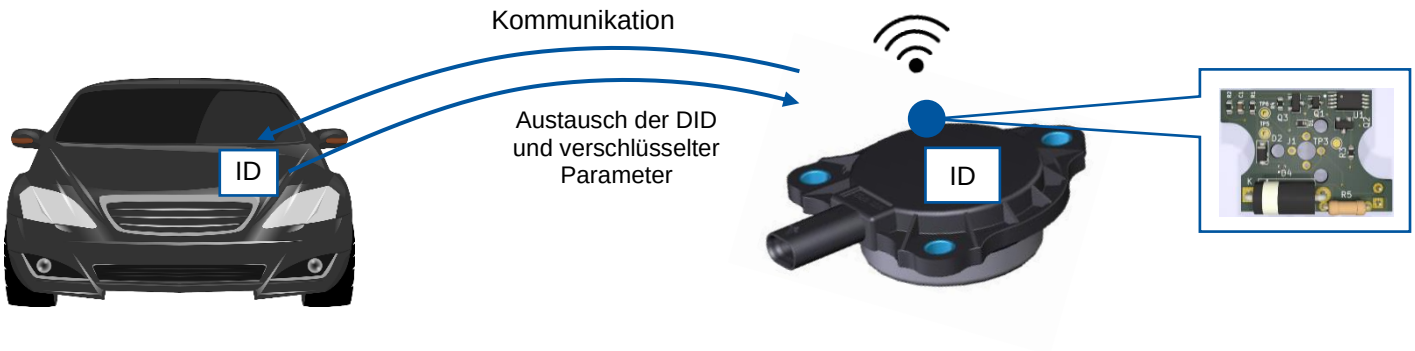
1 Projektübersicht

1.1 Projektbeschreibung und Zielsetzung

Das Forschungsvorhaben TRADE zielt auf die Entwicklung einer sicheren und skalierbaren Identitätsmanagement-lösung ab, die eine globale standardisierte Identitätsschicht für ein Automotive Cyber System ermöglicht.
Die Lösung soll Anforderungen sämtlicher Stakeholder sowie des automobilen Lebenszyklus berücksichtigen. Der Fokus liegt auf einer dezentralen Lösung, um eine Vielzahl von Stakeholdern einbinden zu können, den Anforderungen von KMUs gerecht zu werden und die Anbindung bestehender, herstellerspezifischer Lösungen zu ermöglichen. Mit der Konzentration auf die Schaffung eines dezentralen und kooperativen Authentifizierung- und Autorisierungsmechanismus wird die Grundlage für weitere sicherheitsrelevante Methoden geschaffen.

Wie kann effizient und dezentral Vertrauen und Kontrolle in einem vollkooperierenden Automotive Cyber System (ACS) entlang des automobilen Lebenszyklus erzeugt werden unter Berücksichtigung der Interessen und Beziehungen aller relevanter Stakeholder?

Das Ziel dieses Teilvorhabens ist eine In-Car-Lösung zu entwickeln, welche die Zugriffsrechte auf ACS bzw. auf dessen Teilsysteme (ECUs und DCUs) zulässt. Dazu sollen mittels zu entwickelnden Plagiatsschutzkomponenten die Handlungen „Authentifizierung“ und „Autorisierung“ in echten In-Car-Komponenten von ETO am Beispiel des Anwendungsfalls „Plagiatsschutz“ nachgewiesen werden.



Wesentliche Kernfunktionen von TRADE unterstützen die Vertrauensbildung von Identitäten in ACS und umfassen unter anderem:

- Etablierung eines offenen, aber kontrollierten Identitäts-Ecosystems für sichere Identitäten auf Basis von Distributed Ledger
- Eine Instanz zur Prüfung und Vergabe von verifizierbaren Berechtigungsnachweisen für Identitäten, bei dem nur die zugeordneten Stakeholder Rechte für ihre Teile des ACS vergeben können und das über Zugriffe auf Komponentenebene entscheiden kann
- Eine sichere Verwahrung der Berechtigungsnachweise zur nachvollziehbaren Authentifizierung und Autorisierung an jeder Komponente (z.B. Eletronic Control Unit, Sensoren, etc.) bzw. jedem Fahrzeug-Teilsystem oder Person

Ziel ist dabei eine hohe Transparenz und Auditierbarkeit von Zugriffen unter Berücksichtigung der Vielfalt von Stakeholdern. Um der Heterogenität des Ansatzes gerecht zu werden wird zur Umsetzung eine dezentrale Lösung basierend auf IOTA Distributed-Ledger-Technologien (DLT) angestrebt, wodurch erstmalig eine übergeordnete Sicherheitsarchitektur ermöglicht wird, die im Kontext ACS bisher nicht umsetzbar war. Unter Einbezug der IOTA DLTs ist es möglich, Interoperabilität, Dezentralität,

Transparenz, Sicherheit und Skalierbarkeit umzusetzen. Insbesondere die Dezentralität von IOTA ermöglicht eine Lösung, die auch von kleinen und mittleren Unternehmen gewinnbringend eingesetzt werden kann.

Als Anwendungsfall wird von ETO ein Sensor mit einem für Industrieprodukte entwickelten elektronischen kryptographischen Plagiatsschutz ausgestattet. Der Plagiatsschutz dient der Identifizierung von Komponenten und unterstützt durch das Identitätsprüfergebnis, dass die Verwendung von Plagiaten vermieden werden kann. Nach der Identifizierung eines Originalteils oder Plagiats werden Information an die Steuerung übermittelt, die die Entscheidung über die weiteren Schritte übernimmt. Für die Identifikation eines Plagiates wird ein Hardware Security Module (HSM) eingesetzt und asymmetrische kryptographische Protokolle zur manipulationssicheren Kommunikation verwendet.

Der von ETO bereits entwickelte Plagiatsschutz befindet sich bereits in einer Vor-Industrialisierungsphase und wird als Projektbeitrag von ETO den Kooperationspartnern zur Verfügung gestellt. Mit dem aktuellen technischen Stand werden Firmen in der Lage sein, Informationen zu erfassen, ob es sich um ein Originalbauteil handelt oder nicht. Im Rahmen dieses Projektes wird ETO diese Komponente dann detailliert im Rahmen der ACS Ansprüche weiterentwickeln und erforschen, inwieweit ein kryptographischer Plagiatsschutz sich in einem In-Car ACS Umfeld einsetzen lässt. Dafür werden auch Muster aufgebaut und in den elektrischen Steckern von Aktoren und Sensoren integriert. Zudem wird an ein Fahrzeugsteuergerät (bzw. eine DCU) eine zweite bereits entwickelte elektronische Einrichtung montiert, die die Abfrage des Plagiatsschutzelementes vornimmt und die Information an das Fahrzeugsteuergerät übergibt.

Diese elektronische Einrichtung kann im besten Fall in einem späten Projektverlauf als reine Softwarelösung direkt in ein Fahrzeugsteuergerät (bzw. eine DCU) integriert und getestet werden, wobei dies nur dann möglich ist, wenn ein Fahrzeughersteller dem Projekt ein entsprechendes Fahrzeug mit DCU Zugang zur Verfügung stellt.

Auch weitere grundlegende sicherheitsbedürftige Szenarien, wie das Aufspielen und Signieren von Flashware auf Board-Komponenten, das Ändern von Konfigurationseinstellungen, die Durchführung von Diagnosen am Fahrzeug und insbesondere eine Herstellerübergreifende C2C/C2I-Kommunikation werden untersucht und in eine Lösung übertragen. Dafür ist zunächst ein Rollen- und Berechtigungsmodell zu entwickeln (u. a. auf Basis der oben genannten Vorevaluierung mit Kunden), dass eine effiziente, nachvollziehbare, aber auch kontrollierte Interaktion mit dem ACS ermöglicht. Für eine einfachere Umsetzbarkeit der Modellierung des Gesamtkonzepts sollen die im Rahmen des Modells definierten ökonomischen und technischen Rollen den Stakeholdern „backend-seitig“ an der Peer-to-Peer-Identitäts-Plattform Authentifizierungs- und Autorisierungscredentials einfach zugewiesen werden können. Dabei wird auch darauf geachtet, dass das System verwaltbar bleibt und wesentliche sicherheitstechnische Funktionen wie z.B. die sichere Aushändigung des kryptographischen Materials, die transparente Abbildung, Verwaltung und der Entzug der Berechtigungen sowie das einheitliche Schema für die Anbindung der Stakeholder abbildet.

Dabei werden die folgenden Teilziele verfolgt:

- Anpassung an die ACS-Ansprüche, die im Rahmen des Projektes ermittelt.
- Integration der Entwicklungsergebnisse aus den Arbeitspaketen der filancore und THI.
- Entwicklung und Anpassung der In-Car-Lösung
- Herstellung und Montage der Muster
- Entwicklung und Anpassung der Abfrageeinheit eines Fahrzeugsteuergeräts
- Integration und Montage der Abfrageeinheit in das Fahrzeugsteuergerät

Die Verwertung der Projektergebnisse zielt auf die Ausstattung serientauglicher Produkte mit einer Kopierschutzlösung ab, die flächendeckend auf Basis der zu erarbeitenden Einsatzempfehlung zum sicheren und effizienten ACS-Betrieb eingesetzt werden können.

1.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Das Vorhaben „TRustworthy Autonmous Driving by DEzentralized Authentication and Authorization - TRADE“ ist ein Verbundvorhaben aus Industrie, Start Up und Hochschule. Die am Verbundvorhaben beteiligten Partner waren neben der ETO GRUPPE TECHNOLOGIES GmbH die filancore GmbH und die Technische Hochschule Ingolstadt.

Voraussetzungen zur Durchführung des Verbundvorhabens waren der Informationsaustausch zwischen den Partnern und die Bereitschaft zur Zusammenarbeit. Über einen Kooperationsvertrag zwischen den Parteien wurde die Zusammenarbeit formal geregelt und der Umgang mit bestehenden sowie neu erworbenen Schutzrechten festgelegt.

Die Voraussetzung für die im Vorhaben durchgeführten Arbeiten im Teilvorhaben „In-Car-DLT-Lösung“ des Verbundvorhabens TRADE waren die nachfolgend gelisteten Arbeitspakete, wobei die Arbeitspakete 1, 4, 6 und 8 keine wesentlichen Aktivitäten von ETO erfordern.

AP 1: Projektmanagement: Koordination des Porjektablaufs und Sicherstellung des Wissenstransfers; Leitung von filancore

AP 2: Anforderungen basierend auf Stakeholder, Lebenszyklus und Anwendungsszenarien: Relevante Stakeholder im Lebenszyklus eines Fahrzeugs werden analysiert. Mehrere typische Anwendungsszenarien für TRADE werden identifiziert. Aus den gewonnenen Informationen werden Anforderungen an TRADE definiert. Durch eine Bedrohungs- und Risikoanalyse in den Anwendungsszenarien werden relevante Sicherheitsanforderungen in TRADE erhoben und abschließend konsolidiert.

AP 3: Systemspezifikation: Entwurf der Gesamt-Systemarchitektur bestehend aus einer Grob-Sicherheitsarchitektur basierend auf der Risikoanalyse aus AP2, einem Konzept der Identitätsmanagementlösung sowie einem ersten Konzept der In-Car-DLT-Lösung. Analyse der Grobarchitektur mit Hinblick auf den Automotive-Einsatz und Ableitung eines geeigneten Identifikations- und Berechtigungsmodells für das Gesamtkonzept sowie die In-Car-Komponente.

AP 4: Integration „Registrierung-Verifizierungs-Verfahren“: Analyse verschiedener Verfahren zur Erzeugung von Vertrauen während der Registrierung und der Verifikation von Komponenten in einem System mit vielen Akteuren und Stakeholdern basierend auf dem in AP6 entwickelten Identitätsmanagementlösung am Beispiel der in AP 5 entwickelten Fahrzeugsensoren mit Authentifizierungsfunktion. Entwurf eines Vertrauensmodells für TRADE. Detailspezifikation des gewählten Vertrauensverfahrens als Basis für die Vertrauensbeziehung im Gesamtsystem und in den Anwendungsszenarien; Durchführung von filancore.

AP 5: Entwurf In-Car-DLT-Lösung: Detail-Entwurf der im ACS (am Beispiel Fahrzeugsensor) verwendeten und zu realisierenden Komponenten, basierend auf den identifizierten Randbedingungen aus AP2 und AP3 sowie unter Berücksichtigung der Konzepte aus AP4. Entwicklung eines Prüfverfahrens für die Inputparamter am ACS zur dezentralen Authentifizierung und Autorisierung. Überprüfung der Umsetzbarkeit hinsichtlich des Schlüsselmanagements und –Verfahrung im Automotive-Umfeld. Prototypische Umsetzung zur Idenitäts- und Berechtigungsprüfung am ACS

AP 6: Entwurf Identitätsmanagementlösung: Detail-Entwurf der Identitätsmanagementlösung. Die Lösung soll sicherstellen, dass nur Personen und Technical Clients auf ACS bzw. Fahrzeugsensoren zugreifen dürfen. Dabei bildet die Lösung eine Prüf-, Vergabe-, und Verwaltungsinstanz von Identitäten und Berechtigungen. Die Basis dafür bildet das definierte Identifikations- und Berechtigungsmodel; Durchführung von THI.

AP 7: Rapid Prototyping: Die in den AP 4-6 entwickelten Lösungen werden technisch zusammengeführt und projektbegleitend prototypisch implementiert, um die technische Machbarkeit laufend im Blick zu halten.

AP 8: Evaluierung: Die Leistungsfähigkeit der Lösung wird wissenschaftlich evaluiert. Dazu sollen neben konzeptioneller Analyse auch Angriffe auf die prototypische Implementierung durchgeführt und dokumentiert werden; Durchführung von THI.

1.3 Planung und Ablauf des Vorhabens

Der Durchführungszeitraum des Vorhabens war der 01.07.2023 bis 30.06.2024.

Die Arbeiten des Gesamt- sowie des Teilvorhabens „In-Car-DLT-Lösung“ folgten im Ablauf der Logik des Projektphasenmodells nach **Fehler! Verweisquelle konnte nicht gefunden werden.**. Die einzelnen Phasen sind durch Meilensteine abgegrenzt, bei denen die für die weiteren Arbeiten relevanten Ergebnisse des Teilvorhabens dem gesamten Projektteam vorgestellt wurden und die Kontrolle des Fortschritts des Vorhabens ermöglichten.

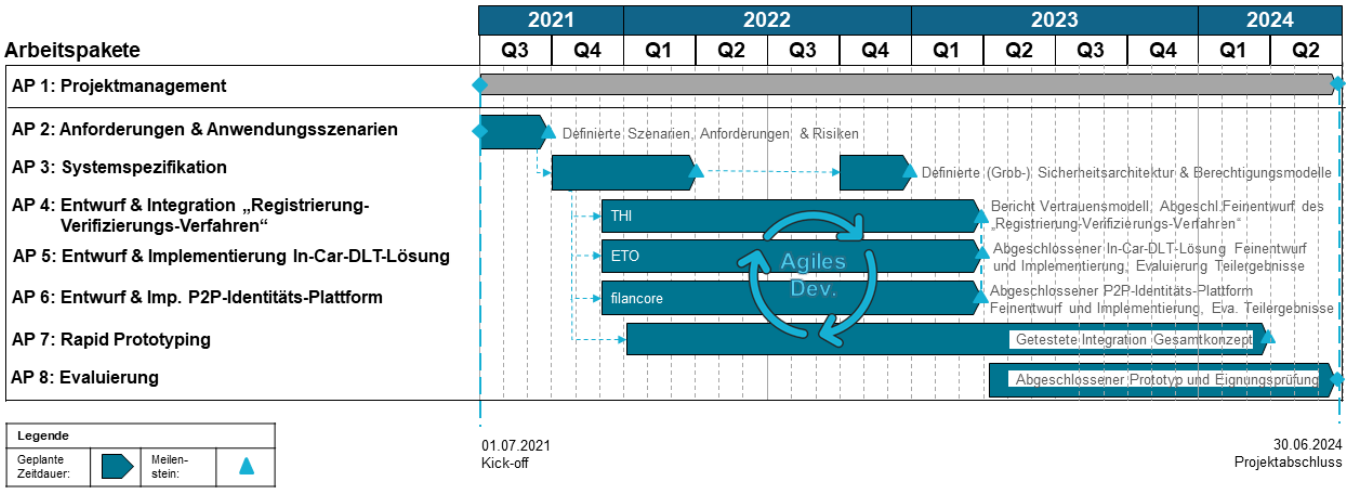


Abbildung 1 Projektphasenmodell des Gesamtvorhabens TRADE

Aus der Planung der Arbeitspakete ergeben sich die folgenden drei Phasen:

- Phase 1: Erstellung der Systemanforderung, Konzepterstellung und Systemspezifikation des Gesamtsystems
- Phase 2: Entwurf und Implementierung der In-Car-DLT-Lösung
- Phase 3: Evaluationsphase und Abschluss des Vorhabens

In den einzelnen Phasen wurden folgende Aufgaben durchgeführt:

<u>Phase 1:</u>

Die Systemanforderung dient der Anforderungsformulierung und der Abstimmung der einzelnen Arbeitspakete untereinander. Hierauf basierend wurde dann das Gesamtkonzept entwickelt, basierend auf folgendem Schema

Abbildung 2 Arbeitsschema

Konkret wurden folgende Arbeitsleistungen erbracht:

- Auswahl konkreter Anwendungsszenarien für die Projektbeteiligten
- Definition der Randbedingungen an das Gesamtsystem unter Berücksichtigung der verschiedenen Anwendungsszenarien, des Security-Lebenszyklus im automotive Bereich und spezieller Anforderungen von Fahrzeugen
- Ermittlung potentieller Risiken und Evaluation nach HEAVENS
- Erstellung eines Konzepts für das Gesamtsystem einschließlich des externen Elements Backend (filancore Identity Gateway)
- Erstellung eines Konzepts für die einzelnen Stufen des Lebenszyklus eines Fahrzeugs oder einer Fahrzeug-Komponente von Herstellung, Lagerung/Transport, Installation/Deinstallation und Betrieb
- Ausarbeitung des Verifikationskonzepts mit den Verifikationsmethoden, -ebenen, der Modellphilosophie und den Verifikationsstufen;
- Definition der Schnittstellen (intern und extern, erster Entwurf)
- Definition der Daten- und Kommunikationsbudgets (erster Entwurf)
- Definition der Daten- und Kommandoflüsse zwischen den einzelnen Elementen des Gesamtsystems
- Definition der Softwarearchitektur und der Software Hauptmodi
- Ausarbeitung eines Konzepts für die Datensicherheit und Nachweisbarkeit der Echtheit der Daten im Gesamtsystem mit dezentralen Identitäten (DID) und nachprüfbaren Zeugnissen (VC)

Phase 2:

Die Demonstratorphase dient der Feinentwicklung, der Erstellung und dem Test von Prototypen zu Demonstrationszwecken sowie der Überarbeitung der Konzepte und der Prüfung des Zusammenspiels der einzelnen Module.

- Feinentwurf der In-Car-DLT-Lösung unter Berücksichtigung des Gesamtkonzepts
- Nachweis der grundsätzlichen Machbarkeit
- Beschaffung von Material
- Inbetriebnahme der Prototypen der In-Car-DLT-Lösung
- Test aller elektrischen Schnittstellen
- Verifikation der Funktionsfähigkeit
- Durchführung von funktionalen Tests

Phase 3:

Die Phase 3 dient im Wesentlichen der Auswertung der Ergebnisse der einzelnen Arbeitspakete sowie der Erstellung der Abschlussberichte der Arbeitspakete und des Gesamtprojekts.

1.4 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

Das Internet hat längst Einzug in die Automobilindustrie gehalten – vernetzte Fahrzeuge und deren Datenaustausch mit Fahrzeugherstellern, Werkstätten, Versicherungen oder Ersatzteilproduzenten sind Realität. Dies ermöglicht neue Anwendungen und Geschäftsmodelle, birgt aber auch neue Risiken. Im Rahmen von Forschungsprojekten wie IUNO, das nationale Referenzprojekt zur IT-Sicherheit in Industrie 4.0 und SeDaFa (Selbstdatenschutz im vernetzten Fahrzeug) haben die Projektteilnehmer die Erkenntnis gewonnen, dass die reine Anpassung von PKI-basierten Mechanismen zur Authentifizierung an die Anforderungen der I4.0 oder in der Automobilindustrie nicht ausreichen, da die Abhängigkeit, Skalierbarkeit, der Lebenszyklus der Schlüssel, das Schlüsselmanagement (Verwaltbarkeit) und Widerrufung der zugrundeliegenden Zertifikate nicht mit den langen Laufzeiten der Maschinen und ACS in Einklang gebracht werden können. Zudem weisen gerade die ACS und ACS-Komponenten derzeit noch unüberwindbare Limitierungen hinsichtlich Rechenleistung und Geschwindigkeit bei Verwendung von kryptografischen Mechanismen auf, um eine kryptographisch abgebildete Maschinenidentität umfangreich implementieren und nutzen zu können. Der Bedarf für eine nachvollziehbare und dezentrale Lösung für

Identitäten zur Authentifizierung und Autorisierung mit günstiger technologischer Basis besteht jedoch weiterhin. TRADE setzt sich mit dieser Problematik auseinander, führt die Lösungsfindung logisch fort und überträgt die Erkenntnisse auf den Bereich einer dezentralen Identitätsmanagementlösung. Bislang existieren weder für das industrielle Identity Management im Kontext Industrie 4.0 oder für die Anwendungsszenarien im Automotive-Umfeld ausreichend belastbaren Ansätze.

Eine potenzielle Lösung weisen Distributed Ledger-Technologien auf, wenngleich die wissenschaftliche Basis für entsprechende Ansätze in der Breite für die Identifikation und den operativen Betrieb ökonomisch autonomer und vernetzter Systeme gering ist. Die DLT hat innerhalb der letzten Jahre enorme Aufmerksamkeit durch Forschung, Industrie und Medien erfahren. Nicht zuletzt durch die Forschungsarbeit der gemeinnützigen IOTA-Stiftung mit Sitz in Berlin und der anstehenden Standardisierung derselben konnte sich Deutschland in diesem Bereich einen signifikanten Vorsprung erarbeiten, den es zu nutzen gilt. Der Vorteil dieser Technologie besteht grundlegend darin, dass der IOTA DLT eher, im Gegensatz zu anderen DLT, wie ein Kommunikationsprotokoll operiert und eigens für das Internet der Dinge konzipiert wurde. Die IOTA-Technologie könnte zudem in Kombination mit dem W3C Entwurf „Decentralized Identifiers (DIDs) v1.0“ (W3C, 2020) einen Lösungsansatz für das Problem des Vertrauens und der Skalierbarkeit bieten.

So ist die Bereitstellung von Werkzeugen für Vertrauensinstanzen notwendig, die eine Identität für jeden Use Case bestätigt und diese anlegt. Hierbei muss sichergestellt werden, dass eine eineindeutige Digitale Identität genutzt wird, die nur besagter „Maschine“ bzw. Person zugewiesen wurde und nicht von unberechtigten Dritten kopiert oder verändert werden kann. Faktoren wie mehrere beteiligte Entitäten und die komplexe Interaktion zwischen Komponenten in einer Entität machen die Schaffung eines hohen Vertrauensniveaus in einem Netzwerk zu einer enormen Herausforderung. Mit dem W3C-Ansatz wird die Komplexität reduziert und die notwendigen Kommunikationsbeziehungen sicherer. So kann eine dezentrale Identität das Identitätsmanagement sowie den Austausch von Profilattributen stark vereinfachen und die Implementierung wiederverwendbarer Identitäten erreichen. Hinzu kommt, dass der Eigentümer oder das ACS selbst seine Identität kontrolliert und so eine übermäßige Datenverbreitung verhindern kann, indem der „Weg“ über überprüfbare Ansprüche / Anmeldeinformationen (Verifiable Credentials) ermöglicht wird. Vielmehr können erstmals die Bewältigung von Problemen bei Governance, Skalierbarkeit, Benutzererfahrung, Interoperabilität, dezentrales Schlüsselmanagement, Datenschutz und Sicherheit ausgeräumt werden.

Nachteilig ist, das dezentrale Identitäten bisher eine sorgfältige geschäftliche und technische Planung erfordern. Viele technische Fachleute im Bereich Sicherheits- und Risikomanagement sind mit dem Konzept jedoch nicht vollständig vertraut. Dies kann dazu führen, dass Unternehmen nicht darauf vorbereitet sind, sich schnell anzupassen, wenn diese Technologien in den nächsten zwei bis fünf Jahren häufiger eingesetzt werden. Das Projekt TRADE wird dabei die Problemstellung aufgreifen, analysieren und im Rahmen eines ACS Systems integrieren. Hierfür werden zunächst die Bedingungen für einen rein technischen Ansatz im Kontext einer ausgebenden Vertrauensinstanz untersucht und definiert.

Seit 2019 setzt sich die ETO intensiv mit der Entwicklung von smarten Sensoren und smarten Sensor-Aktoren-Modulen auf Basis von Blockchain und Distributed Ledger Technologien auseinander. Da im Bereich von smarten Komponenten der Schlüssel zum langfristigen technischen und wirtschaftlichen Erfolg liegt, werden schon seit Anfang 2018 gruppenübergreifend eigene F&E-Anstrengungen unternommen, die seit 2019 auf Blockchain und Distributed Ledger Technologien ausgerichtet werden.

1.5 Aktueller Stand der Wissenschaft und Technik

Es gibt analoge Mechanismen wie etwa das Einprägen von Seriennummern zum Plagiatsschutz. Diese sind jedoch weder fälschungssicher noch digital automatisiert prüfbar. Für einzelne komplexe Untersysteme – beispielsweise Navigationssysteme oder Multimediasysteme – oder digitale Autoschlüssel sind digitale Sicherungsmethoden über digitale Schlüssel oder Zertifikate vereinzelt zu finden, jedoch sind diese stets zentral angelegt und bedürfen einer „intelligenten“ Gegenstelle (beispielsweise Wallet-Funktion im Smartphone), welche auf Sensorseite nicht zu erwarten ist. ETO sind keine digitalen Schutzmechanismen für einzelne Sensoren und Aktor-Sensor-Module im automotive Bereich bekannt.

2 Verwendung der Zuwendung, Durchführung und Ergebnis des Vorhabens

2.1 Übersicht des Projektverlaufs

2.1.1 Erzielte Ergebnisse

2.1.1.1 Übersicht über das Gesamtsystem

Grundlage der sicheren und skalierbaren Identitätsmanagementlösung im Rahmen des Projekts TRADE sind - neben einem geeigneten Vertrauensmodell - dezentrale Identitäten (DIDs) und verifiable credentials (VCs). Dazu gibt es eine standardisierte Richtlinie, die für solch verteilte Identitäten festgelegt ist (https://www.w3.org/TR/did-core/). Ein DID besteht lediglich aus einem String, welche einen eindeutigen Identifier einer Entität (Nutzer, Gerät, Software etc.) repräsentiert. Der DID selbst dient zwar als Identifikator, für die Verwendung, also beispielsweise das Überprüfen einer Identität (Authentifizierung) oder das Signieren von Daten, sind stets weitere Informationen aus dem DID Document notwendig. Das DID Document ist ein JSON-Dokument, welches weitergehende Informationen zu der beschriebenen Identität enthält. Insbesondere findet man mindestens eine explizite Methode, mit denen sich der Besitzer des DID authentifizieren kann. Jede dieser Methoden ist eindeutig identifizierbar und umfasst meist einen Public Key sowie die Spezifikation des verwendeten Algorithmus. Das DID Dokument muss für jeden potentiellen Nutzer des Systems abrufbar sein und wird beispielsweise auf verteilten Datenbanken (Distributed Ledgern) abgelegt. Der zugehörige private Schlüssel befindet sich unter der Kontrolle des Inhabers der Identität. Die Authentifizierung kann wie folgt geschehen:

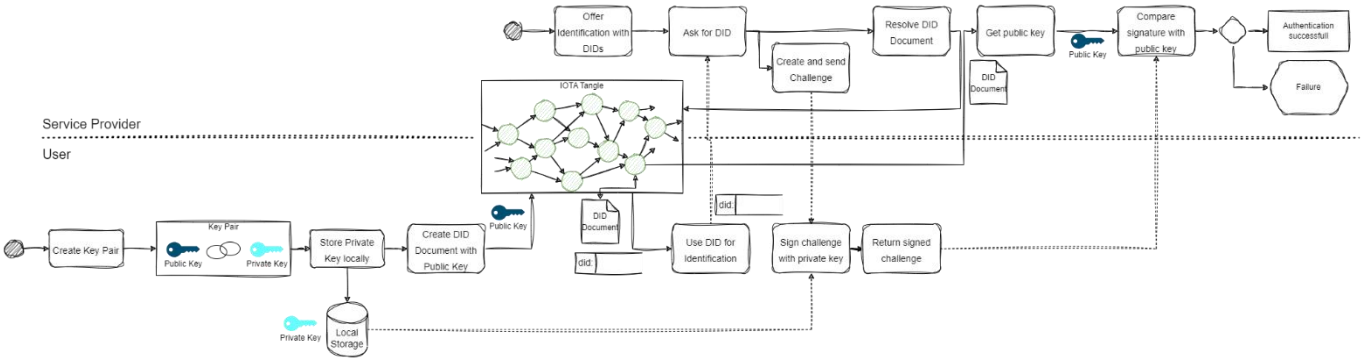


Abbildung 3 Schametisches Modell der Authentifizierung mit Tangle

Bei Verifiable Credentials (VCs) handelt es sich ebenfalls um einen offenen Standard, der mit DIDs verwendet werden kann. Sie haben das Ziel, Aussagen verifizierbar darstellen zu können. Die Art der Aussagen ist dabei nicht festgelegt, im Allgemeinen handelt es sich jedoch um Aussagen, die einer bestimmten Identität zugewiesen werden können. Mit ihrer Hilfe kann beispielsweise der Zusammenhang zwischen einem DID und einem anderen Identifier, etwa eine E-Mail Adresse oder ein Name, hergestellt werden. Will ein Nutzer bei einem Empfänger gewisse Aussagen nachweisen, so kann dies über einen VC erfolgen. Ob der Empfänger dem VC - auch bei korrekten Signaturen - vertrauen kann hängt vom Aussteller ab. Sofern dieser aus Sicht des Empfängers für das Ausstellen von VCs mit den entsprechenden Claims vertrauenswürdig ist, so kann auch dem spezifischen VC vertraut werden. Daher ist ein geeignetes Vertrauensmodell hier unabdingbar.

Aus Sicht des Datenschutzes ist das Verfahren äußerst datensparsam. Der Aussteller braucht die notwendigen Informationen, um den VC ausstellen zu können. Dies kann neben den reinen Angaben noch weitere Informationen umfassen, mit denen der Aussteller die Informationen verifiziert. Nach der

Übermittlung an den Halter des VC hat der Aussteller jedoch keinen Einfluss mehr auf die Verwendung des VC uns erfährt insbesondere nicht, wann und zu welchem Zweck dieser verwendet wird. Lediglich über die Invalidierung eines VC könnte noch eine Interaktion stattfinden, dies hängt jedoch vom konkreten Mechanismus ab. Werden für verschiedene Claims unterschiedliche VCs erstellt, können diese auch einzeln vorgelegt werden, was die Verknüpfung unterschiedlicher Informationen erschwert.

Die Zuweisung der Rechte an einen Nutzer über VCs kann als Attribut des Nutzers gesehen werden, weshalb das Konzept als eine Form der attributbasierten Zugriffskontrolle (ABAC attribute-based access control) gesehen werden kann. Darüber hinaus ist die Definition von Regeln (Policies) notwendig, welche für einen konkreten Fall angewendet entscheiden, ob der Zugriff zugelassen oder abgelehnt wird. Seitens ETO wurde ein Konzept entwickelt, welches die Definition von Policies in Verbindung mit VCs darstellt. Dabei wurde insbesondere das Zusammenspiel der unterschiedlichen Aktoren (OEM, ETO, filancore, IOTA-Tangle, 3rd-Party etc.) sowie die konkrete Anwendung im Umfeld von Fahrzeugen und deren Komponenten betrachtet. Das Konzept ermöglicht es, Policies für ABAC zu definieren, die in einem VC eingebettet sind und damit auch authentisch verteilt und eingesetzt werden können.

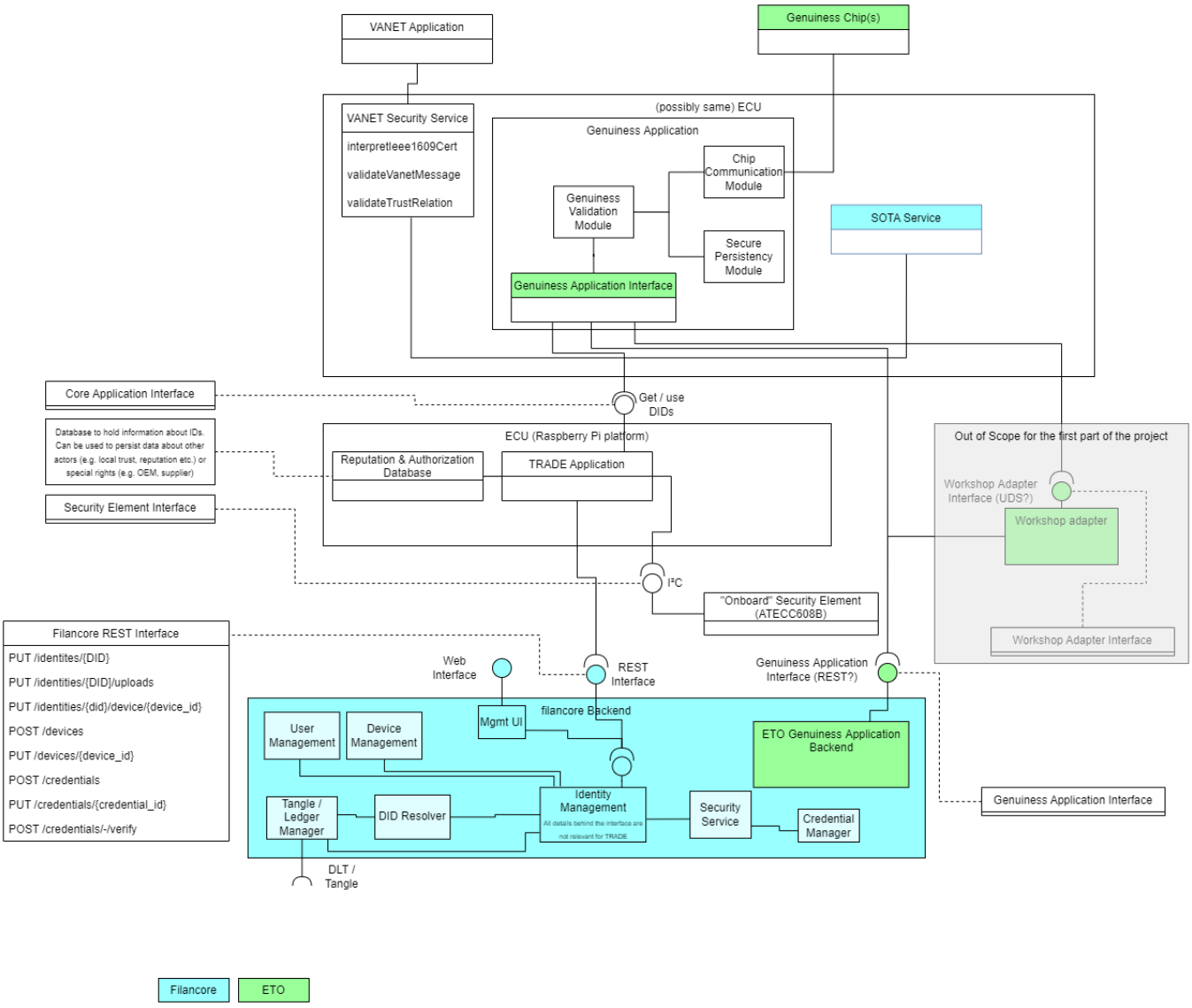


Abbildung 4 Gesamtkonzept

Häufig wird, um die Sicherheit und Wartbarkeit zu erhöhen, ein einzelner Zugangspunkt zum System modelliert, welcher die Zugriffskontrolle effektiv durchsetzt. Im erarbeiteten Konzept sollen notwendige Berechtigungen und Umstände, die für die Zugriffskontrolle verwendet werden, aus unterschiedlichen Regeln aufgebaut werden. Jede dieser Regeln für sich prüft einen bestimmten Aspekt des Zugriffs. Durch logische Verknüpfung entsteht dann das Gesamtresultat, ob ein Zugriff gewährt wird.

Für das Gesamtsystem braucht es demnach einen Ort, an dem DIDs und VCs erzeugt und verwaltet werden können, ein passendes Vertrauensmodell, welchen DIDs vertraut werden kann, sowie ein Berechtigungsmodell mit passend umgesetzten Policies zur Wahrung der Berechtigungen. Diese Bausteine werden für drei ausgewählte Use Cases, nämlich VANETs, SOTA Service sowie den DLT-Kopierschutz in Fahrzeugen aus mehreren miteinander agierenden Komponenten wie in Abbildung 2 ersichtlich zusammengestellt. Wesentliche Bestandteile sind das Backend, die On Board Application sowie die spezifischen Anwendungen wie die Genuiness Application.

2.1.1.1.1 Backend

Hauptbestandteil auf der Backend-Seite ist das Identity Gateway beziehungsweise Identity Management, welches hauptverantwortlich auf Seiten von filancore entwickelt wurde. Hier werden neben Standardanwendungen wie Signaturerstellung, Labeling und Geheimniswahrung die verschiedenen Identitäten (DIDs) und Berechtigungen (VCs) ausgestellt, verwaltet und an ein Distributed Ledger geknüpft.

2.1.1.1.2 On Board Application

Hauptbestandteil und Kern des Sicherheitskonzepts ist eine Verwaltungseinheit bzw. eine Fahrzeug-Applikation, welche im Fahrzeug zentral die Verwaltung der Identitäten, Berechtigungen und Schlüssel managet. Dabei greift dieser Teil auf einen sicheren Co-Prozessor oder eine sonstige Möglichkeit zur sicheren Speicherung von kryptographischem Material sowie zur sicheren Durchführung von kryptographischen Operationen zurück. Um abhängig vom geforderten Sicherheitslevel die Anforderung eines dedizierten Sicherheitsmoduls auch anpassbar zu machen, wird für das Konzept eine generische Schnittstelle modelliert. Der Zugriff auf die Applikation von Seiten der OEMs wird ebenfalls über eine generische Schnittstelle gewährleistet. Diese ist bewusst unabhängig von der konkreten Umgebung gewählt, um diese beispielsweise für AUTOSAR Adaptive zugänglich zu machen.

Die Applikation selbst bietet eine Schnittstelle an, über welche die letztendlichen (Kunden-) Funktionen die angebotenen Dienste verwenden kann. Mit dem Ledger kommuniziert die Applikation nur indirekt: Der Zugriff auf Daten des Ledgers geschieht über das Filancore-Backend.

2.1.1.1.3 Kopierschutz (Genuiness Application)

Exemplarisch wird hier das Szenario “Plagiatsschutz” als eines von drei Szenarien, welche im Rahmen von TRADE zentral für die Erstellung des Identifikations- und Authentifizierungssystem für ein Automotive Cyber System verwendet werden, betrachtet. In diesem Szenario geht es darum, die Echtheit von (Ersatz-)Teilen in einem Fahrzeug sowie deren fachgerechten Einbau überprüfen zu können. Dieses Szenario wurde als Demonstrator umgesetzt. Die Verifikation einer Komponente erfolgt nach gemäß Abbildung 5.

Da die komplette Verantwortung beim OEM liegt und von diesem das System gesteuert wird, kann die Vertrauensbildung innerhalb dieser Funktion **ebenfalls zentral beim OEM landen.** Dies bedeutet, dass alle schützenswerten Interaktionen vom OEM freigegeben werden müssen und diese vom OEM autorisiert werden. Durch den dezentralen Ansatz wäre es aber auch denkbar, diese Aufgabe bei einem Zulieferer oder dem Zulieferer der jeweiligen Teile zu verorten. Darüber hinaus muss dem OEM eine dynamische Verwaltung der VCs in der Nutzungs- als auch der Verwertungsphase eingeräumt werden.

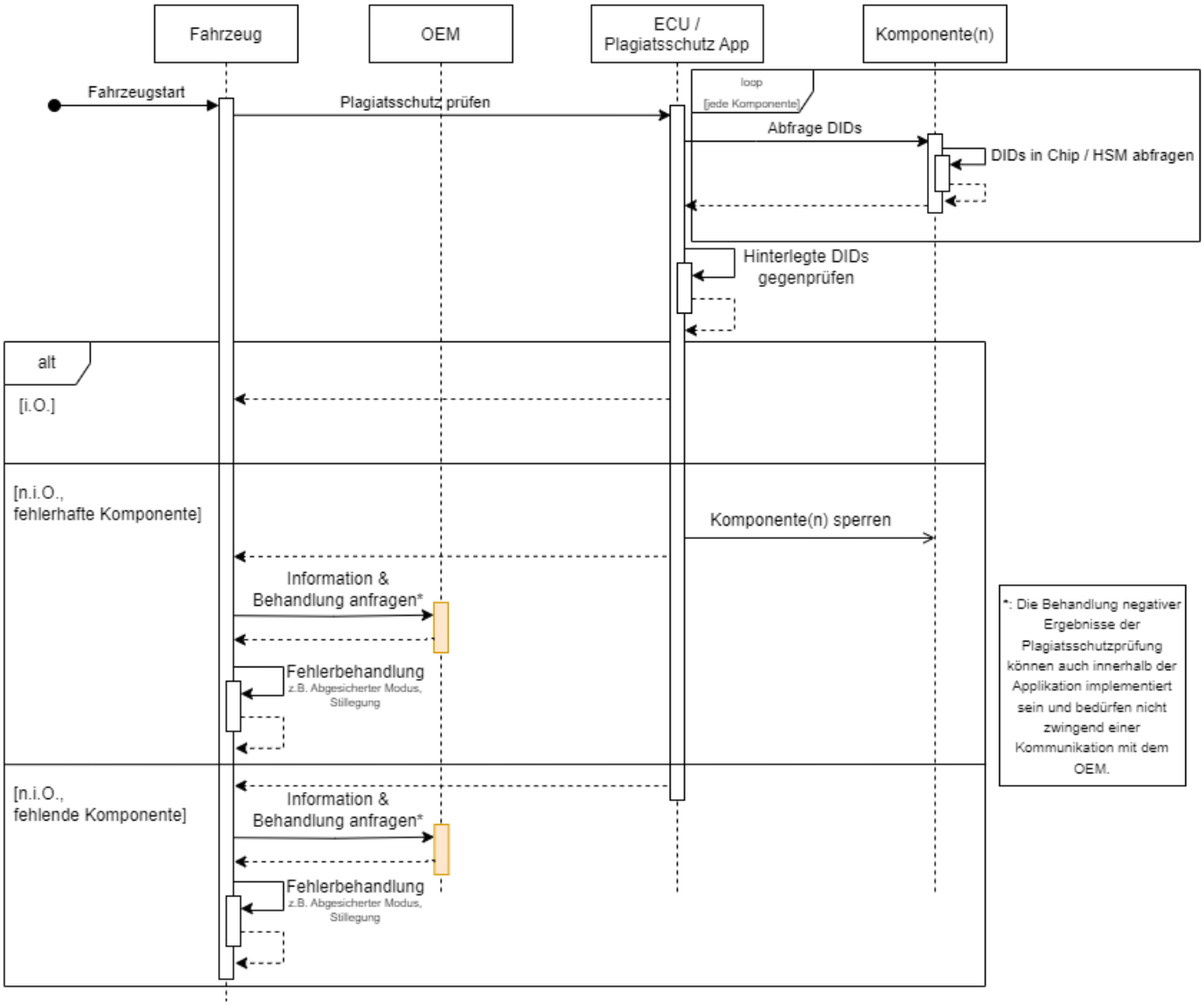


Abbildung 5 Validierungsprozess

Werkstattadapter

Im Grobkonzept ist ein Werkstattadapter vorgesehen, um die Kommunikation zwischen Fahrzeug (Plagiatsschutz-App) und der Werkstatt zu übernehmen und kryptographisch abzusichern. Der Werkstattprozess, welcher das Anlernen und Autorisieren neuer oder neu verbauter Teile in einem Fahrzeug ermöglicht, ist ein essentieller Teil des Konzepts zum Plagiatsschutz. Obwohl die Kommunikation für die Umsetzung des Prozesses notwendig ist, ist der Werkstattadapter selbst kein essentieller Bestandteil des Prozesses. Da in der Praxis die Werkstätten bereits über ein Diagnosesystem mit Zugang zum Fahrzeug verfügen, ist die Integration von auf Standards basierenden Authentifizierungsverfahren in ein Werkstattsystem ist jedoch mit Hilfe des jeweiligen OEM möglich und erscheint zudem realistischer, als alle Werkstätten des OEM mit neuer, zusätzlicher Hardware auszustatten. Die On Board Application wurde daher um Funktionen erweitert, die die kritischen Aktionen auslösen und eine entsprechende Autorisierung für diese Aktionen einfordern können.

2.1.1.1.4 Vertrauensmodell

Ein großer Teil der Arbeit fiel auf die Erstellung des grundlegenden Konzepts zum Berechtigungs- und Vertrauensmodell und des Konzepts zur Schlüsselverwaltung unter Berücksichtigung der Lebensphasen eines ACS.

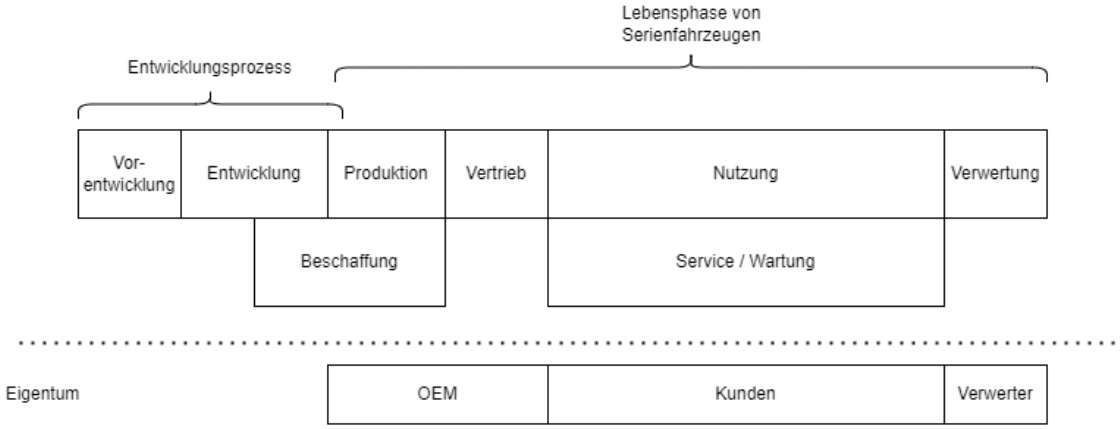


Abbildung 6 Lebensphasen eines ACS

Eine Übersicht über die elektronische Kommunikation zeigt die Komplexität des Systems, die im Vertrauensmodell berücksichtigt werden muss.

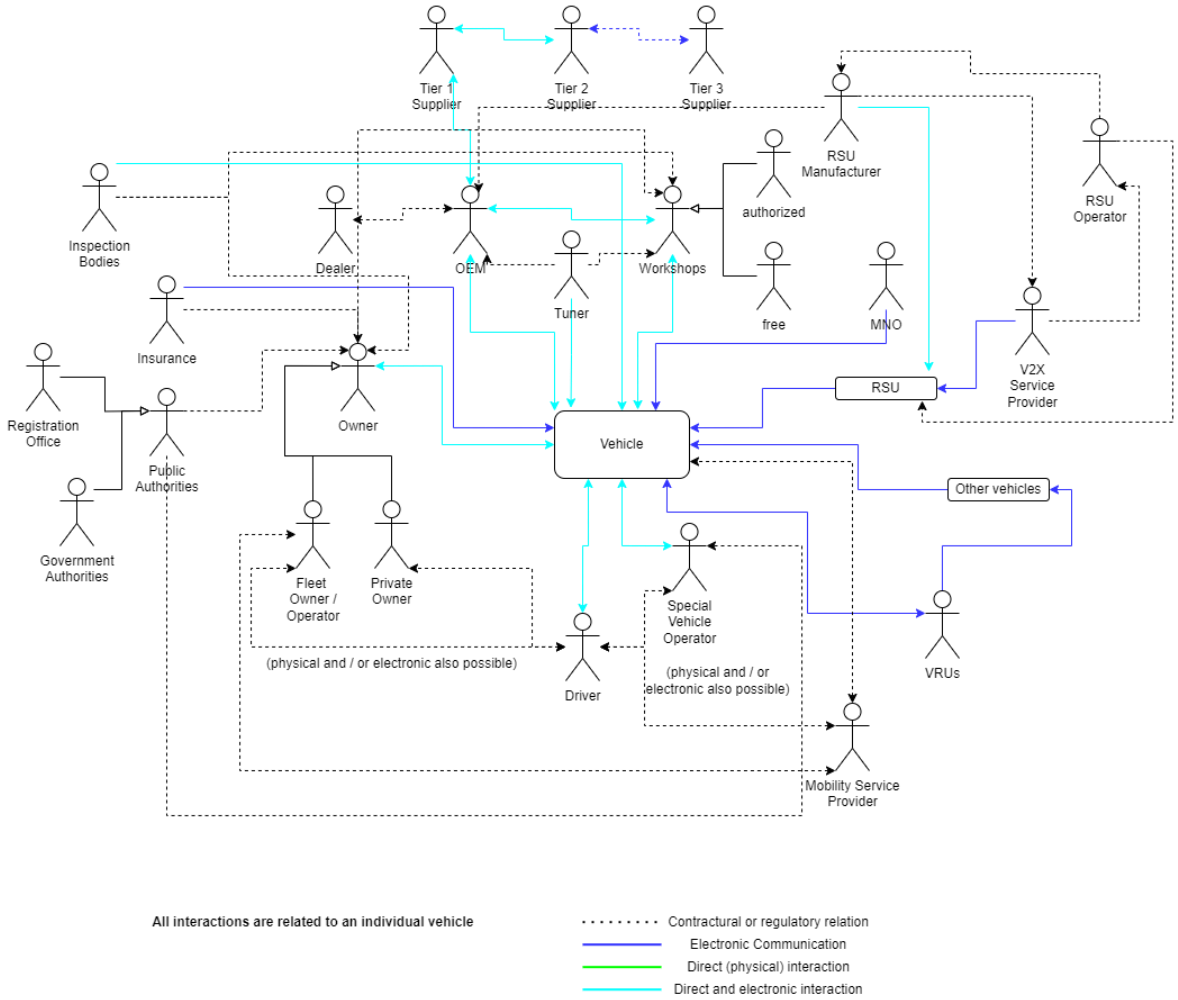


Abbildung 7 Übersicht elektronische Kommunikation im Gesamtsystem

Hierbei muss man formal unterscheiden zwischen zentral autorisierten Interaktionen, rein dezentral autorisierten Interaktionen und etwaigen hybriden Interaktionen. Das entsprechende Vertrauensmodell wurde hauptverantwortlich von der THI entwickelt und gemeinschaftlich in der TRADE Application unter Berücksichtigung der Anforderungen im Automotivebereich umgesetzt.

2.1.1.2 Schlüsselverwaltung

Für ein valides System ist eine sichere und vertrauliche Kommunikation fundamental. Hierzu werden in erster Linie – neben standardisierten kryptographischen Methoden - sichere und geheime Schlüssel benötigt. Gleichzeitig dienen Schlüssel als Vertrauensanker zur Erzeugung einer Vertrauenskette im System und sind essentieller Bestandteil von DIDs und DID Dokumenten.

In der TRADE-Anwendung fallen diese insbesondere in der ECU der On Board Applikation, an der ETO-Komponente bzw. der Kopierschutz Applikation, am Backend sowie am End-of-Line Server (in der Produktionsphase) an. Hierbei kann die Erzeugung geheimer und sicherer Schlüssel an der ECU, am EoL-Server sowie am Backend üblicherweise über ein HSM oder ein USB-HSM (etwa Nitro-Key) erzeugt werden. Kritischer ist die Erzeugung sicherer Schlüssel auf der einzelnen Komponente. Hierfür wird ein Atec-Microchip C608B oder ein automotive konformer Cryptochip sowie ein externer Microcontroller oder FPGA verwendet. Hierdurch kann allumfassend Sicherheitslevel 4 erreicht werden.

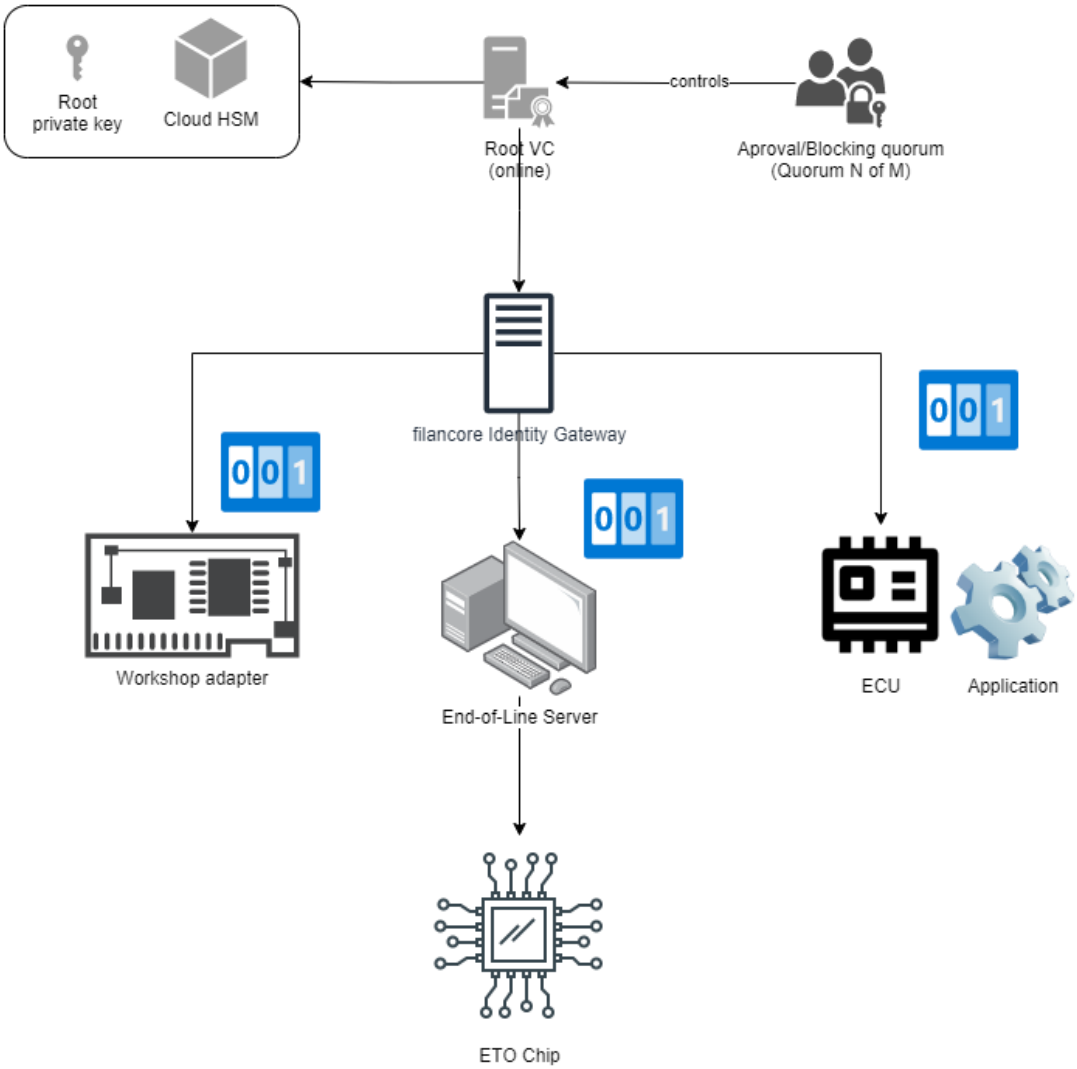


Abbildung 8 Konzept der Schlüsselratifizierung

Neben harter Speicherung auf sicheren Co-Prozessoren, welche gegen Auslesen und Sidechannel-Attacken gesichert sind, gibt es auch schwache Speicher, welche Schlüssel lediglich in Software speichern. Diese sind anfälliger für Manipulation von Zufallszahlgeneratoren. Die ETO-Komponente sowie die ECU kann üblicherweise mit einem harten Speicher versehen werden, wohingegen das Backend und der EoL-Server schwache Speicher vorweisen. Für die schwachen Speicherkomponenten wurde eine Lösung mit einem cloudbasierten HSM von securosys verwendet, welche eine starke Speicherung garantiert und von den schwachen Speicherkomponenten verwendet werden kann, um ihre in einer schwachen Umgebung erzeugten Schlüssel zu ratifizieren. Allerdings wird der Zugriff auf das securosys HSM nun zum schwächsten Glied und ersetzt den Angriffsvektor von der schwachen Speicher- zur schwachen Schnittstellensicherheit. Um die schwache Schnittstelle zu umgehen, wurde der folgende Mechanismus eines rollen- und zeitbasierten Zugriffs umgesetzt.

Außerdem wurde eine effiziente Schlüsselbereitstellung zum Aufbau sicherer Kommunikationskanäle mittels temporärer Schlüssel umgesetzt.

Der Prozess zur Erstellung eines DID Dokuments an einer Komponente sowie die gegenseitige Authentifizierung und Autorisierung basierend auf den vorliegenden Schlüsselpaaren wurde nach folgendem Schema konzipiert um umgesetzt.

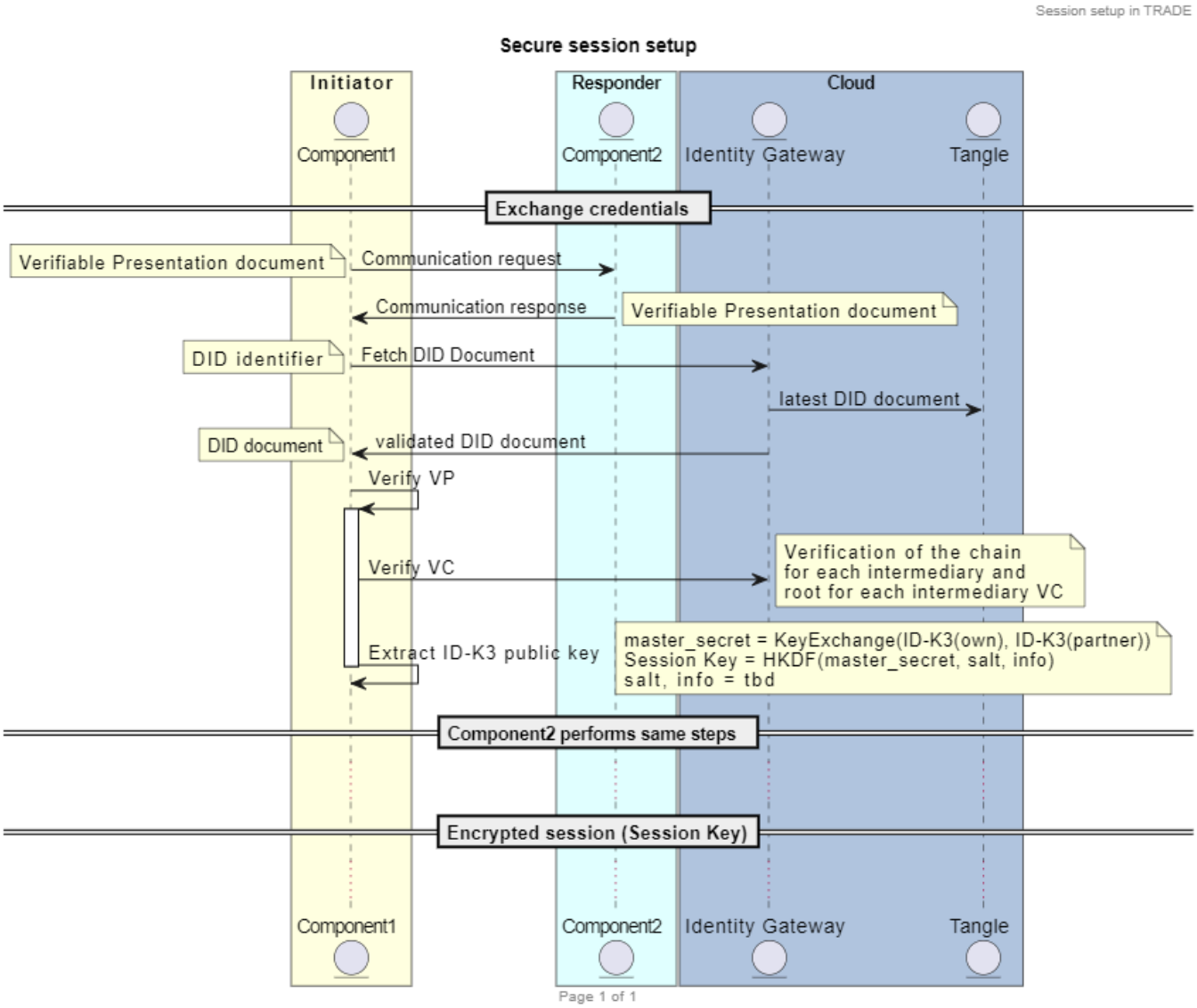


Abbildung 9 Prozess der Validierung eines DID

Für den Fall, dass eine Komponente keinen sicheren Kommunikationskanal zum Backend aufbauen kann, wurde ebenfalls ein geeignetes Konzept entwickelt und umgesetzt.

2.1.1.3 Demonstrator

Für den Demonstrator wurde eine Test PKI aufgebaut, um die generelle Schlüsselverwaltung zu testen. Insbesondere wurde Zufallszahlengenerator für das embedded System sowie der Command Handler zum Aufbau der nötigen Kommunikation im Rahmen der Challenge Response umgesetzt. Das Konzept der Schlüsselerzeugung und Provisionierung wurde auf einem Nucleo F446ZE erfolgreich demonstriert und das konzipierte Autorisierungs- und Authentifizierungsverfahren umgesetzt.

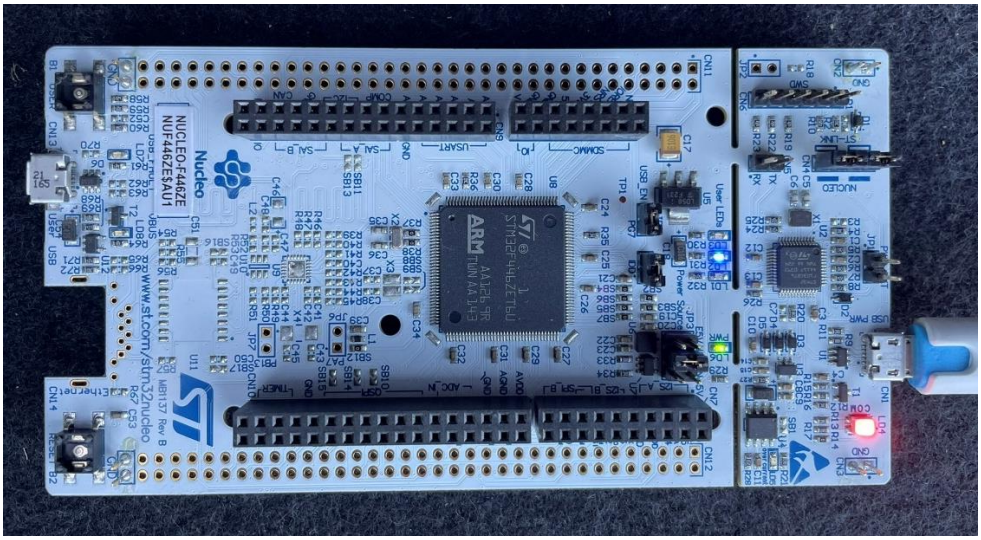


Abbildung 10 Nucleo F446ZE zur Demonstration

Außerdem konnte mit dem STM32 Nucleo WB15CC ein Funkdemonstrator basierend auf Bluetooth Low Energy (BLE) erstellt werden, um neben der Datenübermittlung per Kabel eine Alternative anbieten zu können. Hierdurch kann ein späterer Einbau in ein bestehendes Fahrzeug ermöglicht werden, welches die Chancen der Verwertbarkeit deutlich erhöht.

Abbildung 11 Testfahrzeug und Demonstratoren

Hiermit wurden zur Veranschaulichung zwei Demonstratoren – einmal als Original, einmal als Plagiat – erstellt. In einem angepassten Golf VIII wurde abschließend der Kopierschutzvorgang der Trade-Anwendung demonstriert und angezeigt.

Abbildung 12 Anzeige im Testfahrzeug bei Anschluss des Plagiats

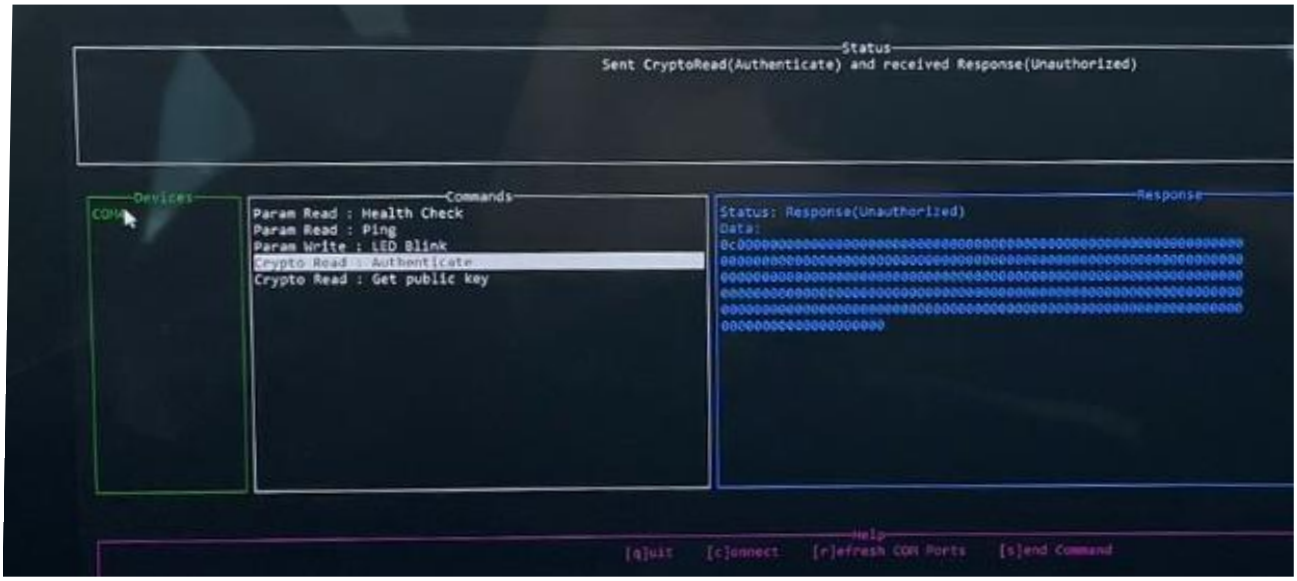


Abbildung 13 Anzeige im Display vergrößert

2.1.1.4 Sonstiges

Neben der Arbeit an der eigentlichen Kopierschutzlösung wurde eine rege Diskussion mit der IOTA-Foundation geführt, da die Identitäts-Library auf deren Seite noch angepasst werden muss. Dies dient dazu, dass diverse nötige Sicherheitsstandards erfüllt werden können und die Verwendung der Kryptographiemethoden agil bleiben, um auf etwaige unbekannte Angriffsvektoren, etwa durch Quantencomputer, auch in Zukunft reagieren zu können.

Die Entwicklung des Systems und der Prozesse wurde nach den Compliance-Regeln aus der Automotive-Industrie als TISAX®-zertifiziertes Unternehmen umgesetzt, beispielsweise wurden die Anforderungen gemäß ISO 26262 erfasst und berücksichtigt. Lediglich in der Tiefe der technischen Dokumentation wurden kleine Abstriche gemacht, etwa wurde die durch Tickets rückverfolgbare Softwareentwicklung nicht final noch einmal gesondert dokumentiert. Insbesondere wurde auch eine notwendige Sicherheits- und Risikoanalyse (nach HEAVENS) durchgeführt und die Parameter – speziell bei den kryptographischen Methoden – entsprechend angepasst. Insgesamt ist eine ASIL-Dokumentation vorbereitet und kann im Rahmen einer sensorspezifischen Produktanpassung kurzzeitig nachgezogen werden.

2.1.2 Gegenüberstellung mit den vorgegebenen Zielen

Die Ziele des Teilvorhabens In-Car-DLT-Lösung konnten grundsätzlich erreicht werden. Insbesondere die Konzeption und der Nachweis einer hinreichend performanten Umsetzung der Kopierschutzlösung unter Berücksichtigung von automotive-gerechten Randbedingungen konnte gezeigt werden. Die Umsetzung auf tatsächlich serienreifer Hardware wurde zurückgestellt und somit nicht vollumfänglich erbracht.

2.1.3 Abweichungen in der Arbeits-, Zeit- und Ausgabenplanung

Die Arbeiten verliefen grundsätzlich gemäß der in der Vorhabenbeschreibung gezeigten Arbeits- und Kostenplanung.

Die ursprüngliche Beschaffung zweier automotive-konformer Steuergeräte samt Originalsoftware eines OEM stellte sich als nicht zielführend heraus, da diese einen Eingriff von externer Seite offiziell nicht zulassen. Entgegen unserer Annahme kann auch keine zusätzliche Software, welche in das System selbst nicht eingreift, integriert werden. Daher wurde mit allen Projektpartner beschlossen, die Applikation auf einem nicht automotive-zertifizierten Hilfsrechner zu entwickeln. Trotz vielfältiger Versuche konnten keine der benötigten automotive-konformen Crypto-Chips beschafft werden. Diese wurden nach einer prognostizierten Lieferzeit von 9 Monaten vom Lieferanten storniert. Ein automotive-konformer Ersatz war innerhalb der Projektlaufzeit nicht erhältlich. Dementsprechend wird der In-Car Demonstrator mit einem handelsüblichen ATECC-Chip betrieben. Außerdem wurde die Anzahl der Demonstratoren deutlich reduziert, da die neuen Demonstratoren im Gegensatz zum ursprünglichen Konzept mehrfach verändert werden können.

Durch den Wegfall der Steuergeräte ist eine nachträgliche Anpassung der Leiterplatten auf die spezifischen Bedürfnisse der jeweiligen OEM-Steuergeräte in jedem Fall nötig. Hierbei ist noch einmal der gleiche hardwarespezifische Arbeitsaufwand wie ursprünglich vorgesehen notwendig. Daher wurde entschieden, diesen Arbeitsschritt, welcher durch die innerbetrieblichen Leistungen gefördert werden sollte, erst in der Industrialisierungsphase auf eigene Kosten an den spezifischen Kundenanforderungen adaptiert durchzuführen.

Ausgleichend hierzu wurde das System statt als OEM-spezifische Speziallösung als generalisiertes System aufgesetzt. Hierdurch kann zum einen in der Verwertungsphase eine schnellere Adaption an die OEM-spezifischen Bedürfnisse erreicht werden, welches die zusätzlichen Aufwände in der Hardwareanpassung in Teilen ausgleicht. Zum anderen kann das gesamte TRADE-System hierdurch leichter auf andere Anwendungsfälle übertragen werden, wodurch das eigentliche Projektziel in Teilen sogar übertroffen werden könnte. Aus ebendiesem Grund war eine moderate Erhöhung (von ca. 10%) der Personalmittel erforderlich, welche durch eine kostenneutrale Umwidmung erzielt wurde.

2.2 Wichtigste Positionen des zahlenmäßigen Nachweises

Die wichtigsten Positionen des zahlenmäßigen Nachweises sind in der nachfolgenden Tabelle 1 aufgeführt.

Tabelle 1: Gesamtfinanzierungsübersicht

Nr.	Position	Entstandene Kosten
0813	Material	2.272 EUR
0837	Personalkosten	488.146 EUR
0881	Gesamte Selbstkosten	559.426 EUR

Die Materialkosten ergeben sich durch die Beschaffung der Elektronikeinheiten und (nicht automotive-konformen) Crypto-Chips für die entwickelten Demonstratoren der In-Car-DLT-Lösung.

Die Personalkosten teilen sich auf die Entwicklung des Gesamtkonzepts, die Entwicklung der Software im Allgemeinen sowie im Speziellen auf den Demonstratoren, deren Herstellung, Integration und Test auf.

2.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Alle im Vorhaben „TRustworthy Autonmous Driving by DEzentralized Authentication and Authorization - TRADE, Teilvorhaben: In-Car-DLT-Lösung“ geleisteten Arbeiten waren zum Erreichen der Ziele des Vorhabens notwendig. Die durchgeführten Arbeiten stehen im Einklang mit den Zielen des Projekts und die Kosten im Verhältnis zum erwarteten Nutzen. Die durchgeführten Arbeiten haben einen klaren und direkten Beitrag zur Erreichung der Projektziele geleistet und waren angemessen. Während des Vorhabens wurde die Notwendigkeit und Angemessenheit der Arbeiten regelmäßig überprüft, um sicherzustellen, dass das Projekt weiterhin einen Mehrwert bietet und die staatlichen Mittel effizient genutzt werden.

2.4 Nutzen und Verwertbarkeit der Ergebnisse

2.4.1 Wirtschaftliche Verwertung

Das erworbene Wissen kann in die weiteren Arbeiten der ETO GRUPPE bei eigenständigen technologischen Programmen eingebracht werden. Es wurde weiteres Know-how bei ETO auf dem Gebiet der Entwicklung von komplexen, interagierenden Systemen (Embedded Systems), der Softwareentwicklung und Gewährleistung von Datensicherheit und Datenintegrität sowie Identitätsmanagement im automotive Kontext geschaffen.

Die Verwertung erfolgt im Anschluss an das Vorhaben in einem bereits geplanten Forschungsvorhaben durch Integration des Kopierschutzmoduls und der TRADE-Applikation in einer Weiterentwicklung des im Forschungsprojekt ALFRIED entwickelten intelligenten Leitpfostens als Konzept zur Datenintegrität bei der Bereitstellung von externen Sensordaten im autonomen Fahren.

2.4.2 Wissenschaftliche/technische Verwertung

Das Projekt trägt dazu bei, die deutschen Standorte der ETO GRUPPE zu stärken, so dass langfristig Arbeitsplätze erhalten und aufgebaut werden können. ETO kann sich durch ein ergänzendes Produktportfolio sowie eine softwaretechnische Verbesserung des bestehenden Portfolios in den globalen Märkten besser positionieren und wird sich weiterhin im Bereich Ausbildung und Weiterbildung engagieren können.

Dies trägt dazu bei, dass ETO sein Netzwerk zu Unternehmen, Universitäten und wissenschaftlichen Einrichtungen weiter ausbauen kann. In diesem Projekt wird keine klassischen Kunde-Lieferanten-Beziehung gepflegt, sondern partnerschaftliche Kooperationen mit den Projektpartnern für die Zukunft gebildet.

2.5 Erfolgte oder geplante Veröffentlichungen

Die Ergebnisse des Vorhabens wurden von ETO auf dem Messestand des Aachen Colloquiums sowie auf den firmeneigenen Tagen der offenen Tür vorgestellt. Darüber hinaus wird der entwickelte Code weitestgehend als Open Source der Allgemeinheit zur Verfügung gestellt. Durch die Verwertung in einem weiteren Forschungsprojekt wird die öffentliche Sichtbarkeit zudem erhöht. Eine öffentliche Veranstaltung zur Vorstellung der Ergebnisse des Vorhabens TRADE für Interessierte aus dem Automotive-Bereich ist für 2025 angedacht, zum jetzigen Zeitpunkt jedoch noch nicht finalisiert.

TRADE - Teilvorhaben: In-Car-DLT-Lösung **FKZ 16KIS1408**

Kurzbericht

Aufgabenstellung und technischer Stand, an den angeknüpft wurde

Das Forschungsvorhaben TRADE zielt auf die Entwicklung einer sicheren, skalierbaren Identitätsmanagement-lösung ab, die eine globale standardisierte Identitätsschicht für ein Automotive Cyber System ermöglicht. Der Fokus liegt auf einer dezentralen Lösung basierend auf IOTA Distributed-Ledger-Technologien (DLT), wodurch erstmalig eine übergeordnete Sicherheitsarchitektur ermöglicht wird, die im Kontext ACS bisher nicht umsetzbar war. Hierdurch erhalten wir Interoperabilität, Dezentralität, Transparenz, Sicherheit und Skalierbarkeit, um eine Vielzahl von Stakeholdern einbinden zu können, den Anforderungen von KMUs gerecht zu werden und die Anbindung bestehender, herstellerspezifischer Lösungen zu ermöglichen. Das Ziel dieses Teilvorhabens ist eine Lösung zu entwickeln, welche die Zugriffsrechte auf ACS bzw. auf dessen Teilsysteme zulässt. Dazu sollen mittels zu entwickelnden Plagiatsschutzkomponenten die Handlungen „Authentifizierung“ und „Autorisierung“ am Beispiel des Anwendungsfalls „Plagiatsschutz“ nachgewiesen werden.

Wesentliche Kernfunktionen von TRADE unterstützen die Vertrauensbildung in ACS und umfassen unter anderem:

- Etablierung eines offenen, kontrollierten Identitäts-Ecosystems für sichere Identitäten auf Basis von DLT
- Instanz zur Prüfung und Vergabe von verifizierbaren Berechtigungsnachweisen für Identitäten, bei dem nur die zugeordneten Stakeholder Rechte und Zugriffe für ihre Teile des ACS vergeben können
- Sichere Verwahrung der Berechtigungsnachweise zur nachvollziehbaren Authentifizierung und Autorisierung an jeder Komponente bzw. jedem Fahrzeug-Teilsystem oder Person

Die Verwertung der Projektergebnisse zielt auf die softwaretechnische Ausstattung serientauglicher Produkte mit einer Kopierschutzlösung ab, die flächendeckend auf Basis der zu erarbeitenden Einsatzempfehlung zum sicheren und effizienten ACS-Betrieb eingesetzt werden können.

Die reine Anpassung von PKI-basierten Mechanismen zur Authentifizierung an die Anforderungen der Automobilindustrie sind nicht ausreichend, da die Abhängigkeit, Skalierbarkeit, der Lebenszyklus der Schlüssel, das Schlüsselmanagement und Widerrufung der zugrundeliegenden Zertifikate nicht mit den langen Laufzeiten der Maschinen und ACS in Einklang gebracht werden können. Zudem weisen gerade ACS-Komponenten derzeit noch unüberwindbare Limitierungen hinsichtlich Rechenleistung und Geschwindigkeit bei Verwendung von kryptografischen Mechanismen auf, um eine kryptographisch abgebildete Maschinenidentität umfangreich implementieren und nutzen zu können. Eine potenzielle Lösung weisen Distributed Ledger-Technologien auf, wenngleich die wissenschaftliche Basis für entsprechende Ansätze in der Breite für die Identifikation und den operativen Betrieb ökonomisch autonomer und vernetzter Systeme gering ist. Die DLT hat innerhalb der letzten Jahre enorme Aufmerksamkeit durch Forschung, Industrie und Medien erfahren. Der IOTA DLT operiert, im Gegensatz zu anderen DLT, wie ein Kommunikationsprotokoll und kann mit dem W3C Entwurf „Decentralized Identifiers (DIDs) v1.0“ (W3C, 2020) kombiniert werden, um obiges Problem zu lösen.

Ablauf des Vorhabens

Der Durchführungszeitraum des Vorhabens war der 01.07.2023 bis 30.06.2024. Das Projekt wurde in 8 Arbeitspakete unterteilt, AP 1: Projektmanagement, AP 2: Anforderungen basierend auf Stakeholder, Lebenszyklus und Anwendungsszenarien, AP 3: Systemspezifikation, AP 4: Integration „Registrierung-Verifizierungs-Verfahren, AP 5: Entwurf In-Car-DLT-Lösung, AP 6: Entwurf Identitätsmanagementlösung,

AP 7: Rapid Prototyping, AP 8: Evaluierung. Die Hauptaspekte des Teilvorhabens In-Car-DLT-Lösung lagen auf AP 5 und 7, eine Zusammenarbeit in den anderen Arbeitspaketen war für die Erstellung des Gesamtsystems jedoch unabdingbar. Die Arbeitspakete wurden in drei Phasen – 1. Erstellung der Systemanforderung und Konzepterstellung und Systemspezifikation des Gesamtsystems, 2. Entwurf und Implementierung der Use Cases, 3. Evaluation – in agiler Verfahrensweise abgearbeitet.

Wesentliche Ergebnisse

Es wurde sich grundlegend auf ein System mit DID (dezentrale Identität) und VC (verifiable credential) festgelegt, welche dezentral an ein IOTA Tangle geknüpft sind. Für die Funktionsfähigkeit ist ein geeignetes Vertrauensmodell unabdingbar, welches im Rahmen des Projektes zusammen mit entsprechenden Policies, einem an den automotive Lebenszyklus angepasstes Rollenmodell sowie einer dementsprechenden Schlüsselverwaltung entwickelt und für drei Use Cases – VANETs, SOTA und Kopierschutz - exemplarisch implementiert wurde. Die Kernfunktionen laufen dabei über eine zentrale On Board Applikation im Fahrzeug, welche mit dem Backend als Identity Gateway kommunizierten kann. Hierbei wurden die Anforderungen aus der Automotive-Industrie und die damit einhergehenden sicherheitsrelevanten Anforderungen an Kryptographie sowie Datenautorität und Datenintegrität eingepflegt. Um abhängig vom geforderten Sicherheitslevel die Anforderung eines dedizierten Sicherheitsmoduls auch anpassbar zu machen, wurde für das Konzept eine generische Schnittstelle modelliert. Der Zugriff auf die Applikation von Seiten der OEMs wird ebenfalls über eine generische Schnittstelle gewährleistet. Diese ist bewusst unabhängig von der konkreten Umgebung gewählt, um diese beispielsweise für AUTOSAR Adaptive zugänglich zu machen.

Im Kopierschutz-Szenario geht es darum, die Echtheit von (Ersatz-)Teilen in einem Fahrzeug sowie deren fachgerechten Einbau überprüfen zu können. Die fachgerechte Implementierung eines Autorisierungs- und Verifizierungsverfahrens unter den eingeschränkten Möglichkeiten von automotive-konformen Sensoren wurde erarbeitet und umgesetzt. Ein wesentlicher Aspekt fiel auf die sichere Schlüsselerzeugung, welche an der ECU und am Backend üblicherweise über ein HSM erzeugt werden können, an einzelnen Komponenten jedoch einer anderen Lösung bedürfen. Hierfür wird ein Atec-Microchip sowie ein externer Microcontroller oder FPGA verwendet, um allumfassend Sicherheitslevel 4 zu erreichen. Für die sichere Schlüsselverwahrung wurde die ETO-Komponente sowie die ECU mit einem harten Speicher versehen und für das Backend eine Lösung mit einem cloudbasierten HSM von securosys erarbeitet.

Für den Demonstrator der Kopierschutzanwendung wurde eine Test PKI aufgebaut, um die generelle Schlüsselverwaltung zu testen. Insbesondere wurde Zufallszahlengenerator für das embedded System sowie der Command Handler zum Aufbau der nötigen Kommunikation im Rahmen der Challenge Response umgesetzt. Das Konzept der Schlüsselerzeugung und Provisionierung wurde auf einem Nucleo F446ZE erfolgreich demonstriert und das konzipierte Autorisierungs- und Authentifizierungsverfahren im Zusammenspiel mit der prototypisch umgesetzten On Board Applikation umgesetzt. Nach der Identifizierung eines Originalteils oder Plagiats werden Information an die Steuerung übermittelt, die die Entscheidung über die weiteren Schritte übernimmt. Dieser Demonstrator wurde in einem angepassten Golf VIII vorgeführt.

Außerdem wurde ein Funkdemonstrator basierend auf Bluetooth Low Energy (BLE) erstellt werden, um neben der Datenübermittlung per Kabel eine Alternative anbieten zu können. Hierdurch kann ein späterer Einbau in ein bestehendes Fahrzeug ermöglicht werden, welches die Chancen der Verwertbarkeit deutlich erhöht.