

Sachbericht zum Verwendungsnachweis

Teil II

2025

Verbundvorhaben

SILKOSTU

Sicherheit in der intelligenten Kommunikation zwischen Verkehrsteilnehmern und städtischer Infrastruktur

Gefördert durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Konsortialführung: consider it GmbH Wilma-Witte-Stieg 1 22097 Hamburg	Förderkennzeichen: 01MO23004A
Laufzeit des Vorhabens: von: 31.12.2022 bis: 31.03.2025	
Berichtszeitraum: von: 31.12.2022 bis: 31.03.2025	Datum: 28.06.2025

Projektpartner:

1. Behörde für Verkehr und Mobilitätswende (BVM) der Freien und Hansestadt Hamburg (FHH)
2. Giesecke+Devrient Mobile Security GmbH (GD)
3. Universität zu Lübeck (UzL)
4. consider it GmbH (CIT)

Teil II:

1. Aufgabenstellung

(ausführliche Darstellung der durchgeführten Arbeiten, insbesondere im Vergleich zu ursprünglichen Vorhabensbeschreibung. Bei Einzelvorhaben soll möglichst ein Umfang von 20 Seiten nicht überschritten werden. Die Verwendung der Zuwendung sowie die erzielten Ergebnisse im Einzelnen müssen nachvollziehbar sein.)

CIT

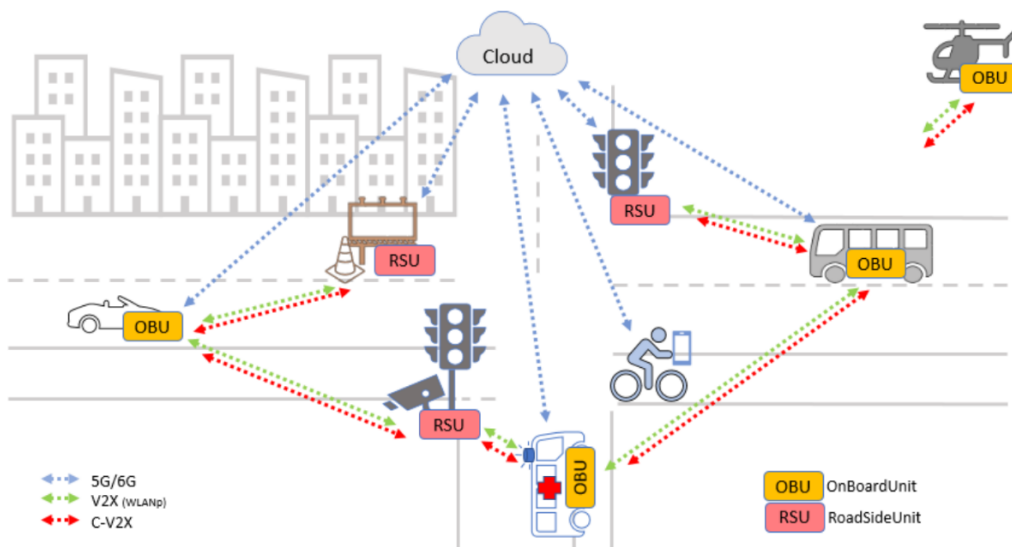
AP 1: Anforderungsanalyse

Zu den Aufgaben der CIT gehörte das Forschen und Recherchieren an einer sicheren und effizienten Hardware, die eine abgesicherte V2X-Kommunikation zwischen Verkehrsteilnehmern untereinander und Verkehrsinfrastruktur ermöglicht. V2X, kurz für "Vehicle to Everything", ist ein Kommunikationssystem, das es Fahrzeugen und der Infrastruktur ermöglicht, mit ihrer Umgebung in Echtzeit zu interagieren. Ziel war es, eine möglichst hohe Resilienz gegen Störungen in der Netzwerkstruktur und Netzsicherheit zu bekommen. Die Kommunikation sollte in Echtzeit (Reaktionszeiten < 50ms) erfolgen. Aus diesen Vorgaben wurde eine Plattform entwickelt, die den technologisch aktuellen Stand um diese auf verschiedenen Ebenen abgesicherte Multi-Kommunikation erweitert und diese Anforderungen umsetzte.

Ziel war, die Technologie im Bereich 5G/6G zu nutzen, um die Souveränität Deutschlands zu fördern. Die Untersuchung der Möglichkeiten, wie eine gleichzeitige Absicherung der Kommunikation und erhöhte Resilienz umgesetzt werden kann, war Teil umfangreicher Recherchen. Die Hardware war für diese Umsetzung so auszuliegen, dass trotz verbesserter Resilienz weiterhin eine Echtzeitkommunikation ohne Verzögerung möglich ist; ebenso der parallele Betrieb der Kommunikation.

Für die Absicherung wurde sowohl die prozessorinterne Kommunikation abgesichert als auch die Kommunikation mit weiteren Teilnehmern. Die Angriffsfläche für Cyberangriffe war zu minimieren, um eine Resilienz gegen bekannte und neue unbekannte Angriffe vorzusehen.

Es wurde eine Recherche durchgeführt, welche Kommunikationseinheiten (5G/6G, C-V2X (Cellular), V2X-dsrc, (Dedicated Short Range Communication), WLAN, LAN) wie zusammenarbeiten und mit welchen Schnittstellen diese angebunden werden müssen. Die Untersuchung der Schnittstellen diente zur flexiblen, zukunftsorientierten Auslegung des Systems. Bauteile und Baugruppen sollten mit minimalem Aufwand getauscht werden können; angestrebt und umgesetzt wurde ein einfaches Plug&Play. Falls erforderlich sollten benötigte Softwareanpassungen per Update verteilt werden können.



SILKOSTU – Sicherheit in der intelligenten Kommunikation zwischen Verkehrsteilnehmenden und städtischer Infrastruktur

Abbildung 1 Kommunikation zwischen Teilnehmern

AP 2: Hardwareentwurf

Bei Systemen ist die Stromaufnahme, bedingt durch die gleichzeitige Benutzung verschiedener Sende- und Empfangskomponenten, von wesentlicher Bedeutung. Die Kommunikationseinheiten benötigen im Sendebetrieb, abhängig von der Verbindungsqualität, unterschiedlichen Stromaufnahmen. Spannungseinbrüche an einzelnen Komponenten, hervorgerufen durch Strom-Burst beim Senden, können das gesamte System instabil werden lassen. Das Optimum aus Stromaufnahme, Wirkungsgrad und Ressourcen-Verbrauch zu ermitteln, ist ein aufwändiger Prozess. In diesem Zusammenhang wurde auch eine Untersuchung des Temperaturverhaltens durchgeführt. Durch die Sendeleistung entsteht in den Kommunikationseinheiten Wärme, die im Dauerbetrieb zielgerichtet abgeführt werden musste.

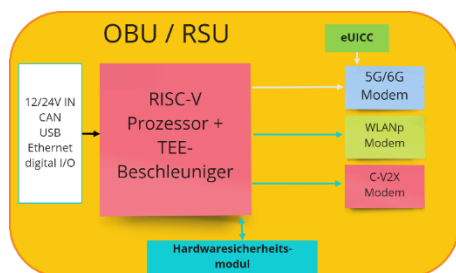


Abbildung 2 Systemübersicht

Die resultierenden Ergebnisse sind in Berechnungen, Schaltpläne und Layouts eingeflossen. Die daraus entstandenen Messaufbauten und Messergebnissen wurden mit den berechneten Ergebnissen verglichen. Dadurch ergab sich die Erweiterung der Basisarchitektur.

Zu den weiteren Recherchen zählte die Ermittlung der gesetzlichen Anforderungen an Produkte. Im KFZ sind internationale Regelungen vorhanden. Hier ist unter anderem die ECE-R10 (Economic Commission for Europe - Regulation 10) zu nennen. Diese regelt das EMV-Verhalten (Elektromagnetische Verträglichkeit) im KFZ, um die Betriebssicherheit zu gewährleisten. Für den Einsatz in Bussen sind weitere gesetzliche Vorgaben einzuhalten, z.B. eine Brandprüfung (ECE-R118).

Für stationäre Geräte wurden Umweltaforderungen, wie z.B. Bewitterung und UV-Belastung, berücksichtigt. Die gültigen EU-Regulativen, wie CE (Conformité Européenne) und die Funkrichtlinie RED (Radio Equipment Directive), mussten erfüllt werden.

Da jeweils mehrere gültige Vorschriften auf die Anwendung zutreffen, wurden unterschiedliche Anforderungen betrachtet. Jede Vorschrift bzw. Norm erfüllt einen spezifischen Teil, wie z.B. bei EMV (CE und ECE-R10), Sicherheit oder Umweltbedingungen. Die Unterschiede in den Regularien sind u.a. bei Messaufbauten für Prüfungen und Grenzwerte eingeflossen.

AP 3: Softwarearchitektur

Zur Implementierung wurden die benötigten Schnittstellen zwischen Hardware und Software untersucht. Die Ergebnisse wurden beim Hardwareentwurf eingearbeitet. Eine Feinabstimmung erfolgte bei der Implementierung und Integration zwischen Software und Hardware. Eine Abschätzung des Datenaufkommens zur Auslegung des Systems wurde durchgeführt.

AP 4: Implementierung und Integration

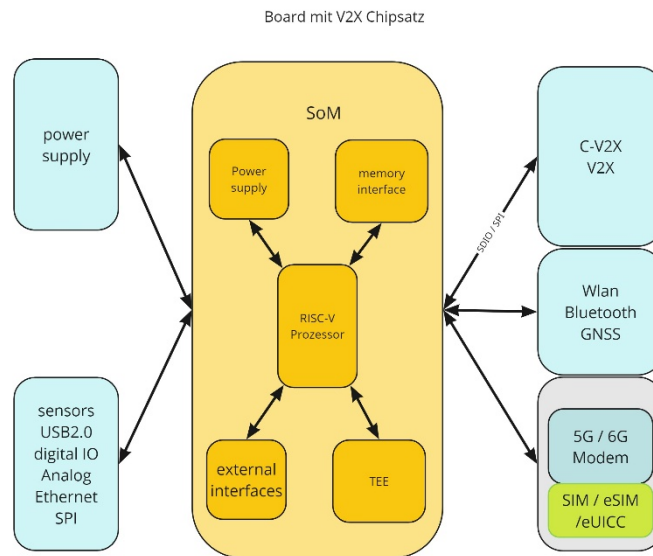


Abbildung 3 Implementierung

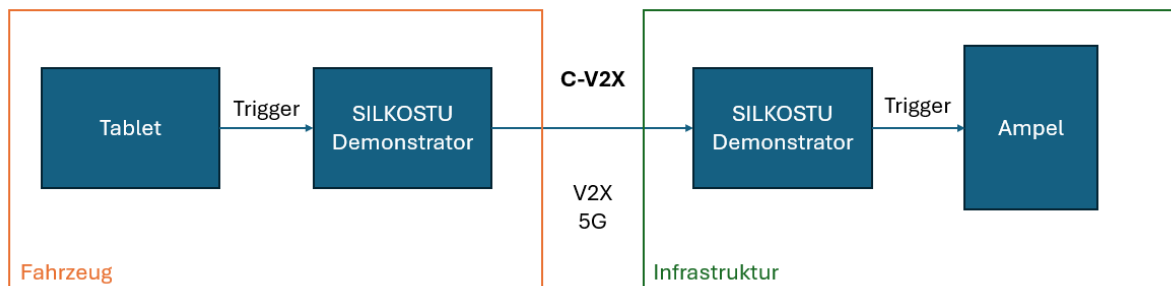
Nachdem in der EU bis heute nicht geklärt ist, welcher Standard bei der Kommunikation sich durchsetzt (5G/6G, C-V2X, V2X-dsrc), wurde dies in der Implementierung berücksichtigt. Weiterhin ist der C-V2X-Standard in 2 Versionen verfügbar, basierend auf C-V2X-LTE oder C-V2X-5G. C-V2X-5G ist zu C-V2X-LTE abwärtskompatibel, jedoch noch nicht weit verbreitet. Daraus resultiert eine notwendige Flexibilität bei der Komponenten-Auswahl. Es wurde ein modularer Aufbau angestrebt. Dieser bedingte wiederum einen endsprechenden Schnittstellenabgleich. Je nach eingesetzter Komponente unterscheidet sich die elektrische Schnittstelle, auch wenn die Stecker mechanisch kompatibel sind. Die Belegung unterscheidet sich komponentenspezifisch. Eine mögliche Softwareanbindung wurde bei der Auswahl zusätzlich betrachtet, um keine aufwändigen Anpassungen beim Komponenten-Tausch zu erzeugen. Dies schränkte die Auswahl der zu verwendeten Komponenten ein, worunter wiederum die Flexibilität litt. Alternativ waren Standard-Schnittstellen, z.B. USB2.0, USB3.0, SPI (Serial Protocol Interface) UART (Universal Asynchronous Receiver Transmitter) zu verwenden, um die eingeschränkte Flexibilität zu erweitern. Die Möglichkeit, über Zwischenadapter eine verbesserte Flexibilität zu erlangen, erhöhte den Hardware-Aufwand und die Wahrscheinlichkeit eines teilweisen Systemausfalls. Trotz dieser Widrigkeiten sind Komponenten im Demonstrator zum Einsatz gekommen, die diese Anforderungen erfüllten.

AP 5: Test und Demonstrator

Der Aufbau mehrerer Demonstratoren, bis hin zum abschließenden Demonstrator, wurde in einem iterativen Prozess realisiert. Es wurden mehrere finale Demonstratoren entwickelt, um die Funktion zwischen verschiedenen Kommunikationseinheiten zeigen zu können. Es wurden zusätzliche Aufbauten erstellt, um in einem iterativen Prozess, begleitet von Messungen, die optimalen Parameter zu eruieren. Die Betrachtungen zur Wärmeentwicklung wurden in den Demonstratoren effektiv umgesetzt.

Im Demonstrator wurden alle Kommunikationsschnittstellen umgesetzt (C-V2X, V2X-dsrc und 5G/6G, zusätzlich GNSS). Diese mussten teilweise mehrfach verbaut werden. Zukünftige Entwicklungen sollen dies optimieren, um den notwendigen Hardwareeinsatz zu reduzieren. Gemäß den durchgeführten Recherchen sind Entwicklungen bei Herstellern in der Entstehung, die diese Nachteile kompensieren können.

Die Kooperation mit potenziellen Kunden und das daraus resultierende Feedback hatte einen positiven Impact auf das Projekt. Der Use-Case konnte detailliert definiert und die Anbindung an eine Lichtsignal-Anlage (LSA) zur Bus-Priorisierung realisiert werden. Eine anstehende Änderung in der Infrastruktur, hervorgerufen durch den beschlossenen Wegfall der analogen Frequenzen (2028) bei der Bus-Priorisierung, konnte im praktischen Einsatz gezeigt werden.



G&D

AP 1: ANFORDERUNGSANALYSE

In enger Zusammenarbeit mit den Projektpartnern wurden die funktionalen und sicherheitsrelevanten Anforderungen an eSIM-basierte Lösungen für den V2X-Bereich ermittelt. G&D führte dazu eine Analyse der angedachten Szenarien (z.B. Fahrzeug-zu-Infrastruktur, Fernwartung von Netzwerkprofilen) durch, wobei Anforderungen an Hardware und Software präzisiert wurden. Aus den Ergebnissen entstand ein Kriterienkatalog, der Sicherheit und Updatefähigkeit der eSIM in den Vordergrund rückt. Hierzu zählen insbesondere Vorgaben für den späteren Profiltausch sowie das Remote-Management über das Hintergrundsystem.

AP 2: HARDWAREENTWURF

Zwar lag der Hauptfokus auf Softwareaspekten; G&D wirkte jedoch bei Fragen zum Hardware/Software-Co-Design unterstützend mit. So wurden Schnittstellenanforderungen für das 5G/6G-Modem und die benötigten Ressourcen (z.B. Energiebedarf, Prozessorleistung) an die Hardwarepartner kommuniziert, um die korrekte Einbindung der eSIM-Komponenten sicherzustellen. Ziel war eine Kompatibilität mit der von CIT und anderen Konsortialpartnern verwendeten Hardware, insbesondere um gemeinsame Demonstratoren aufbauen zu können.

AP 3: SOFTWAREARCHITEKTUR UND -ENTWICKLUNG

AP 3.1: Initialer Architekturentwurf

Aufbauend auf den in AP 1 definierten Anforderungen entwarf G&D eine eUICC-Architektur, die zentrale Verwaltungs- und Updatefunktionen ermöglicht. Dabei stand die sichere, orthogonale Trennung von Netzwerkprotokollen, Applikationen und Kryptofunktionen im Vordergrund.

AP 3.2: Entwicklung sicherer Kommunikationsprotokolle

G&D entwickelte ein Protokoll auf Basis von SGP.32, um das Sicherheitsbetriebssystem der eSIM über ein Hintergrundsystem partiell steuern und aktualisieren zu können.

Dabei wurden verschlüsselte Kommunikationspfade und robuste Sitzungsmechanismen realisiert, um etwaige Angriffe auf Profile oder Authentisierungsdaten abzuwehren.

Durch gezieltes Zusammenspiel mit dem 5G/6G-Modem konnten Profil- und Session-Handovers (z.B. bei Netzwechsel oder schlechter Funkverbindung) zuverlässig gehandhabt werden.

AP 3.3: Sichere Netzwerkprofilverwaltung

Die Projektarbeiten umfassten die Implementierung einer Fernverwaltung von eSIM-Profilen. Hierdurch kann ein kompromittiertes Profil zentral erkannt und ersetzt werden, ohne dass Eingriffe am Endgerät erforderlich sind.

Eine wichtige Neuerung war die Updatefähigkeit des Authentisierungsmechanismus: so kann das Herzstück der eSIM-Sicherheit im laufenden Betrieb modifiziert werden, um bei Angriffen rasch zu reagieren.

Alle Kernfunktionen wurden anhand von Modultests und ersten Integrationsszenarien gegen ein G&D-internes Backend und das CIT-System geprüft.

AP 3.4: Sichere Ausführung von Applikationen

G&D nahm Anpassungen innerhalb des Sicherheitsbetriebssystems vor, um Applikationen (z.B. Java Card Applets) in separierten Bereichen sicher abzuwickeln.

Dafür wurden bestehende Virtual-Machine-Komponenten erweitert, sodass kritische Anwendungen getrennt vom Netzwerkprofilmanagement lauffähig sind.

Diese Maßnahmen stellen sicher, dass Angriffe auf Applikationen die Mobilfunkzugänge (insbesondere die Authentisierung) nicht beeinträchtigen.

AP 3.5: Aktualisierung des Architekturentwurfs

Während der Implementierung erfolgten sukzessive Verfeinerungen des ursprünglichen Ansatzes (AP 3.1). Dazu zählten Verbesserungen bei den Sicherheits-Routinen (z.B. für den Profiltausch) und der Updatefähigkeit von SGP.32.

Das finale Architekturkonzept bildet die Grundlage für den späteren Produkthochlauf und die Übernahme in standardisierte eSIM-Lösungen für den V2X- und IoT-Bereich.

AP 4:

G&D war am AP 4 nicht beteiligt

AP 5: TEST UND DEMONSTRATION

G&D validierte den Gesamtdurchstich zwischen eSIM, 5G/6G-Modem und Hintergrundsystem auf einer Raspberry Pi-basierten Linux-Plattform.

Ein wesentlicher Demonstrationsteil war die erfolgreiche Fernverwaltung der eSIM (Profiltausch, Update des Authentisierungsalgorithmus) in einer realitätsnahen Testumgebung.

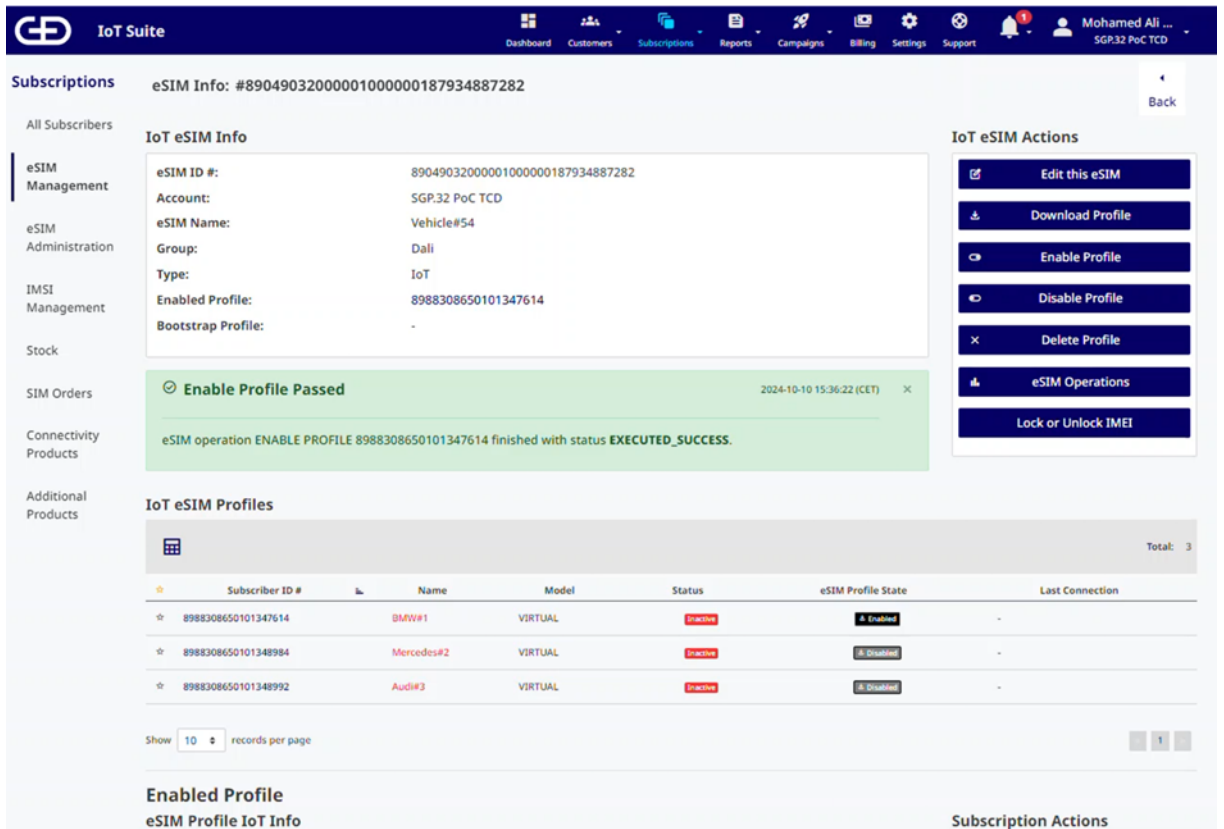


Abbildung 1: Hintergrundsystem zum Verwalten der Profile

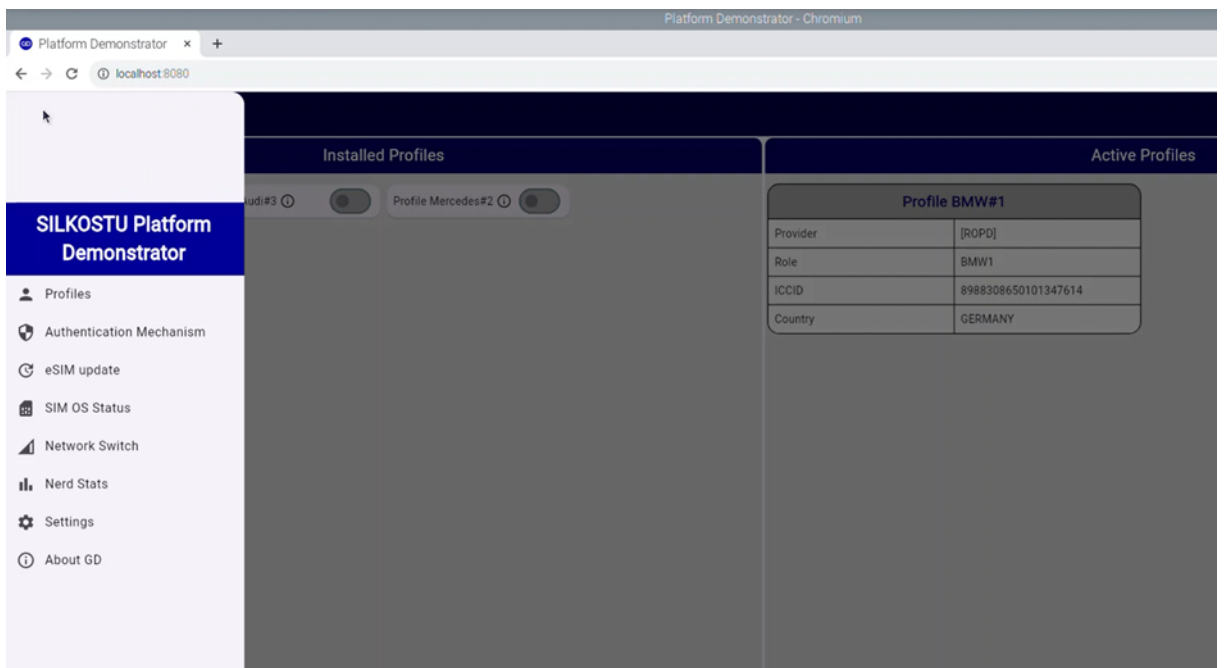


Abbildung 2: eSIM welche durch das Hintergrundsystem gesteuert wird
 - Das Sicherheitsbetriebssystem einer eSIM wurde erweitert um die Updatefähigkeit eines Authentisierungsschemata:

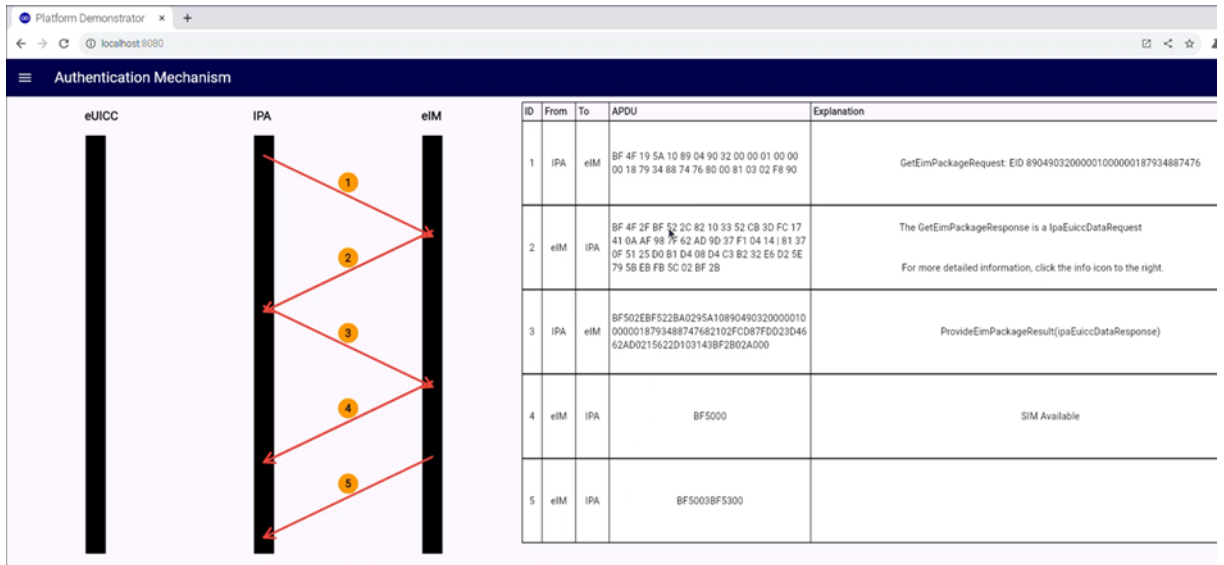


Abbildung 3: Update des Authentisierungsmechanismus

Die finale Vorführung fand u.a. im Zuge des Konsortial- bzw. Abschlusstreffens statt, wo die Funktionalitäten gegenüber den Partnern, inkl. CIT-System, demonstriert wurden. Hier zeigte sich, dass viele sicherheitskritische Abläufe "unsichtbar" im Hintergrund ablaufen und sich für die reine Präsentation spezielle Visualisierungen eignen mussten.

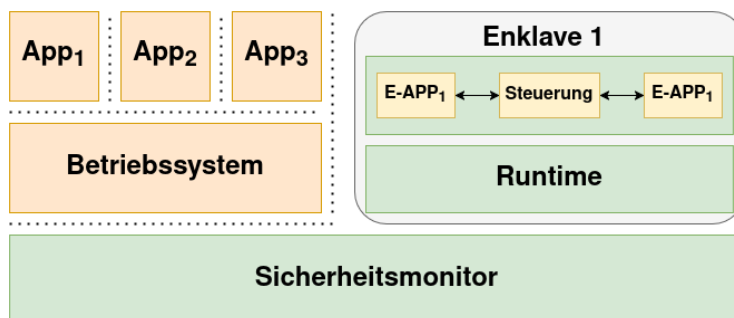
UzL-ITI & UzL-ITS

AP 1:

Der Fokus der Aufgabe von UzL-ITS lag auf den Anforderungen an die Sicherheit, Performanz und Zuverlässigkeit der Softwarekomponenten. Dazu gehört auch die Definition einer Trusted Computing Base und minimaler Schnittstellen zum Betriebssystem.

Im Hinblick auf die Performance wurden verschiedene Optionen für die vertrauenswürdige Ausführung evaluiert. Aufgrund der Performanzanforderungen besteht der Bedarf an leistungstärkeren Prozessoren, die auch Out-of-Order-Ausführung unterstützen. Diese sind jedoch anfälliger für Mikroarchitekturangriffe, was entsprechende Anforderungen an die Sicherheit mit sich bringt. Während eine herkömmliche Trusted Execution Environment (TEE) generell teurer als eine In-Prozessisolierung ist, bietet eine TEE eine höhere Sicherheit.

Aufgrund der Unterschiede zwischen einem einzelnen Prozess und modernen Enklaven ergeben sich entsprechend hohe Anforderungen an eine In-Prozessisolierung. So ist der Speicherschutz bei herkömmlichen Enklaven einerseits generell durch die Hardware gewährleistet und andererseits besteht eine geringere Anfälligkeit für Mikroarchitekturangriffe



Für die In-Prozessisolation bieten sich verschiedene Möglichkeiten als Vertrauensanker an. Generell ist das Betriebssystem als vertrauenswürdige Instanz wichtig, um die Grundfunktionalitäten der auf Benutzerebene ausgeführten In-Prozessisolation zu gewährleisten. Diese lässt sich auch in eine TEE auslagern, wodurch sich jedoch unter Umständen die Funktionalität einschränkt. Für Anwendungen im Kontext von Silkostu ergibt sich eine erhöhte Abhängigkeit von Kommunikationsdiensten wie z. B. Netzwerktreibern.

UzL-ITI war verantwortlich für die Definition der technischen Anforderungen an ein sicheres, offenes Hardware-Grundsystem zur Ausführung eines Trusted Execution Environments (TEE). Dabei wurden insbesondere die Schnittstellenanforderungen zur Einbindung unterschiedlicher Kommunikationsmodule wie 5G/6G, C-V2X und WLANp spezifiziert. Ziel war es, durch die Nutzung quelloffener RISC-V-Technologie ein modulares, austauschbares SoC-System mit klarer Fokussierung auf digitale Souveränität zu entwerfen. Die Anforderungsanalyse erfolgte in enger Abstimmung mit CIT, um die Systemkompatibilität mit den Kommunikationsmodulen zu gewährleisten.

AP 2:

Auf Basis der Anforderungen wurde ein RISC-V-SoC mit BOOM-Core unter Verwendung von Chipyard entwickelt. Dabei wurde ein Hardwareaufbau auf einem FPGA (Xilinx VCU128) realisiert, der die definierte Peripherie (u. a. PCIe, UART, DDR, SPI) unterstützt. Besonderes Augenmerk lag auf der Integration sicherheitsrelevanter Komponenten sowie auf einem leistungsfähigen, stabilen Systemdesign. Die Hardwarearchitektur wurde so konzipiert, dass sie sowohl eine abgesicherte Ausführungseinheit als auch die flexible Anbindung an externe Kommunikationsmodule unterstützt. Die Eignung der Plattform für Echtzeitanforderungen wurden im Design berücksichtigt.

AP 3:

Das Ziel bestand darin, kritische Dienste in einer abgesicherten Ausführungseinheit auszuführen, um die Angriffsfläche für diese Dienste zu verringern und somit die Zuverlässigkeit und Sicherheit zu erhöhen. In einem weiteren Schritt sollte die Einheit als performante TEE (Trusted Execution Environment) realisiert werden. Dabei sollte eine In-Prozessisolation erarbeitet werden, die die Anforderungen von AP1 erfüllt.

Der in AP1 definierte Anwendungsfall stellt eine Applikation in den Vordergrund, die aus verschiedenen Komponenten besteht, denen aus Sicherheitsperspektive teilweise nicht vertraut werden kann. Um diesen Komponenten dennoch Schutz zu bieten, sollen sie durch eine Separierung voneinander getrennt werden. Dabei spielen zwei Eigenschaften eine wichtige Rolle: Speicherschutz und sichere Kontextwechsel. Der Speicherschutz stellt sicher, dass nur die Komponente, die gerade ausgeführt wird, auf ihre Daten zugreifen darf und andere Komponenten zu keinem Zeitpunkt darauf zugreifen können. Sichere Kontextwechsel sollen gewährleisten, dass das Wechseln der Zugriffsrechte kontrolliert erfolgt und nicht von den Spezifikationen abweicht. Schließlich ergibt sich noch der Anspruch auf effiziente Kontextwechsel, da die Applikation durch die Unterteilung in einzelne Komponenten hochfrequent Kontextwechsel durchführt.

Im Rahmen dieses Arbeitsschritts wurden vorhandene Implementierungen von Trusted Execution Environments (TEEs) und In-Prozessisolation evaluiert. Dabei zeigte sich, dass der Kontextwechsel bei TEEs wie Keystone zu einem hohen Performanzverlust führen kann, da hierfür viele CPU-Zyklen benötigt werden. Die In-Prozessisolation bietet hingegen wesentlich effizientere Möglichkeiten für den Kontextwechsel.

Da Kontextwechsel von den verwendeten Speicherschutzmechanismen abhängig sind, wurde evaluiert, welche möglichen Umsetzungen es für den Speicherschutz im Rahmen der Isolation gibt. Dabei haben sich zwei Varianten herausgestellt, die auch in vorangegangenen Arbeiten bereits zum Einsatz kamen: herkömmlicher Zugriffsschutz und Verschlüsselung der Daten.

Ein Aspekt, der in vorangegangenen Arbeiten nur am Rande behandelt wird, ist der Schutz vor Seitenkanalangriffen. Unsere Evaluation hat ergeben, dass die meisten In-Prozessisolierungen nicht analysieren, inwieweit sie gegen diese Art von Angriffen schützen. Um den Anforderungen

aus AP1 zu entsprechen, ist es daher ein wichtiger Aspekt dieses Arbeitsschrittes, dass wir verschiedene Lösungen hinsichtlich dieser Art von Angriffen analysieren, um den durch In-Prozessisolation erbrachten Schutz zu erhöhen. Da der Bereich der Seitenkanalangriffe sehr umfangreich ist, fokussieren wir uns im Folgenden auf eine Klasse von Angriffen, die besonders schwer zu erkennen und zu verhindern sind. Im Folgenden haben wir In-Prozessisolation daher im Hinblick auf transiente Ausführungsangriffe analysiert, wobei wir uns insbesondere auf Spectre-Angriffe konzentriert haben, die das Feature der spekulativen Ausführung ausnutzen, um unbemerkt Daten zu extrahieren. Die spekulative Ausführung ist dabei kein Bug, sondern ein Feature, das in modernen Prozessoren die Performance erhöht. Bei herkömmlicher Prozessisolation gibt es bereits verschiedene Gegenmaßnahmen, die Angriffe erschweren oder verhindern sollen. Diese sind jedoch auf der Ebene der In-Prozessisolation nicht anwendbar.

Um Spectre-Angriffe auf In-Prozessisolation zu analysieren, haben wir verschiedene Spectre-Gegenmaßnahmen und In-Prozessisolierungen untersucht. Dabei haben wir ein Modell erstellt, mit dem wir verschiedene Punkte in einer Spectre-Angriffssequenz identifizieren konnten, die sich besonders gut für die Anwendung in der In-Prozessisolation eignen. Dabei haben sich drei Elemente herausgestellt, die für die In-Prozessisolation verwendet werden können. Zum einen bietet der Zugriffsschutz einen beachtlichen Schutz, auch bei spezifischen Spectre-Angriffen, sofern er sowohl architekturell als auch spekulativ funktioniert. Dabei kann dieser Zugriffsschutz über Zugriffsberechtigung, Verschlüsselung oder Maskierung gleichermaßen Schutz bieten. Der zweite Aspekt sind sichere Kontextwechsel für spekulativen Kontrollfluss. Hier muss verhindert werden, dass die Sicherheitsmechanismen ausgehebelt werden, wenn die Ausführung nur spekulativ erfolgt. Der letzte Aspekt, den wir identifiziert haben, ist die Ausführungsprävention. Ein Angriffsvektor bei Spectre-Angriffen besteht darin, dass sich die Ausführung im spekulativen Modus stark von der architekturellen Ausführung unterscheiden kann. Das kann dazu führen, dass Kontextwechsel in der spekulativen Ausführung nicht beachtet werden und die Komponenten undefiniert gewechselt werden. Diese Angriffsstrategie ist zwar komplexer, kann aber dennoch dazu führen, dass Daten extrahiert werden. Um dies zu verhindern, sorgt die Ausführungsprävention dafür, dass nur die Komponenten spekulativ ausgeführt werden, die zu diesem Zeitpunkt auch architekturell ausgeführt werden können.

Unsere Analyse ergab, dass der Zugriffsschutz weitreichend in der In-Prozessisolation vorhanden ist, während sichere Kontextwechsel für spekulative Ausführungen nur implizit in einzelnen Implementierungen zu finden sind. Eine Ausführungsprävention ist dagegen weitgehend nicht umgesetzt.

Da es bereits einige wissenschaftliche Arbeiten zur In-Prozessisolation gibt, war es für Silkkostu eine wichtige Fragestellung, inwieweit diese Arbeiten erweitert werden können, um eine effizientere und sicherere In-Prozessisolation zu ermöglichen. In Zusammenarbeit mit der RPTU Kaiserslautern haben wir deshalb eine Hardwareerweiterung entwickelt, die sich auf den Schutz gegen Spectre-Angriffe fokussiert. Diese Lösung erweitert die Hardware so, dass diese über ein zusätzliches Bit die Erlaubnis erhält, auf bestimmten Daten zu spekulieren. Dieses Bit wird bei einem korrekten Zugriff gesetzt und kann über eine eigens dafür vorgesehene Instruktion wieder zurückgesetzt werden. Design-Details sind unter Punkt 6, Veröffentlichungen, zu finden.

AP 4:

In diesem Arbeitsschritt sollten die Software- und Hardwaresysteme aus AP2 und AP3 zusammengeführt und ersten Tests unterzogen werden.

Aufbauend auf der Analyse in AP3 haben wir verschiedene In-Prozessisolierungen getestet und sie entsprechend mit den drei identifizierten Elementen für den Seitenkanalschutz ausgestattet. Dabei haben wir eine Isolation verwendet, die auf Memory Protection Keys (MPK) aufbaut, einem Zugriffsschutzfeature auf User-Level, und diese entsprechend erweitert. MPK stellt Zugriffsschutz für verschiedene Domänen bereit, sodass in Silkkostu Komponenten unterschiedlichen Domänen zugeordnet werden können. Diese können über spezifische Instruktionen effizient geändert werden. Ein Aspekt von MPK ist, dass es implizit den Schutz für sichere Kontextübergänge unter Berücksichtigung spekulativer Ausführung ermöglicht. Ausführungsprävention kann hingegen nicht durch MPK umgesetzt werden, da MPK nur Lese- und Schreibrechte verwalten kann. Um diesen Schutz

zu simulieren, haben wir hier den Ausführungsschutz mithilfe des mprotect-Systemaufrufs umgesetzt. Dieser Systemaufruf kann auch zur Verwaltung von Rechten verwendet werden, einschließlich Ausführungsrechten.

Ein weiterer Bestandteil unserer Arbeiten war die Entwicklung von Compiler-Erweiterungen, die für die Verwendung der erforschten Techniken benötigt werden. In Zusammenarbeit mit der RPTU wurden verschiedene Optionen für die Verwendung der neuen Instruktionen untersucht, die entweder automatisch oder durch manuelles Annotieren die benötigten Instruktionen einfügen können. Ein weiterer Aspekt, der hier betrachtet wurde, ist die automatisierte Trennung einer Applikation in verschiedene Komponenten im Zusammenspiel mit einer Compilererweiterung. Dabei wurden verschiedene Ebenen der automatisierten Unterteilungen untersucht.

UzL-ITI: Die zuvor entworfene Hardware wurde mit der entwickelten TEE-Struktur auf dem Board 2 zusammengeführt. In einem internen Integrationstest konnte erfolgreich ein Linux-Betriebssystem gebootet und ein Enklavenstart demonstriert werden. Die Integration der Funkmodule wurde hardwareseitig abgeschlossen, die vollständige Verifikation der PCIe-Schnittstelle war projektbedingt jedoch noch nicht vollständig abgeschlossen. Die einzelnen Komponenten wurden modular verbunden und in mehreren Testszenarien auf ihre Kompatibilität und Funktion geprüft.

AP 5

In diesem Arbeitspaket sollten die erstellten Komponenten evaluiert und getestet werden. Darüber hinaus sollte eine Sicherheitsanalyse zur architekturellen und mikroarchitekturellen Sicherheit durchgeführt werden.

Im Rahmen dieses Arbeitspakets wurden die erweiterten In-Prozessisolationen analysiert und auf ihre Sicherheit gegen Spectre-Angriffe überprüft. Dazu wurden drei Angriffsszenarien erstellt, in denen die verschiedenen Schutzelemente gegen unterschiedliche Spectre-Angriffsvarianten getestet wurden. Bei diesen Tests konnte die Wirksamkeit der drei Elemente nachgewiesen werden. Im weiteren Verlauf wurde die Ausführungsprävention in Bezug auf die Performance mit Lösungen ohne diese Erweiterung verglichen. Dabei verursacht die exemplarische Umsetzung mit dem mprotect-Systemaufruf einen signifikanten Overhead. Im Rahmen des Projekts war es zeitlich nicht möglich, eine hardwarebasierte Lösung für die Ausführungsprävention zu erarbeiten und zu testen.

Im Rahmen eines Demonstrators wurde eine Beispielanwendung entwickelt, die über einen Netzwerktreiber mit einem Endpunkt kommuniziert. Dabei wurden sowohl die Anwendung als auch der Netzwerktreiber in eine Enklave ausgelagert, um die Inter-Enklaven-Kommunikation zu simulieren. Diese Anwendung dient dazu, einen realistischen Use Case im Rahmen von Silkostu darzustellen.

Die Sicherheitsanalyse, die sich aus den zuvor diskutierten Analysen und Evaluierungen von Prozess- und In-Prozessisolation ergibt, zeigt, welche Elemente für eine In-Prozessisolation erforderlich sind, um auch Schutz gegen Seitenkanalangriffe zu gewährleisten. Während die im Rahmen von Silkostu durchgeführten Forschungsarbeiten die Sicherheitseigenschaften der In-Prozessisolation durch entsprechenden Schutz gegen Spectre-Angriffe verbessern, sind andere Mikroarchitektur-Angriffe immer noch möglich. Viele Seitenkanäle lassen sich jedoch durch Software-Gegenmaßnahmen oder eine fehlerfreie Hardware-Implementierung lösen und stellen damit keine so schwerwiegende Bedrohung wie Spectre-Angriffe dar.

UzL-ITI war maßgeblich an der Erstellung und Bewertung eines funktionalen Demonstrators auf Basis von Board 2 beteiligt. Dieser beinhaltete die wesentlichen Komponenten der RISC-V-Architektur und der TEE-Funktionalität. Für den Test wurden Enklaven gestartet. Eine Kommunikation mit externen Funmodulen wurde zudem auf einem RISC-V basierten Hostsystem umgesetzt. Das Setup ermöglichte realitätsnahe Evaluierungsszenarien und diente der Bewertung auf Systemebene.

BVM

AP1

Eine der Aufgaben der Freien und Hansestadt Hamburg (FHH), vertreten durch die BVM, war es die Anwendungsanforderungen der Stadt Hamburg als Infrastruktur Betreiber sowie potenzieller Anwender im öffentlichen Sektor (Verkehrsbetriebe, Feuerwehr, Polizei) bei der Entwicklung einer C-ITS-Kommunikationseinheit einzubringen und deren Erfüllung zu validieren. Unterstützt wurde die BVM bei diesen Aktivitäten durch ihren Realisierungsträger HHVA (Hamburg Verkehrsanlagen GmbH).

Zu den Anforderungen gehören unter anderem:

- Die Kompatibilität mit der städtischen C-ITS Security Infrastruktur
- Die Erfüllung der BSI-KritisV
- Die Überprüfbarkeit der Funktionalität auch im Betrieb
- Eine gute Performance zur Erfüllung der C-ITS Use Cases
- Anforderungen des Datenschutzes.
- Die Möglichkeit der Durchführung von Registrierungsprozesse auch durch Dritte
- Anforderungen, welche aus dem Ziel der Implementierung und Betrieb der Kommunikationseinheiten in Fahrzeugen der öffentlichen Hand (z.B. Feuerwehr, Polizei, ÖPNV) erwachsen, wie zum Beispiel geeignete Zertifizierungen zum dauerhaften Betrieb in öffentlichen Fahrzeugen sowie die notwendigen Schnittstellen zum Bordrechner des Fahrzeugs.

Beim Zusammentragen der Anforderungen wurden auch die Erfahrungen aus dem Austausch mit den Hamburger Verkehrsbetrieben und der Feuerwehr im Kontext von Projekten zur Priorisierung mit C-ITS-Technologie berücksichtigt.

Eine weitere Aufgabe der BVM in diesem Zusammenhang war im Austausch mit anderen Städten/Kommunen und Institutionen (wie z.B. Verkehrsbetrieben) die allgemeine Sensibilisierung für das Thema Security und Trust in der V2X-Kommunikation voranzubringen. Dies geschah im Rahmen von allgemeinen Vorträgen sowie in bilateralen Gesprächen. Ein besonderes Augenmerk lag dabei auf den beiden Verkehrsunternehmen Hamburger Hochbahn AG und Verkehrsbetriebe Hamburg Holstein GmbH. Grund hierfür ist, dass beide in naher Zukunft die Ausstattung Ihrer kompletten Flotten mit C-ITS-Kommunikationseinheiten beginnen und daher wichtig ist, dass sie sich den Sicherheitsanforderungen bewusst sind.

Im Rahmen der Use-Case-Definition wurden zunächst die aktuellen ITS-Projekte der BVM präsentiert. Anschließend wurden potenzielle Use-Cases herausgearbeitet und gemeinsam mit den Projektpartnern abgestimmt. Dabei wurde die Priorisierung des öffentlichen Personennahverkehrs als wichtigster Use-Case ausgewählt. Für die Tests und Demonstrationen (AP5) wurden von Seiten der der Stadt Hamburg die betrieblichen und organisatorischen Anforderungen festgelegt. Zudem wurden mögliche Szenarien und Standorte für den Demonstrator diskutiert sowie ein Umsetzungsplan für die zweite Jahreshälfte 2024 erstellt.

In der Begleitung des Gesamtfortschrittes des Projekts wurde sichergestellt, dass die städtischen Anforderungen aus AP1 Berücksichtigung finden.

AP 2

Hier war die BVM nicht beteiligt

AP 3

Hier war die BVM nicht beteiligt

AP 4

Hier war die BVM nicht beteiligt

AP 5

Gemäß dem Umsetzungsplan (AP1) wurde ein geeignetes Gebiet für den Demonstrator gemeinsam mit HHVA identifiziert. Infrastruktureitige Anforderungen wurden in die Planung eingebracht

und die Strecke wurde durch HHVA hardware-technisch für Test- und Demonstrationsfahrten ausgerüstet.

Sobald die Kommunikationseinheiten bereit für Tests waren, wurde deren Versorgung mit den notwendigen Daten für eine Priorisierung an den Lichtsignalanlagen der Demonstrator-Strecker sichergestellt. Die Test- und Demonstrationsfahrten wurden durch die FHH begleitet, sodass dabei die Einhaltung der erarbeiteten, städtischen Anforderungen überprüft werden konnte.

Insbesondere konnte eine Anbindung an die städtische PKI (Public-Key-Infrastructure) realisiert und der Use-Case der Priorisierung von Bussen mit den entwickelten Komponenten erfolgreich auf der Straße demonstriert werden.

2. die wichtigsten Positionen des zahlenmäßigen Nachweises

CIT

AP 1: keine Abweichungen

AP 2: keine Abweichungen

AP 3: keine Abweichungen

AP 4: Kostenneutrale Verlängerung um 3 Monate, auf Grund von Lieferschwierigkeiten, gemäß Änderungsantrag.

AP 5: keine Abweichungen

G&D

AP 1: keine Abweichungen

AP 2: keine Abweichungen

AP 3: keine Abweichungen

AP 4: nicht beteiligt

AP 5: Kostenneutrale Verlängerung um 3 Monate. Um die Zusammenarbeit des Gesamtprojekts nicht zu gefährden und den Partnern eine Unterstützung in der Verlängerung zu geben, hat Giesecke+Devrient seine Aktivitäten entsprechend ebenfalls verlängert.

UzL-ITI & UzL-ITS

AP 1: keine Abweichungen

AP 2: keine Abweichungen

AP 3: Kostenneutrale Verlängerung um 3 Monate, auf Grund von Lieferschwierigkeiten, gemäß Änderungsantrag.

AP 4: Steht in Zusammenhang mit AP3

AP 5: keine Abweichungen

BVM

Aufgrund von Umstellungen im SAP-System verzögerten sich stadt-interne Abrechnungen, so dass zunächst weniger Mittel als geplant abgerufen wurden.

Ferner wurde festgestellt, dass die Personalmittel fälschlicherweise als Position 0822 deklariert wurden. Daher wurde eine Umwidmung in die korrekten Positionen 0812 und 0817 durchgeführt. Hierbei wurden insbesondere Mittel für eine Projektassistenz eingerichtet werden, welche zur erfolgreichen Durchführung des Projektes notwendig war.

AP 1: keine Abweichungen

AP 2: nicht beteiligt

AP 3: nicht beteiligt

AP 4: nicht beteiligt

AP 5: keine Abweichungen

3. Notwendigkeit und Angemessenheit der geleisteten Arbeit

CIT:

Die Technologie, verschiedene Kommunikationswege in Verbund mit mobilen Anwendungen zu realisieren, benötigte intensive Recherchen zur Prüfung der Umsetzung; insbesondere das Zusammenspiel von Hard- und Software war ein großer Bestandteil der Recherche.

Das Erstellen einer passenden Infrastruktur, die sowohl mobil als auch stationär betrieben wird, benötigte eine umfassende Planung, die Realisierung der technologischen Entwicklung und deren umfangreiche Evaluation. Dies rechtfertigte den geplanten und tatsächlichen Aufwand bei der Umsetzung. Die Skalierbarkeit, Sicherheit im Backend, auf den umgesetzten Systemen und die Anbindung an die Infrastruktur musste an allen Schnittstellen berücksichtigt werden. Auch die Verwendung verschiedener Schnittstellen durch Umschalten durfte die Sicherheit nicht beeinflussen. Alle Tätigkeiten waren notwendig und angemessen, um die Projektergebnisse zu erzielen.

G&D

Die Weiterentwicklung und Absicherung der eSIM-Technologie sowie die Implementierung von Fernverwaltungs- und Updatefunktionen erforderten intensive konzeptionelle und praktische Arbeiten. Insbesondere das Zusammenspiel mit den unterschiedlichsten Netzwerkkomponenten (z. B. 5G/6G-Modem) und die Berücksichtigung hoher Sicherheitsansprüche machten eine umfassende Planung sowie wiederholte Entwicklungs- und Testzyklen notwendig. Durch die Herausforderungen der Demonstrierbarkeit – viele sicherheitsrelevante Abläufe sind für Außenstehende nicht sichtbar – war ein zusätzlicher Aufwand für das Erstellen spezieller Demonstratoren erforderlich.

All dies rechtfertigt den eingeplanten Ressourcenbedarf und unterstreicht die Angemessenheit der geleisteten Arbeiten. Zum einen wurde so gewährleistet, dass die entwickelten Funktionen (Profiltausch und Updatefähigkeit der Authentisierung) praxisnah erprobt werden konnten. Zum anderen konnten durch enge Abstimmung mit den Projektpartnern Synergieeffekte genutzt werden, um die zentrale Steuerbarkeit der eSIM (z. B. bei Angriffsszenarien) zielgerichtet umzusetzen. Damit wird die Sicherheit und Resilienz der V2X-Kommunikation deutlich gesteigert, was die projektierte Arbeits- und Kostenplanung retrospektiv als notwendig und angemessen bestätigt.

UzL-ITI

Die Entwicklung einer abgesicherten RISC-V-basierten Plattform zur Ausführung eines Trusted Execution Environments (TEE) erforderte eine tiefgehende Auseinandersetzung mit der hardwarenahen Systemarchitektur, insbesondere im Hinblick auf die sichere Ausführung sensibler Anwendungen in einem offenen, modularen Umfeld.

Die Erarbeitung einer geeigneten Architektur, die sowohl vertrauenswürdige Ausführung als auch Schnittstellen für moderne Kommunikationsmodule (z. B. 5G, C-V2X) unterstützt, machte eine umfassende Planung und Entwicklung erforderlich. Dabei mussten funktionale Anforderungen, Sicherheit und Erweiterbarkeit in Einklang gebracht werden. Die Kombination aus FPGA-Entwicklung, TEE-Integration und Schnittstellenanbindung erforderte eine enge Verzahnung zwischen Hardwaredesign und softwareseitiger Steuerung.

Die entwickelten Komponenten wurden in ein lauffähiges Gesamtsystem integriert und evaluiert. Die Arbeiten waren notwendig, um die angestrebte digitale Souveränität technisch fundiert umzusetzen. Der dafür aufgewendete Arbeitsumfang war sowohl technisch als auch organisatorisch gerechtfertigt und angemessen, um die gesetzten Projektziele zu erreichen.

UzL-ITS

Die In-Prozessisolation ist ein wichtiges Feld der effizienten Applikationsisolation und kann in vielen Bereichen Anwendung finden. Obwohl es bereits einige Vorarbeiten zu diesem Themenfeld gab, ist naheliegend, dass frühere Lösungen noch keine umfassende Sicherheit gegenüber Architekturelle und Mikroarchitekturelle Angriffen bieten. Unsere Ergebnisse konnten diese These bestätigen und Lösungswege aufzeigen, um die vorhandenen Probleme zu beheben. Eine umfangreiche Sicherheitsanalyse war diesbezüglich notwendig, um Ergebnisse mit entsprechend hohen Sicherheitsanforderungen zu erzielen.

BVM

Durch die Berücksichtigung städtischer Anforderungen bei der Entwicklung von C-ITS-Kommunikationseinheiten wurde sichergestellt, dass eine Lösung entsteht, welche nicht nur für Hamburg, sondern auch für andere Kommunen, geeignet ist. Insbesondere wird der Weg für einen späteren flächendeckenden Einsatz geebnet, bei welchem keine nachträglichen Anpassungen notwendig werden. Durch die Erfahrungen aus anderen C-ITS-Projekten leistete die BVM somit einen wichtigen Beitrag für einen nachhaltigen Erfolg des Projekts.

Die Vorbereitung des Demonstrators im städtischen Kontext erforderte die Identifikation eines geeigneten Testgebiete, die Festlegung der betrieblichen und organisatorischen Anforderungen sowie die hardware-technische Ausstattung der Hamburger Infrastruktur entlang Teststrecke. Teil hiervon war auch die Sicherstellung der Anbindung der SILKOSTU-Kommunikationseinheiten an die Hamburger PKI, damit die Kommunikation mit der Lichtsignalanlage gewährleistet ist. Darüber hinaus war die Begleitung der Test- und Demonstrationsfahrten durch HHVA essenziell, um sicherzustellen, dass die Kommunikation einwandfrei funktioniert und dass ggf. notwendige kleinere Anpassungen direkt durchgeführt werden konnten.

Insgesamt macht dies sowohl den geplanten als auch den realen Aufwand der BVM bei der Realisierung nachvollziehbar und notwendig, um die Ziele des Projekts zu erreichen.

4. Voraussichtlicher Nutzen und Verwertbarkeit

CIT:

CIT konnte im Projekt wesentliche technologische Grundlagen schaffen, um zukünftig eine abgesicherte Kommunikationsinfrastruktur für den V2X-Bereich in urbanen Räumen zu realisieren. Der entwickelte Demonstrator erlaubt die gleichzeitige Nutzung und Absicherung mehrerer Kommunikationsstandards (5G/6G, C-V2X, V2X-dsrc) in einem modularen Hardwareaufbau. Dies bietet die notwendige Flexibilität für zukünftige Marktanforderungen - insbesondere unter der Prämisse, dass sich auf europäischer Ebene noch kein einheitlicher Kommunikationsstandard etabliert hat.

Die hohe Integrationsdichte sicherheitsrelevanter Funktionen - etwa über eUICC, Hardware-TEE und standardisierte Schnittstellen - bildet die Voraussetzung für eine sichere Kommunikation in Echtzeit und damit für eine großflächige Skalierbarkeit in Smart-City-Anwendungen. CIT konnte durch die Projektdurchführung seine Kompetenzen im Bereich hardwaregestützter Kommunikationssysteme mit Sicherheitsfokus signifikant erweitern.

CIT verfügt bereits über bestehende Kundenbeziehungen im Bereich V2X-Kommunikationseinheiten und erwartet ab Ende 2025 erste Verkäufe auf Basis der im Projekt entwickelten Technologie. Durch die bereits angekündigten Vorbestellungen und das wachsende Interesse von Städten und Flottenbetreibern - insbesondere für Anwendungen wie Bus- oder Einsatzfahrzeug-Priorisierung - wird ein Absatzvolumen von mindestens 2.000 Einheiten jährlich ab Ende 2027 als realistisch angenommen. Beim Ausbau der Infrastruktur wird ein ähnliches Absatzvolumen angenommen.

Die Projektergebnisse sind so angelegt, dass sie über das Projekt hinaus anschlussfähig bleiben. CIT plant die Weiterentwicklung der Boards und deren Optimierung, um den Hardwareeinsatz zu minimieren und die Systemintegration weiter zu verbessern. Diese Weiterentwicklung wird voraussichtlich ab 2027 zu neuen Produkten führen, die modular in bestehende Smart-City-Infrastrukturen integriert werden können - sowohl stationär als auch mobil.

Zudem ergeben sich neue Forschungsfragen an der Schnittstelle von Kommunikationssicherheit, Energiemanagement und Echtzeitsystemverhalten. CIT positioniert sich damit nicht nur als Systemintegrator, sondern zunehmend auch als Innovationsmotor im Bereich vernetzter Mobilitätslösungen.

CIT kann damit zukünftig einen wichtigen Beitrag zur „Vision Zero“ und der Steigerung der Resilienz urbaner Mobilitätssysteme leisten.

G&D

- Zentrale Verwaltung und Updatefähigkeit

Die im Rahmen von SILKOSTU weiterentwickelten eSIM-Technologien (z.B. SGP.32-Protokoll, Fernwartbare Authentisierung) ermöglichen ein zentrales Management von Mobilfunkzugängen. Damit wird ein Wechsel vom bislang lokal administrierten Mobilfunkzugang hin zu einer zentral gesteuerten, hochsicheren Infrastruktur unterstützt.

- Einsatz in unterschiedlichen Märkten

Durch die im Projekt gezeigte Updatefähigkeit der eSIM lassen sich neue Anwendungen im IoT-Kontext sowie in vernetzten Verkehrsszenarien (V2X, Logistik, Smart Home, Smart Car) adressieren. G+D plant, die Lösungen binnen ca. zwei Jahren in die nächste Generation von eSIM-Produkten einfließen zu lassen. Insbesondere im Automotive-Bereich ist für Funktionen wie Over-the-Air-Profilwechsel ein langfristiges (2–4 Jahre) Marktpotenzial erkennbar.

- Erhöhte Resilienz und Sicherheit

Dank zentralen Profil- und Authentisierungsupdates lassen sich Angriffssituationen zeitnah abfedern. Dies stärkt die Resilienz im laufenden Betrieb und bietet Unternehmen sowie öffentlichen Stellen einen deutlichen Mehrwert – etwa in Flottenanwendungen oder bei smarten Stadtinfrastrukturen.

- Standardisierung und globale Vermarktung

Auf Basis der im Projekt erprobten Mechanismen (z.B. Updatefähigkeit der Netzwerkauthentisierung) wird G+D die Ergebnisse in internationale Gremien (z.B. GSMA, GlobalPlatform) einbringen. Daraus erwächst eine größere Interoperabilität am Weltmarkt. In etwa vier Jahren werden erste Produkte erwartet, die diesem erweiterten Standard genügen und global einsetzbar sind.

- Nachhaltige Einbindung in künftige Produktentwicklungen

Die Entwicklungen aus SILKOSTU fließen unmittelbar in G+D-interne Roadmaps ein. Langfristig soll dadurch eine breite Verwertung in verschiedenen Branchen (Automotive, IoT, Smart City) erfolgen. Das Projekt hat zudem gezeigt, dass zentrale Sicherheitslösungen für vernetzte Systeme nur durch enge Zusammenarbeit mit Partnern (etwa CIT oder anderen Forschungseinrichtungen) rasch und effizient in marktreife Plattformen überführt werden können.

UzL-ITI

Die im Projekt entwickelten Konzepte zur Integration einer Trusted Execution Environment (TEE) auf einer quelloffenen RISC-V-Plattform wurden im Rahmen einer wissenschaftlichen Arbeit aufbereitet und für die Veröffentlichung vorbereitet. Im Fokus standen dabei die Beschleunigung von TEE, insbesondere durch hardwaregestützte Optimierungen zur effizienteren Ausführung vertrauenswürdiger Enklaven bei gleichzeitig erhöhter Sicherheit gegenüber spekulativen Angriffen.

Diese Ergebnisse bilden die Grundlage für weiterführende Forschungsarbeiten im Bereich hardwareunterstützter Sicherheitsarchitekturen. Die entwickelten Mechanismen eröffnen neue Perspektiven für den Entwurf effizienter, vertrauenswürdiger Systemkomponenten in sicherheitskritischen Anwendungen.

UzL-ITS

Die Forschungsergebnisse von Silkostu wurden oder werden auf Konferenzen veröffentlicht. Unsere Analyse hat besondere Schwierigkeiten vorhandener Lösungen aufgezeigt und präsentiert auch Ansätze zur Erhöhung der Sicherheit. Dies eröffnet insbesondere für zukünftige Forschungsarbeiten viele Möglichkeiten, die In-Prozessisolierung in Bezug auf Performanz und Sicherheit zu verbessern. Die Inhalte der Forschungsarbeiten fanden außerdem Anwendung in der Lehre. So wurde beispielsweise ein Aspekt der Forschungsarbeiten in einer Master-Fallstudie umfangreich untersucht.

BVM

Die BVM profitiert auf vielfältige Weise von den Projektergebnissen: Bereits während der Projektlaufzeit können erste Komponenten der neuen Technologie in der Hamburger Infrastruktur integriert werden, um den Weg für einen späteren flächendeckenden Einsatz zu ebnen. Speziell On-Board-Units (OBUs), die den städtischen Anforderungen entsprechen, ermöglichen es nicht nur Hamburg, sondern auch anderen Kommunen, politische Ziele wie die Attraktivitätssteigerung des öffentlichen Nahverkehrs (z.B. in Hamburg via Busbeschleunigung im Rahmen des „Hamburg Takts“) oder die Gewährleistung von Hilfsfristen für die Feuerwehr durch gezielte Priorisierung umzusetzen.

Ein weiterer Nutzen liegt in der zunehmenden Ausstattung des Individualverkehrs mit vernetzten Systemen, wodurch Dienste wie GLOSA (Green Light Optimized Speed Advisory) ihr volles Potenzial entfalten und positive Effekte auf die Emissionsreduktion erzielen können. Durch die Beteiligung an Kooperationsprojekten wie C-Roads werden die gewonnenen Erkenntnisse anderen Städten zur Verfügung gestellt und der Erfahrungsaustausch gefördert.

Das Projekt SILKOSTU liefert der BVM wichtige Grundlagen für die Entscheidung über den Roll-Out von C-ITS-Diensten im urbanen Kontext, insbesondere hinsichtlich Technologieauswahl und verkehrssteuernder Anwendungen. Insbesondere wird mit einer steigenden Durchdringung vernetzter Verkehrsteilnehmer gerechnet, unterstützt durch die Harmonisierung der Kommunikationsstandards im Rahmen von C-Roads und Initiativen wie dem Car-2-Car Communication Consortium. Dies schafft die Voraussetzungen für sichere, ressourcenschonende und effiziente Mobilität auch außerhalb des Projekts.

Die BVM erwartet, dass zeitnah sowohl Nachrüst- als auch Erstausrüstungsmöglichkeiten für C-ITS-Technologien zur Verfügung stehen werden, sodass sowohl öffentliche als auch private Fahrzeuge ausgestattet werden können. Damit leistet das Vorhaben einen wesentlichen Beitrag zur Mobilitätswende.

Eine über die allgemeinen Erwartungen an Ergebnisse des Vorhabens, entsprechend den obigen Erläuterungen, hinausgehende wirtschaftliche Verwertung strebt die BVM nicht an.

5. Fortschritt bei anderen Stellen

CIT:

Der in dem Projektantrag vorgesehene Verwertung steht nach aktuellen Recherchen nichts im Wege. Uns sind keine Produkte, Marktentwicklungen oder Förderprojekte bekannt, die der geplanten Verwertung entgegenstehen.

G&D

G+D hat die aktuellen Entwicklungen im Bereich sicherer Mobilfunkkommunikation und IoT-Anwendungen fortlaufend beobachtet und in Austausch mit anderen Institutionen sowie Standardisierungsgremien (z. B. GSMA) gestanden. Nach aktuellem Kenntnisstand existieren keine konkurrierenden Produkte oder Forschungsergebnisse, die den beabsichtigten Einsatz oder die Vermarktung der im Projekt erzielten Ergebnisse beeinträchtigen würden.

UzL-ITI & UzL-ITS

Die Forschungsarbeiten im Rahmen von SILKOSTU bilden eine gute Grundlage für zukünftige Forschung. So konnte entsprechendes Know-how erlangt und ausgetauscht werden. Der geplanten Verwertung steht nichts entgegen.

BVM

Nach unserem Kenntnisstand gibt es keine Produkte, Marktentwicklungen oder Förderprojekte, die den Entwicklungen im Projekt SILKOSTU widersprechen.

6. Erfolgte und geplante Veröffentlichungen (Website, Paper, Messeauftritt...)

CIT:

Projekt-Webseite

<https://www.silkostu.de/>

Abschlusspost

https://www.linkedin.com/posts/leutrimmustafa_silkostu-cit-c-activity-7311015054450040833-DJd4/?originalSubdomain=de

G&D

Beitrag/Nachrichtenartikel auf internen Unternehmensplattformen. Derzeit wird geplant, Elemente aus dem Demonstrator, der für die Präsentation der Funktionen beim Abschlussmeeting des Projekts entwickelt wurde, auf Messen und bei Kundengesprächen einzusetzen.

UzL-ITI & UzL-IST

<https://www.its.uni-luebeck.de/forschung/silkostu>

Philipp Schmitz, Tobias Jauch, Alex Wezel, Mohammad R. Fadiheh, Thore Tiemann, Jonah Heller, Thomas Eisenbarth, Dominik Stoffel, and Wolfgang Kunz,

Okapi: A Lightweight Architecture for Secure Speculation Exploiting Locality of Memory Accesses, in Proceedings of the 20th ACM Asia Conference on Computer and Communications Security, ASIA CCS 2025 (to appear), 2025.

Okapi- Preprint: <https://arxiv.org/abs/2312.08156>

BVM

<https://www.hamburg.de/politik-und-verwaltung/behoerden/bvm/die-themen-der-behoerde/intelligente-verkehrssysteme/archiv/sicherheit-in-der-its-kommunikation-963832>

<https://lsbg.hamburg.de/ueber-uns/unsere-geschaeftsbereiche/lsbg-digital/its-projekte-und-ministerielle-aufgaben/silkostu>

Weitere

[5G/6G Forum: Cybersicherheit und digitale Souveränität - Sicherheit gemeinsam gestalten - cybersicherheit-bsi.de](#)

[BSI - SILKOSTU – Cyber-Sicherheit in der intelligenten 5G/6G-Kommunikation zwischen Verkehrsteilnehmenden für eine lernende städtische Infrastruktur und höhere Verkehrssicherheit - Projekt SILKOSTU](#)