Gefördert durch:

Bundesministerium
für Forschung, Technologie
und Raumfahrt

HoVerSiD

Gemeinsamer Sachbericht

Verbundvorhaben HoVerSiD: Homomorphe Verschlüsselung für Sichere Offene Urbane Datenplattformen in der Cloud

Datum: 12.06.2026

Editoren: Stephan Borgert ([ui!]), Lisa Brunzel ([ui!]), Philipp Lämmel (FOKUS)

Projektlaufzeit: 01.05.2023 – 30.04.2026

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Konsortium

[ui!] the urban institute®	Konsortialführung Urban Software Institute GmbH - [ui!] **Förderkennzeichen: 16KIS1866K** Stephan Borgert Rößlerstraße 88, 64293 Darmstadt Stephan.Borgert@the-urban-institute.de Telefonnummer: +49 (0) 160 858 7586
Fraunhofer FOKUS	Fraunhofer FOKUS **Förderkennzeichen: 16KIS1867** Philipp Lämmel Kaiserin-Augusta-Allee 31, 10589 Berlin philipp.laemmel@fokus.fraunhofer.de Telefonnummer: +49 30 34637256

Inhalt

1 Aufgabenstellung 1
1.1 [ui!] 1
1.2 FOKUS 1
2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde 2
2.1 [ui!] 3
2.2 FOKUS 3
3 Planung und Ablauf des Vorhabens 4
3.1 [ui!] 4
3.2 FOKUS 5
4 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde 5
4.1 [ui!] 6
4.2 FOKUS 6
5 Zusammenarbeit mit anderen Stellen 7
6 Erzielte Ergebnisse mit Gegenüberstellung der vorgegebenen Ziele 8
6.1 AP 1 Use Cases entwickeln, Anforderungen, technische Architektur, Projektmanagement 8
6.1.1 AP 1.1 Projektmanagement 8
6.1.2 AP 1.2 Use Cases 8
6.1.3 AP 1.3 Anforderungen 9
6.1.4 AP 1.4 Technische Architektur 10
6.2 AP 2 Homomorphe Verschlüsselung: Theoretische und technische Vorarbeiten 10
6.2.1 AP 2.1 Stand der Technik im Bereich Homomorphe Verschlüsselung 10
6.2.2 AP 2.2 Standardisierung 11
6.2.3 AP 2.3 Open-Source-Lösungen 11
6.2.4 AP 2.4 Installation und Einrichtung der [ui!] UrbanPulse Demonstrator-Basis 12
6.3 AP 3 Konzeption, Umsetzung und Integration Homomorphe Verschlüsselung 12
6.3.1 AP 3.1 Konzeption und Umsetzung von HE-Kernkomponenten auf der UrbanPulse 12
6.3.2 AP 3.2 Konzeption und Umsetzung von HE-Layer auf der UrbanPulse 13
6.3.3 AP 3.3 Konzeption und Umsetzung von HE-Verschlüsselung für Identitäts- und Zugriffsmanagement 14

6.3.4 AP 3.4 Erforschung und Umsetzung von HE für weitere Datenbanken für weitere sensible Daten 14

6.3.5 AP 3.5 Erforschung und Umsetzung von Plattform- und logischen Services zur Nutzung der HE 14

6.3.6 AP 3.6 Erforschung und Umsetzung von HE-Adaptern zur Ertüchtigung von Plattform- und logischen Services 14

6.4 AP 4 Validierung der theoretischen Konzepte 15

6.4.1 AP 4.1 Einrichtung der Validierungsumgebung und Definition von Test-Cases und Test-Verfahren 15

6.4.2 AP 4.2 Anwendung der Test-Cases und Test-Verfahren unter Nutzung der Validierungsumgebung 17

6.4.3 AP 4.3 Fehlerbehebung, technische Verstetigung und abschließende Validierung 19

7 Wichtigste Positionen des zahlenmäßigen Nachweises 20

8 Notwendigkeit und Angemessenheit der geleisteten Arbeit 20

9 Voraussichtlicher Nutzen 20

9.1 [ui!] 21

9.2 FOKUS 22

10 Bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen 22

11 Erfolgte oder geplanten Veröffentlichungen des Ergebnisses 23

1 Aufgabenstellung

Moderne Public-Cloud-Plattformen der Hyperscaler bieten Kommunen und kommunalen Unternehmen eine ausgereifte, hochverfügbare und wirtschaftlich attraktive Grundlage, um digitale Smart-City-Lösungen zu betreiben. Zugleich unterliegen sie strengen rechtlichen Anforderungen. Die Verarbeitung personenbezogener Daten nach der EU-Datenschutz-Grundverordnung (DSGVO) sowie die Souveränität über sensible Verwaltungsdaten müssen jederzeit gewährleistet sein. Gerade in der öffentlichen Verwaltung bestehen jedoch erhebliche Unsicherheiten über das tatsächliche Schutzniveau der Public Cloud, etwa durch den CLOUD Act der USA, das Schrems-II-Urteil oder den Zugriff beauftragter Drittunternehmen im Rahmen des Supports.

Das Kernprodukt des Konsortialführers [ui!], die DIN-SPEC-91357-konforme Offene Urbane Datenplattform [ui!] UrbanPulse, wird überwiegend auf der Microsoft-Azure-Public-Cloud betrieben und ist damit unmittelbar von diesen Unsicherheiten betroffen. Bisherige Auswege wie der Hybrid-Cloud-Betrieb einzelner Komponenten in kommunalen Rechenzentren sind mit deutlich erhöhten Betriebs- und Wartungskosten verbunden und stellen keine langfristig tragfähige Alternative dar.

Die Aufgabenstellung von HoVerSiD bestand darin, die Homomorphe Verschlüsselung (Homomorphic Encryption, HE) als zusätzliches Verschlüsselungsverfahren in Offene Urbane Datenplattformen einzuführen und zu erproben. Der entscheidende Vorteil der HE ist ihre Fähigkeit, Berechnungen direkt auf verschlüsselten Daten auszuführen, ohne diese zuvor zu entschlüsseln. Dadurch bleiben sensible Daten selbst während der Verarbeitung in der Public Cloud geschützt, sodass weder Plattformadministratoren noch externe Dritte Klartextzugriff erhalten. Das Hauptziel von HoVerSiD war es, HE-Verfahren für DIN-SPEC-91357-konforme Offene Urbane Datenplattformen zu erforschen und umzusetzen, um die Datensicherheit beim Betrieb in Public-Clouds im Kontext deutscher und europäischer Kommunen zu maximieren.

Zur Erreichung dieses Ziels wurden drei praxisnahe Anwendungsfälle entwickelt und erprobt: der digitale Wohnberechtigungsschein, die privatsphäreerhaltende Parkraumüberwachung sowie privatsphäreerhaltende Origin-Destination-Analysen. Ergänzend wurde mit einem Policy-Enforcement-Ansatz ein zusätzlicher Sicherheitslayer geschaffen, der die kontrollierte Weiternutzung HE-geschützter Daten über den unmittelbaren Anwendungsfall hinaus ermöglicht.

1.1 [ui!]

[ui!] ist Konsortialführer von HoVerSiD und brachte Anwendungsfälle sowie Anforderungen aus Kunden- und FuE-Projekten ein. Der Forschungs- und Umsetzungsschwerpunkt von [ui!] lag auf allen Arbeiten, die eine erfolgreiche Einbettung der HoVerSiD-Lösung in die [ui!] UrbanPulse und einen tragfähigen Betrieb auf der Public-Cloud-Plattform Microsoft Azure gewährleisten. Ein besonderes Augenmerk galt der möglichst hohen Cloud-Agnostik, die primär durch den Einsatz von Open-Source-Komponenten erreicht wurde. Daraus entstanden die technische Architektur, die Plattformintegration, der Demonstrator sowie der ergänzende Policy-Enforcement-Layer.

1.2 FOKUS

Fraunhofer FOKUS verantwortete die wissenschaftlich-technische Umsetzung und Evaluation

des Lösungsansatzes, insbesondere in den Bereichen der Homomorphen Verschlüsselung sowie der Auswahl und Ertüchtigung geeigneter Open-Source-Implementierungen. FOKUS entwickelte die kryptographischen Kernmodule, darunter die Verfahren CKKS und DGK sowie ein neuronales Netz mit homomorph verschlüsselten Gewichten, und beteiligte sich maßgeblich am Aufbau des Demonstrators. Daneben übernahm FOKUS die Qualitätssicherung, die Performanz- und Lasttests sowie die wissenschaftliche Verbreitung der Projektergebnisse durch Publikationen und die Förderung des wissenschaftlichen Nachwuchses.

2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Die Durchführung von HoVerSiD erfolgte vor dem Hintergrund einer wachsenden Verbreitung Offener Urbaner Datenplattformen in deutschen Städten und Kommunen bei gleichzeitig steigenden Anforderungen an Datenschutz und Datensicherheit. Public-Cloud-Angebote der Hyperscaler bieten die ausgereifteste Technik und die besten Sizing-Möglichkeiten, doch im Finanz- und Versicherungssektor sowie in der öffentlichen Verwaltung herrscht weiterhin Unsicherheit über das reale Schutzniveau. Geänderte Gesetzeslagen wie der CLOUD Act und das Schrems-II-Urteil erleichtern ausländischen Behörden unter bestimmten Voraussetzungen den Zugriff auf Daten, die von US-Konzernen verarbeitet werden. Bereits die Existenz dieser Möglichkeiten führt bei Datenschutzbeauftragten und damit bei Kunden zu Bedenken, die sich auch durch Aufklärung nicht vollständig ausräumen lassen.

Als technische Grundlage diente die Homomorphe Verschlüsselung. Während klassische Verschlüsselung Daten nur bei der Speicherung und beim Transport schützt und für jede Verarbeitung eine Entschlüsselung erfordert, erlaubt die Homomorphe Verschlüsselung, Berechnungen unmittelbar auf dem Chiffretext durchzuführen. Das Ergebnis der Berechnung ist selbst verschlüsselt und entspricht nach der Entschlüsselung dem Ergebnis der Berechnung auf den Klartextdaten. Damit schließt die HE die kritische Schutzlücke während der Verarbeitung.

Die grundlegenden Informationen zur homomorphen Verschlüsselung sind in der Infografik in Abbildung 1 zusammengefasst. Charakteristisch für HE-Verfahren ist das kryptographische Rauschen, das jeden Chiffretext absichert. Additionen lassen das Rauschen linear, Multiplikationen exponentiell anwachsen; überschreitet es eine Schwelle, wird das Ergebnis unbrauchbar. Mittels Bootstrapping kann das Rauschen zurückgesetzt werden, was jedoch sehr rechenintensiv ist und den wesentlichen Performanz-Overhead der HE erklärt. Man unterscheidet partiell homomorphe (PHE), somewhat homomorphe (SHE) und vollständig homomorphe Verfahren (FHE). Ab der zweiten FHE-Generation basieren die Verfahren auf dem Learning-With-Errors-Problem (LWE) und gelten als quantencomputerresistent. Für HoVerSiD besonders relevant waren das CKKS-Verfahren für approximative Arithmetik auf reellen Werten sowie das DGK-Protokoll für sichere Vergleiche.

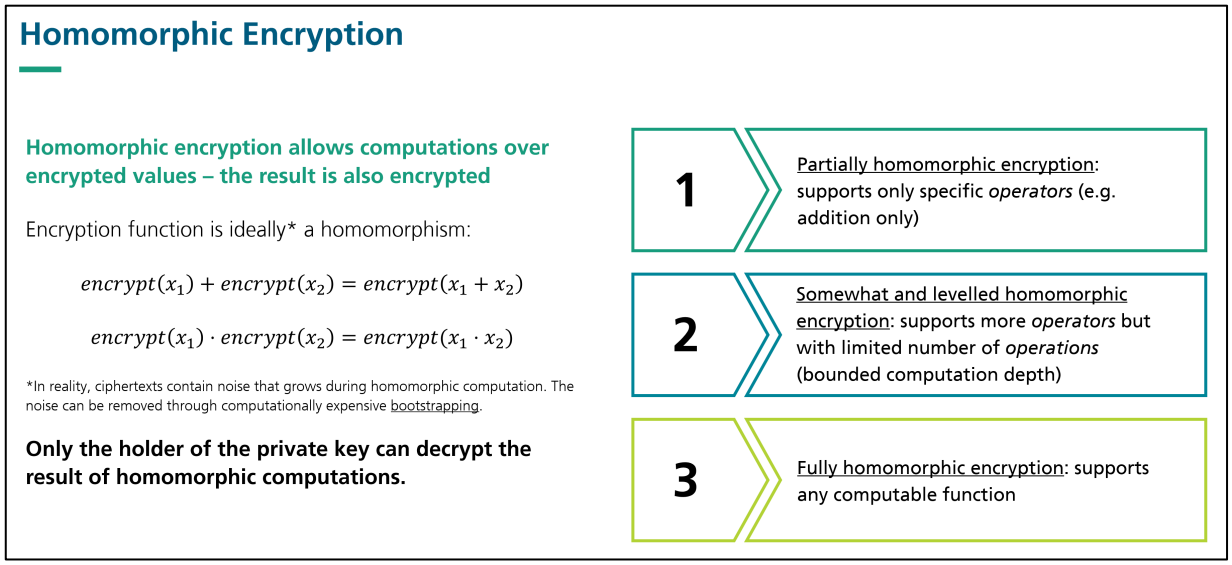


Abbildung 1: Grundprinzipien der homomorphen Verschlüsselung

Die [ui!] UrbanPulse als DIN-SPEC-91357-konforme Plattform mit ihrer Echtzeitarchitektur sowie das ausgewiesene HE- und IT-Sicherheits-Know-how von Fraunhofer FOKUS bildeten die fachliche Ausgangsbasis, auf der die Forschungs- und Umsetzungsarbeiten aufsetzen konnten.

2.1 [ui!]

Die Urban Software Institute GmbH ([ui!]) ist ein führendes Software- und Beratungsunternehmen sowie Inkubator für Smart-City-Lösungen in den Themen nachhaltige städtische Mobilität, emissionsarmer Verkehr, integrierte Straßenbeleuchtung und Energiemanagement für Stadtquartiere. Zu den Kunden zählen Kommunen, Städte und Metropolregionen sowie kommunale und privatwirtschaftliche Unternehmen. Kernprodukt ist die Offene Urbane Datenplattform [ui!] UrbanPulse, die DIN-SPEC-91357-konform und sowohl als Closed-Source- als auch als Open-Source-Variante verfügbar ist. [ui!] verfügt über ausgewiesene Expertise in Echtzeitdatenverarbeitung, Data Analytics, Mehrwertdienst-Entwicklung sowie Maschinellem Lernen und KI und war an mehr als 15 nationalen und internationalen Forschungsprojekten beteiligt.

In HoVerSiD setzte [ui!] auf dieser Basis auf und brachte die langjährige Erfahrung im Betrieb der UrbanPulse auf der Microsoft-Azure-Public-Cloud ein. Die bestehende, durchgängig auf Parallelisierung ausgelegte Echtzeitarchitektur der Plattform sowie die etablierten Integrations- und CI/CD-Prozesse bildeten den unmittelbaren Ausgangspunkt für die Einbettung der HE-Komponenten, der HE-fähigen Konnektoren und des Policy-Enforcement-Layers. Damit war sichergestellt, dass die Forschungsergebnisse nicht im Labor verbleiben, sondern in einer realitätsnahen, einsatzfähigen Plattformumgebung erprobt werden konnten.

2.2 FOKUS

Das Fraunhofer-Institut für Offene Kommunikationssysteme (FOKUS) ist eines der größten Fraunhofer-Institute und mit mehr als 25 Jahren Erfahrung national wie international einer der wichtigsten Akteure der IKT-Forschungslandschaft. Fraunhofer FOKUS entwickelt als neutrales Forschungsinstitut Lösungen für die digitale Vernetzung mit dem Anspruch, die vernetzte Welt sicher, zuverlässig, skalierbar und vertrauenswürdig zu machen. Das Institut

entwickelt und unterstützt zentrale Standardisierungsaktivitäten für Smart Cities, darunter die DIN SPEC 91357 „Referenzarchitekturmodell Offene Urbane Plattform (OUP)“, und ist in zahlreichen Projekten zu Sicherheitstests (DIAMONDS, PREVENT, EU-SEC und weitere) und zur Zertifizierung kritischer Infrastrukturen aktiv.

Im Rahmen von Studien für öffentliche Auftraggeber hatte Fraunhofer FOKUS bereits vor Projektbeginn umfangreiches Know-how im Bereich der Homomorphen Verschlüsselung und ihrer Anwendung zum Schutz sicherheitsrelevanter Daten erarbeitet. Auf diese kryptographische und sicherheitstechnische Kompetenz konnte HoVerSiD unmittelbar aufbauen. FOKUS brachte dieses Fundament gezielt ein, um die wissenschaftlich fundierte Auswahl, Anpassung und Ertüchtigung geeigneter HE-Implementierungen wie Microsoft SEAL, TenSEAL, OpenFHE und Concrete ML voranzutreiben und die kryptographischen Kernverfahren des Projekts, insbesondere CKKS und DGK, für den Einsatz in Offenen Urbanen Datenplattformen nutzbar zu machen.

3 Planung und Ablauf des Vorhabens

Das Vorhaben HoVerSiD wurde von Mai 2023 bis April 2026 durchgeführt und war in vier Arbeitspakete gegliedert. AP1 umfasste die Entwicklung der Use Cases, die Anforderungserhebung, die technische Architektur sowie das Projektmanagement. AP2 schuf die theoretischen und technischen Vorarbeiten zur Homomorphen Verschlüsselung. AP3 verantwortete die Konzeption, Umsetzung und Integration der HE in die Plattform. AP4 diente der Validierung der theoretischen Konzepte am Demonstrator.

Der Ablauf folgte einem iterativen und agilen Vorgehensmodell und verlief in Übereinstimmung mit der Arbeits-, Zeit- und Kostenplanung. Im Jahr 2023 lag der Schwerpunkt auf der Use-Case-Entwicklung, der Anforderungserhebung und der Architekturarbeit. 2024 wurden die HE-Vorarbeiten vertieft, geeignete Open-Source-Bibliotheken evaluiert, die Demonstrator-Basis eingerichtet und erste HE-Kernkomponenten umgesetzt. 2025 standen die Umsetzung und Integration der HE-Layer, des IAM-Konzepts sowie der Aufbau der Validierungsumgebung im Mittelpunkt. Im Jahr 2026 wurden die abschließende Validierung, die technische Verstetigung und der Projektabschluss durchgeführt.

Der Projektfortschritt wurde an vier Meilensteinen gemessen: M1 zu Projektmonat 18 (Implementierung der Methoden und erste Experimente und Systemtests), M2 zu Monat 21 (Abbruchmeilenstein: Demonstrator vorbereitet, erste Forschungsziele zu kritischen Algorithmen und Komponenten erreicht), M3 zu Monat 30 (Plattform und Demonstrator aufgebaut, Methoden entwickelt) und M4 zu Monat 36 (Validierung der theoretischen Konzepte am Demonstrator abgeschlossen). Alle Meilensteine wurden erreicht; das Vorhaben blieb durchgängig sowohl inhaltlich als auch zeit- und budgetbezogen im Plan.

3.1 [ui!]

[ui!] übernahm als Konsortialführer die Gesamtkoordination und steuerte das Vorhaben mit einem agilen Projektmanagement, regelmäßigen Abstimmungen und kontinuierlicher Meilensteinüberwachung. Inhaltlich lag der Schwerpunkt von [ui!] auf AP1 und AP4 sowie auf allen Arbeiten zur Einbettung der Lösung in die [ui!] UrbanPulse. [ui!] modellierte die Use Cases, leitete die Anforderungen ab, entwickelte die technische Architektur und richtete die Demonstrator- und Validierungsumgebung ein. Darüber hinaus konzipierte und erprobte [ui!] den Policy-Enforcement-Layer mit Open Policy Agent, der die kontrollierte Weiternutzung HE-geschützter Daten und die Wahrung der K-Anonymität ermöglicht. Die Arbeiten erfolgten in

enger Abstimmung mit Fraunhofer FOKUS und sicherten die durchgängige Integration der Forschungsergebnisse in eine einsatzfähige Plattformumgebung.

3.2 FOKUS

Fraunhofer FOKUS verantwortete schwerpunktmäßig die wissenschaftlich-technischen Arbeiten in AP2 und AP3 und wirkte in allen weiteren Arbeitspaketen mit. FOKUS erarbeitete den Stand der Technik zur Homomorphen Verschlüsselung, evaluierte und ertüchtigte geeignete Open-Source-Implementierungen und entwickelte die kryptographischen Kernmodule des Projekts, darunter eine eigene DGK-Implementierung, den Einsatz von CKKS sowie ein neuronales Netz mit homomorph verschlüsselten Gewichten für die Kennzeichenerkennung. Zudem entwickelte FOKUS ein datenschutzwahrendes System für die Parkraumüberwachung mit vier Komponenten sowie einen Prototyp eines auf dem DGK-Verfahren basierten WBS-Antragssystems mit einer Frontend- und einer Backend-Komponente. Weiterhin untersuchte FOKUS die Machbarkeit verschlüsselter OD-Analysen und erzielte erste technische Fortschritte dafür. FOKUS übernahm die Qualitätssicherung sowie die Performanz- und Lasttests und konzipierte ein neuartiges Testprotokoll unter Nutzung von HE. FOKUS bereitete die Erkenntnisse in wissenschaftlichen Publikationen auf. Die Arbeiten wurden eng mit [ui!] abgestimmt, um die Anschlussfähigkeit an die Plattform sicherzustellen.

4 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

Das Vorhaben HoVerSiD knüpfte an mehrere relevanten Entwicklungen im wissenschaftlichen und technologischen Stand an. Auf europäischer Ebene bildete insbesondere die Datenstrategie der Europäischen Kommission einen zentralen Referenzrahmen. Diese verfolgt das Ziel, sektorübergreifende europäische Datenräume aufzubauen, unter anderem für öffentliche Verwaltungen, und wird sowohl durch regulatorische Maßnahmen wie den Data Governance Act und den Data Act als auch durch erhebliche Investitionen in Cloud-Infrastrukturen unterstützt. Ergänzend dazu stellt der EU Cloud Code of Conduct einen etablierten Standard zur Sicherstellung der DSGVO-Konformität von Cloud-Diensten dar. Diese Entwicklungen schaffen die Grundlage für vertrauenswürdige, cloudbasierte Datenverarbeitung in Europa und bilden einen wichtigen Ausgangspunkt für HoVerSiD.

Im technischen Umfeld griff das Projekt den aktuellen Stand cloudbasierter Infrastrukturen auf, insbesondere hybride Cloud-Architekturen, wie sie bereits bei der UrbanPulse-Plattform eingesetzt werden. Die Kombination aus öffentlichen Cloud-Angeboten und lokal betriebenen Rechenzentren ermöglicht es, Datenschutzanforderungen umzusetzen, führt jedoch gleichzeitig zu erhöhtem Betriebs- und Wartungsaufwand. Die damit verbundenen Herausforderungen verdeutlichen den Bedarf an innovativen Ansätzen zur sicheren und zugleich wirtschaftlichen Datenverarbeitung in Cloud-Umgebungen.

Auf wissenschaftlicher Ebene baute HoVerSiD maßgeblich auf den Fortschritten im Bereich der homomorphen Verschlüsselung auf. Seit der erstmaligen Einführung voll-homomorpher Verschlüsselungsverfahren durch Gentry im Jahr 2009 hat sich dieses Forschungsgebiet stark weiterentwickelt. Moderne Verfahren, basierend auf gitterbasierten Kryptosystemen und Problemen wie „Learning with Errors“, ermöglichen es, Berechnungen direkt auf verschlüsselten Daten durchzuführen. Insbesondere Weiterentwicklungen wie BGV, BFV oder CKKS sowie effizientere Bootstrapping-Verfahren haben die praktische Anwendbarkeit deutlich

verbessert. Parallel dazu sind erste Open-Source-Bibliotheken und Werkzeuge entstanden, die eine experimentelle Nutzung dieser Verfahren in realen Anwendungsszenarien ermöglichen.

Darüber hinaus existierten bereits erste Forschungsergebnisse zur Anwendung homomorpher Verschlüsselung in rechenintensiven Kontexten wie maschinellem Lernen. Diese zeigen das Potenzial, sensible Daten in Cloud-Umgebungen zu verarbeiten, ohne deren Vertraulichkeit zu gefährden, weisen jedoch auch auf bestehende Herausforderungen hinsichtlich Performanz und Skalierbarkeit hin.

Vor diesem Hintergrund setzte HoVerSiD gezielt an der Schnittstelle zwischen diesen technologischen Entwicklungen an. Das Projekt übertrug die Konzepte der homomorphen Verschlüsselung erstmals systematisch auf Identitätsmanagementsysteme und Offene Urbane Plattformen im Smart-City-Kontext.

4.1 [ui!]

[ui!] knüpfte in HoVerSiD an die eigene, marktführende Offene Urbane Datenplattform [ui!] UrbanPulse an, die DIN-SPEC-91357-konform ist und über eine durchgängig echtzeitfähige, auf hoher Parallelisierung basierende Architektur verfügt. Aus zahlreichen nationalen und internationalen Smart-City-Forschungsprojekten lagen umfangreiche Erfahrungen in der Echtzeitdatenverarbeitung, der Modellierung organisationsübergreifender Prozesse sowie der Integration heterogener Datenquellen über Konnektoren vor. Diese Vorarbeiten bildeten die Grundlage, um HE-fähige Konnektoren, HE-Datenformate und plattformseitige Analysedienste zu entwickeln.

Technologisch baute [ui!] auf etablierte Standards der Offenen Urbanen Datenplattformen und auf das Umfeld Urbaner Digitaler Zwillinge auf, an deren Standardisierung [ui!] im Rahmen der DIN SPEC 91607 mitwirkte. Damit war eine anschlussfähige und interoperable Ausgangsbasis für die Integration der Homomorphen Verschlüsselung in eine produktnahe Plattformumgebung gegeben.

Über die [ui!] UrbanPulse hinaus konnte [ui!] auf einschlägige Vorprojekte aufbauen: Im Vorgängerprojekt KIVEP wurden gemeinsam mit Fraunhofer FOKUS Verfahren zur privatsphäreerhaltenden Protokoll-Anomalie-Erkennung für IoT-Netzwerke untersucht, einschließlich sicherer Deep-Packet-Inspection, Demonstratorentwicklung und Erprobung auf einer offenen urbanen Plattform. Diese Arbeiten lieferten HoVerSiD direkte Vorarbeiten zu IT-Sicherheit, Datenschutz und sicheren kommunalen Dateninfrastrukturen. Aus SDIKA brachte [ui!] Erfahrungen mit sicheren digitalen Identitäten, interoperablen APIs, plattformunabhängigen Adaptern sowie der sicheren Einbindung kommunaler Dienste und Mobilitätsanwendungen ein. Ergänzend lieferte VLUID Vorarbeiten zur Integration heterogener Verkehrs- und Sensordaten, zu nahezu echtzeitfähigen Big-Data-Analysen und zur organisationsübergreifenden Nutzung kommunaler Datenräume. Zusammen bildeten diese Projekte eine belastbare technische Grundlage für die Auswahl, Konzeption und Demonstration privatsphäreerhaltender Verfahren in HoVerSiD.

4.2 FOKUS

Fraunhofer FOKUS konnte in HoVerSiD auf umfangreiches, in Studien für öffentliche Auftraggeber erarbeitetes Know-how im Bereich der Homomorphen Verschlüsselung und ihrer Anwendung zum Schutz sicherheitsrelevanter Daten zurückgreifen. Hinzu kam langjährige Expertise in IT-Sicherheit, Sicherheitstests sowie der Zertifizierung kritischer Infrastrukturen und eine aktive Rolle in der Standardisierung Offener Urbaner Plattformen (DIN SPEC 91357).

FOKUS war an einer Vielzahl von Projekten in den Bereichen Smart Cities/Communities, Cybersicherheit und Datenschutz beteiligt. Diese Projekte umfassen unter anderem:

- **H2020 Triangulum**: Ein Projekt zur Implementierung von Smart City-Lösungen in europäischen Städten.
- **ITEA DIAMONDS**: Ein Projekt zur Verbesserung der Sicherheit und Zuverlässigkeit von Software durch modellbasierte Testmethoden.
- **H2020 EU-SEC**: Ein Projekt zur Entwicklung eines europäischen Sicherheitszertifizierungsrahmens für Cloud-Dienste.
- **H2020 FORTIKA**: Ein Projekt zur Entwicklung von Cyber-Sicherheitslösungen für kleine und mittlere Unternehmen (KMUs).

Darüber hinaus hat FOKUS im Rahmen von Industrieprojekten umfassende Erfahrungen im Testen und Evaluieren von kritischen Infrastrukturen gesammelt.

Durch die Beteiligung an diesen Projekten konnte FOKUS umfangreiche Kenntnisse und technische Fähigkeiten im Bereich der Sicherheit und Datenschutzkonformität der urbanen IT-Systeme entwickeln. Diese Erfahrungen haben es FOKUS ermöglicht, innovative und praxisnahe Lösungen im Rahmen von HoVerSiD zu entwickeln, die hohen Sicherheits- und Datenschutzstandards entsprechen.

Wissenschaftlich knüpfte FOKUS an den aktuellen Stand der Forschung zur Homomorphen Verschlüsselung an. Seit dem ersten vollständig homomorphen Verfahren von Gentry haben sich mehrere Generationen gitterbasierter Verfahren etabliert. HoVerSiD setzte gezielt auf das auf dem Learning-With-Errors-Problem basierende CKKS-Verfahren der vierten Generation, das approximative Arithmetik auf reellen Werten erlaubt, sowie auf das DGK-Protokoll für sichere Vergleiche im Sinne des Millionärsproblems. Auf dieser Basis evaluierte und ertüchtigte FOKUS etablierte Open-Source-Bibliotheken wie Microsoft SEAL, TenSEAL und Concrete ML für den Einsatz in Offenen Urbanen Datenplattformen.

5 Zusammenarbeit mit anderen Stellen

Im Rahmen von HoVerSiD wurde der Anwendungsbezug der Lösungen durch die Einbindung externer Perspektiven kontinuierlich geschärft. Insbesondere wurden Workshops mit relevanten Stakeholdern aus dem Verwaltungsumfeld durchgeführt, um den Praxisbezug der Use Cases zu sichern und ihre Verwertbarkeit zu erhöhen. Aus diesen Workshops ging unter anderem der Anwendungsfall der digitalen Parkraumüberwachung als besonders zukunftsrelevant und umsetzbar hervor.

Daneben wirkte [ui!] in einschlägigen Standardisierungsgremien mit, insbesondere im Kontext der DIN SPEC 91607 zu Digitalen Zwillingen für Städte und Kommunen, und brachte dort Aspekte Offener Urbaner Datenplattformen und ihrer Sicherheit ein. Fraunhofer FOKUS hat die im Projekt HoVerSiD gewonnenen Erfahrungen und Kenntnisse bei der Arbeit an der DIN SPEC 91377 angewandt.

Die wissenschaftlichen Ergebnisse wurden auf der IEEE International Smart Cities Conference 2025 und der Konferenz „Relational and Algebraic Methods in Computer Science“ (RAMICS 2026) mit der Fachöffentlichkeit sowie in der wissenschaftlichen Zeitschrift „Internet of Things“ des Verlags Elsevier geteilt.

Um die Plausibilität und Anwendbarkeit der Use Cases zu validieren, wurden im Rahmen des Projekts Expertengespräche mit erfahrenen Anbietern von Verkehrskameras und Verkehrsanalysten geführt. Darüber hinaus wurde das Projekt im Live-Podcast-Format [ui!]

Flurfunk vorgestellt, hierbei wurden das Fokusthema „Privatsphäre-erhaltende Datenanalyse“ präsentiert und diskutiert.

In Rahmen des Projekts wurden zwei Masterarbeiten verfasst, eine zusammen mit Humboldt-Universität zu Berlin und eine mit der TU Berlin.

6 Erzielte Ergebnisse mit Gegenüberstellung der vorgegebenen Ziele

Im Folgenden werden die erzielten Ergebnisse entlang der Arbeitspaketstruktur dargestellt und den im Arbeitsplan angestrebten Zielen gegenübergestellt. Sämtliche Arbeiten wurden gemäß Zeit- und Arbeitsplan durchgeführt und die angestrebten Ziele und Ergebnisse erreicht.

6.1 AP 1 Use Cases entwickeln, Anforderungen, technische Architektur, Projektmanagement

Angestrebte Ergebnisse laut Arbeitsplan: *Systematisches, agil ausgerichtetes Projektmanagement; Spezifikation relevanter Use Cases für den Einsatz Homomorpher Verschlüsselung in Smart Cities; Anforderungskatalog; technische Architektur, die die Nutzung von HE beim Betrieb Offener Urbaner Datenplattformen in der Public-Cloud ermöglicht.*

6.1.1 AP 1.1 Projektmanagement

[ui!] übernahm als Konsortialführer die Gesamtkoordination und leitete das Vorhaben effektiv und effizient. Das Projektmanagement wurde agil abgewickelt, mit regelmäßigen Abstimmungen, kontinuierlicher Fortschrittsüberwachung und durchgängiger Meilensteinkontrolle. [ui!] sicherte die Kommunikation mit relevanten Stakeholdern und erschloss frühzeitig Synergiepotenziale für die Use Cases mit Verwaltungsfokus. Die gemeinsame Entwicklungspipeline und die Zusammenarbeit der Partner [ui!] und Fraunhofer FOKUS funktionierten hervorragend; das Projekt wurde planmäßig und erfolgreich abgeschlossen.

6.1.2 AP 1.2 Use Cases

Es wurden drei praxisrelevante Use Cases ausgewählt:

1. **Der digitale Wohnberechtigungsschein (WBS).** Das zentrale Kriterium für die Erteilung eines Wohnberechtigungsscheins (WBS) ist, dass das Einkommen der antragstellenden Person unter einem festgelegten Schwellenwert liegt. Die Übermittlung dieser Einkommensdaten birgt jedoch ein Datenschutzrisiko, da sie gemäß DSGVO in Kombination mit weiteren Angaben aus dem Antrag als personenbezogene Daten gelten. Durch den Einsatz homomorpher Verschlüsselung kann die Prüfung, ob das Einkommen unterhalb des Schwellenwertes liegt, erfolgen, ohne dass das exakte Einkommen gegenüber der zuständigen Behörde offengelegt werden muss. Auf diese Weise wird die Einkommensüberprüfung sowohl zuverlässig und nachvollziehbar als auch datenschutzkonform durchgeführt. Dies führt zu einem erhöhten Schutz sensibler persönlicher Daten im WBS-Antragsverfahren.

2. **Privatspäreerhaltende Parkraumüberwachung.** Die Überwachung öffentlicher Parkflächen unterliegt strengen Vorgaben der DSGVO, da dabei personenbezogene Daten (insbesondere Fahrzeugkennzeichen) verarbeitet werden. Gleichzeitig besteht im Falle von Ordnungswidrigkeiten, wie dem Falschparken, ein berechtigtes Interesse daran, diese Daten

zur Ahndung nutzen zu können. Daraus ergibt sich ein Spannungsfeld zwischen effektiver Kontrolle und Datenschutz. Ziel dieses Anwendungsfalls ist es, diesen Konflikt mithilfe homomorpher Verschlüsselung aufzulösen. In der technischen Umsetzung wurde der Fokus auf die automatisierte Erkennung von Falschparkern gelegt. Eine lokal installierte Kamera erfasst Bilder des Parkplatzes und verschlüsselt diese unmittelbar. Die verschlüsselten Bilddaten werden anschließend durch ein speziell trainiertes, homomorph arbeitendes Convolutional Neural Network (CNN) verarbeitet. Ergänzend erfolgt ein verschlüsselter Abgleich zur Identifikation von Verstößen mit Daten aus einem Parkscheinautomaten. Erst nach dem Abgleich werden ausschließlich die Kennzeichen der als Falschparker klassifizierten Fahrzeuge entschlüsselt. Das System gewährleistet somit näherungsweise die Eigenschaft, dass ausschließlich relevante Daten (d. h. Verstöße) sichtbar gemacht werden, während alle anderen Informationen verschlüsselt und somit geschützt bleiben. Auf diese Weise kann die Identifikation von Falschparkern erfolgen, ohne die Privatsphäre regelkonform parkender Personen zu beeinträchtigen. Der Anwendungsfall Parkraumüberwachung ging unmittelbar aus intensiven Workshops mit relevanten Stakeholdern hervor und wurde als besonders zukunftsrelevant und umsetzbar bewertet.

3. **Datenschutzwahrende Origin-Destination Analysen.** Gemäß DSGVO gelten alle Informationen als personenbezogene Daten, die zur Identifizierung einer Person beitragen können. Dieses Risiko besteht auch bei pseudonymisierten Verkehrsdaten, die häufig als Grundlage für Origin-Destination-Analysen (OD-Analysen) genutzt werden. So kann beispielsweise eine regelmäßig aufgezeichnete Route zwischen Wohnort und Arbeitsplatz Rückschlüsse auf die Identität einer Person ermöglichen. Trotz dieser Risiken sind OD-Analysen ein zentrales Instrument für die Verkehrsplanung, da sie wertvolle Einblicke in Mobilitätsmuster liefern. Ziel dieses Anwendungsfalls ist, OD-Analysen mithilfe homogener Verschlüsselung so umzusetzen, dass eine indirekte Identifizierung von Personen ausgeschlossen wird. Ein solches System ermöglicht es Kommunen, fundierte Entscheidungen für eine effiziente und nachhaltige Verkehrsplanung zu treffen, während gleichzeitig ein hohes Maß an Datenschutz gewährleistet bleibt.

[ui!] erarbeitete die Prozessmodelle mit Ereignisgesteuerten Prozessketten (EPK), BPMN und subjektorientierter Modellierung (S-BPM), bewertete die Umsetzbarkeit und leitete die technischen Anforderungen für die Integration in die [ui!] UrbanPulse ab.

Fraunhofer FOKUS betrachtete die Anwendungsfälle aus wissenschaftlicher Perspektive, prüfte die technische Machbarkeit und konzipierte erste Architekturvorschläge. Als eine Idee für ein Use Case wurde ein neues Testprotokoll unter Verwendung der homomorphen Verschlüsselung konzipiert. Nach einer Prüfung wurde die technische Umsetzung des Protokolls jedoch als kostspielig und der Nutzen als nicht ausreichend bewertet. Trotzdem hat FOKUS das theoretische Konzept in einem Paper verfasst und auf RAMICS 2026 veröffentlich und präsentiert.

6.1.3 AP 1.3 Anforderungen

Auf Basis der modellierten Use Cases wurde ein Anforderungskatalog mit funktionalen und nichtfunktionalen Anforderungen erarbeitet und mittels eines agilen Vorgehensmodells iterativ verfeinert. Im Jahr 2025 wurde der Anforderungskatalog vollständig finalisiert; alle Anforderungen für die Use Cases und ihre Umsetzung in Demonstratoren lagen erhoben vor.

[ui!] brachte die Expertise zur UrbanPulse-Integration ein und lenkte den Anforderungsprozess.

Fraunhofer FOKUS erarbeitete eine wissenschaftlich fundierte Bewertung der Sicherheits-

und Datenschutzanforderungen, gestützt auf vertiefende Literaturrecherchen zur Funktionsweise und Sicherheit Homomorpher Verschlüsselung.

6.1.4 AP 1.4 Technische Architektur

Als technische Zielarchitektur wurde eine Erweiterung der DIN-SPEC-91357-konformen Offenen Urbanen Datenplattform um Homomorphe Verschlüsselung, Identitäts- und Zugriffsmanagement sowie einen Policy-Enforcement-Layer erarbeitet und fertiggestellt. Ziel und Ergebnis war eine Architektur, die Daten in Public-Cloud-Szenarien so schützt, dass selbst Plattformadministratoren oder externe Zugriffe ausschließlich verschlüsselte Daten sehen.

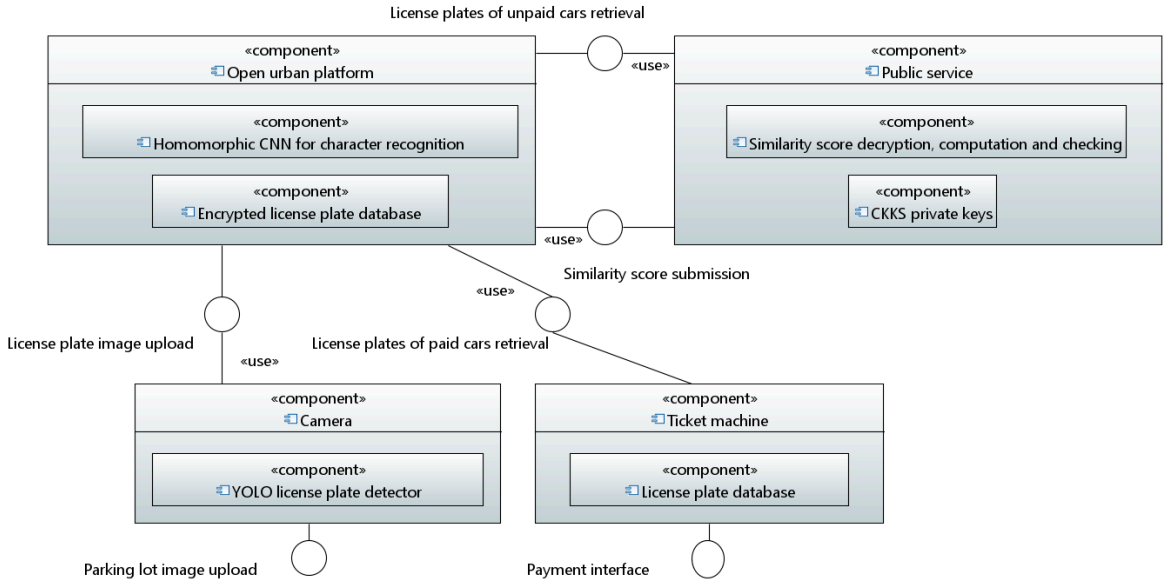


Abbildung 2: Komponentenarchitektur der privatsphäreerhaltenden Parkraumüberwachung (Use Case 2) mit homomorphem CNN, verschlüsselter Kennzeichendatenbank und behördenseitiger Entschlüsselung.

[ui!] erarbeitete die Architektur-Erweiterung der UrbanPulse-Plattform zur effizienten Integration der neuen Sicherheitsmechanismen.

Fraunhofer FOKUS verfasste Architekturentwürfe für die zu den Use Cases relevanten Subsysteme, analysierte die Datenschutz- und Sicherheitsimplikationen, definierte Maßnahmen zur Erhöhung der Datensicherheit und übernahm die Konzeption der HE-Module.

6.2 AP 2 Homomorphe Verschlüsselung: Theoretische und technische Vorarbeiten

Angestrebte Ergebnisse laut Arbeitsplan: *Bewerteter Überblick über existierende HE-Methoden; Erfassung relevanter Standardisierungsaktivitäten; Selektion und Erprobung geeigneter Open-Source-Lösungen für die Integration in OUPs; Demonstrator-Basis.*

6.2.1 AP 2.1 Stand der Technik im Bereich Homomorphe Verschlüsselung

Es wurde ein fundierter theoretischer Überblick über die Homomorphe Verschlüsselung erarbeitet. Dabei wurden über 20 projektrelevante wissenschaftliche Arbeiten ausgewertet und die Grundlagen von Key Generation, Verschlüsselung, Evaluation und Entschlüsselung sowie das kryptographische Rauschen und das Bootstrapping systematisch erfasst. Partiell, somewhat und vollständig homomorphe Verfahren wurden ebenso eingeordnet wie die FHE-

Generationen, die ab der zweiten Generation auf dem quantencomputerresistenten Learning-With-Errors-Problem beruhen, einschließlich des CKKS-Verfahrens. Auch aktuelle Entwicklungen der Post-Quanten-Kryptografie wurden berücksichtigt.

[ui!] untersuchte industrielle HE-Implementierungen und ihre Integration in datenintensive Cloud-Umgebungen und erstellte Benchmarks zur Effizienz.

Fraunhofer FOKUS führte die wissenschaftliche State-of-the-Art-Analyse zu jedem Use Case durch. Für die WBS-Antragstellung wurden wissenschaftliche Quellen zu HE-Protokollen für sichere Vergleiche analysiert, für die Kennzeichenerkennung wurden gezielt Arbeiten zu Public-Key-HE mit der Fähigkeit zur Ausführung neuronaler Netze und für die OD-Analyse Publikationen über homomorphe Traceverarbeitung recherchiert.

6.2.2 AP 2.2 Standardisierung

Zur Förderung der Interoperabilität wurde eine Analyse aktueller nationaler und internationaler Standardisierungsvorhaben durchgeführt. Der Fokus lag insbesondere auf Entwicklungen im Bereich der homomorphen Verschlüsselung (HE), darunter relevante Standards ISO/IEC 18033-6:2019 sowie Initiativen von HomomorphicEncryption.org. Die Konzeption der HoVerSiD-Lösung orientierte sich konsequent an der DIN SPEC 91357 für Offene Urbane Datenplattformen. Vor dem Hintergrund der Projektfokussierung auf Cloud-Infrastrukturen, Offene Urbane Datenplattformen sowie Urbane Digitale Zwillinge wurde insbesondere die Kompatibilität zwischen nationalen Plattformstandards und internationalen HE-Standardisierungsinitiativen untersucht. Die im Projekt gewonnenen Erkenntnisse wurden von beiden Projektpartnern in die Arbeit relevanter Standardisierungsgremien eingebracht und tragen somit zur Weiterentwicklung zukünftiger nationaler Standards bei. Damit wurde sichergestellt, dass die Projektergebnisse anschlussfähig und interoperabel zu etablierten Standards ausgerichtet sind.

[ui!] identifizierte relevante Standardisierungsgremien und arbeitete an der Evaluierung bestehender Normen, insbesondere in Bezug auf Datenschutzanforderungen in Smart Cities. Dazu wirkte [ui!] im Gremium der DIN SPEC 91607 (Digitaler Zwilling für Städte und Kommunen) mit.

FOKUS analysierte die Standardisierungsbemühungen aus wissenschaftlicher Perspektive und evaluierte die zukünftige Einbindung in das HoVerSiD-Projekt. Zusätzlich brachte FOKUS die im Projekt gesammelten Erfahrungen in das Gremium der DIN SPEC 91377 ein.

6.2.3 AP 2.3 Open-Source-Lösungen

Verschiedene Open-Source-HE-Bibliotheken wurden anforderungsbasiert evaluiert und hinsichtlich ihrer Eignung für den HE-Layer und ihrer Integrierbarkeit in Cloud-Umgebungen bewertet. Ausgewählt und durch rapide Prototypenentwicklung erprobt wurden insbesondere OpenFHE, Concrete, Microsoft SEAL sowie deren Erweiterungen für neuronale Netze wie TenSEAL und Concrete ML. Für die Gesamtlösung kamen darüber hinaus etablierte Open-Source-Technologien zum Einsatz, darunter React, Node.js, Flask, NumPy, PyTorch, YOLOv8, ein CNN mit homomorphen Gewichten, Open Policy Agent, Quarkus, Keycloak, OpenSearch und H2.

[ui!] analysierte die Bibliotheken hinsichtlich Skalierbarkeit und Leistungsfähigkeit und führte erste Testimplementierungen für Smart-City-Anwendungen durch.

Fraunhofer FOKUS bewertete die kryptografischen Verfahren wissenschaftlich hinsichtlich Sicherheit und Effizienz und wählte die für die Systemarchitektur geeigneten Bibliotheken aus.

6.2.4 AP 2.4 Installation und Einrichtung der [ui!] UrbanPulse Demonstrator-Basis

[ui!] richtete eine dedizierte Demonstrator-Basis auf Grundlage der [ui!] UrbanPulse ein, die als Entwicklungs- und Testplattform für die Integration der HE-Technologie diente. Auf Basis von Docker und OpenShift wurde gemeinsam mit den in AP2.3 evaluierten Open-Source-Bibliotheken eine Entwicklungspipeline aufgesetzt, die eine effiziente Integration in die UrbanPulse und eine belastbare Vergleichbarkeit der Evaluationsergebnisse ermöglichte.

6.3 AP 3 Konzeption, Umsetzung und Integration Homomorphe Verschlüsselung

Angestrebte Ergebnisse laut Arbeitsplan: *Erweiterung der UrbanPulse-OUP und einer Open-Source-Lösung für Identitäts- und Zugriffsmanagement um die Fähigkeit, kritische Daten mittels HE zu verarbeiten; Absicherung sensibler Daten bei der Ablage in der Public-Cloud; Adapter zur Ertüchtigung von Plattform-Services; HoVerSiD-Demonstrator.*

6.3.1 AP 3.1 Konzeption und Umsetzung von HE-Kernkomponenten auf der UrbanPulse

Es wurden HE-Kernfunktionen für die Use Cases umgesetzt und validiert. Für den Wohnberechtigungsschein wurden CKKS für Berechnungen und DGK für sichere Schwellwertvergleiche im Sinne einer Einkommensprüfung implementiert; für die Parkraumüberwachung wurde ein Schlüsselmanagement implementiert, um die Nutzung homomorpher Verschlüsselung für verteilte Workflows zwischen Kameras, Parkautomaten, OUPs und öffentlichen IT-Systemen zu ermöglichen. Dazu wurden Ver- und Entschlüsselungsroutinen orchestriert. Im Rahmen von AP 3.1 wurden ergänzend auf der [ui!] UrbanPulse weitere DSGVO-konforme Sicherheitsmechanismen implementiert. Hierzu gehörten insbesondere ein Policy-Creator sowie ein Policy-Enforcement-Point. Diese Komponenten ermöglichen eine regelbasierte Steuerung der Datenverarbeitung und stellen sicher, dass die für Analysen bereitgestellte Datengrundlage gezielt begrenzt wird. Dadurch können Rückschlüsse auf einzelne Fahrzeuge vermieden und Anforderungen an die K-Anonymität erfüllt werden. Die Daten bleiben somit weiterhin für statistische Auswertungen und analytische Fragestellungen nutzbar, ohne die Privatsphäre betroffener Personen oder Fahrzeughalter zu gefährden. Ein relevanter Anwendungsfall hierfür ist die mobile ANPR-Erfassung im Kontext der Parkraumüberwachung. Durch mobile Erfassungssysteme kann die Überwachung von Parkflächen effizienter gestaltet werden. Gleichzeitig entsteht die Möglichkeit, auch solche Flächen als Smart-City-Datenquelle zu erschließen, die nicht mit stationärer Sensorik ausgestattet sind. Die implementierten Sicherheitsmechanismen tragen dabei dazu bei, dass die erhobenen Daten nur in datenschutzkonformer, zweckgebundener und aggregierter Form innerhalb der UrbanPulse verarbeitet werden.

[ui!] identifizierte über eine Stand-der-Technik-Analyse geeignete Bausteine für Policy-Durchsetzung und Policy-Management sowie für Identitäts- und Schlüsselmanagement der homomorphen Verschlüsselung. [ui!] implementierte Schlüsselmanagement für HE. Weiterhin definierte [ui!] die notwendigen HE-Erweiterungen und setzte sie zusammen mit FOKUS um.

Fraunhofer FOKUS erarbeitete die Grundlagen für die effiziente Verarbeitung verschlüsselter Daten und finalisierte die kryptographische Funktionalität. In den HE-Kernkomponenten entwickelte Fraunhofer FOKUS eigene Implementierungen des DGK-Protokolls und integrierte

TenSEAL, um CKKS-basierte Inferenz bei neuronalen Netzen zu ermöglichen.

6.3.2 AP 3.2 Konzeption und Umsetzung von HE-Layer auf der UrbanPulse

Der HE-Layer wurde als Integrations- und Abstraktionskonzept der UrbanPulse-Plattform ausspezifiziert. Die Funktionalität des HE-Layers wurde aus den Use Case Anforderungen abgeleitet. Einkommens-, Ticket- und Kameradaten werden homomorph verschlüsselt an die Plattform übertragen, dort verschlüsselt verarbeitet und als verschlüsseltes Ergebnis an die zuständige Stelle weitergegeben; die Plattformadministration sieht ausschließlich verschlüsselte Daten. Die Kopplungspunkte zwischen OUP-Komponenten und HE-Bausteinen wurden einschließlich Datenfluss-, Rollen- und Vertrauensannahmen spezifiziert und als technische Artefakte dokumentiert. Verfolgt wurde durchgängig ein ganzheitlicher End-to-End-Ansatz: Die Schutzwirkung der HE wird nicht durch angrenzende Technologiebausteine reduziert, sondern durch komplementäre Policy- und Governance-Konzepte mit belastbarer Rückverfolgbarkeit bis zu den HE-Ergebnissen abgesichert.

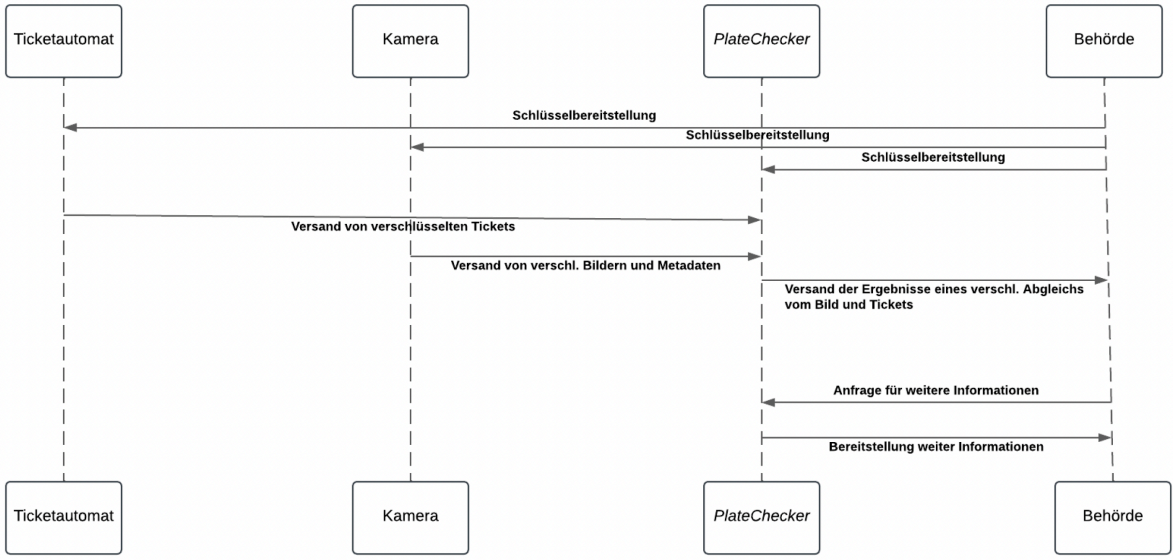


Abbildung 3: Datenfluss der Parkraumüberwachung. Kennzeichen werden homomorph verschlüsselt übertragen, auf der Plattform abgeglichen und nur das verschlüsselte Ergebnis an die Behörde übergeben.

[ui!] konkretisierte die in AP3.1 entwickelten Erweiterungen im Kontext der UrbanPulse-Plattform und überführte die von FOKUS bereitgestellten Schnittstellenmodelle in eine konsistente Spezifikation für die Plattformintegration. Auf Basis der Ergebnisse von Stand-der-Technik-Analyse aus AP 3.1 wurden die Erweiterungen und die notwendigen Verbindungen zwischen den Plattformkomponenten implementiert und als Proof of Concept Demonstrator des HE-Layers umgesetzt. Im Fokus standen die Ausarbeitung der Interaktions- und Datenflüsse zwischen OUP-Komponenten und HE-Bausteinen sowie die formale Beschreibung Use-Case-spezifischer HE-Datenformate (inkl. Serialisierungs- und Transportrepräsentationen).

Fraunhofer FOKUS identifizierte und definierte die notwendigen Schnittstellen und ertüchtigte verschiedene HE-Implementierungen (Microsoft SEAL, TenSEAL, Concrete ML) für die Integration in den HE-Layer.

6.3.3 AP 3.3 Konzeption und Umsetzung von HE-Verschlüsselung für Identitäts- und Zugriffsmanagement

Als Fortsetzung der Arbeiten aus AP 3.2 wurde ein ganzheitliches IAM-Konzept für OUP-Plattformen erarbeitet, welches die Berechtigung zum Zugriff auf und zur Entschlüsselung von HE-Ergebnissen über wohldefinierte Rollen-, Policy- und Vertrauensannahmen eindeutig regelt. Dadurch können ausschließlich autorisierte Instanzen, etwa die zuständige Bußgeldstelle im Kontext der Parkraumüberwachung, HE-Ergebnisse kontrolliert erhalten und entschlüsseln. Als Enterprise-Authentifizierung im Demonstrator wurde Keycloak eingesetzt.

[ui!] leitete Personas, Rollen- und Verantwortlichkeitsmodelle ab, klassifizierte die schutzbedürftigen Artefakte und überführte sie in ein konsistentes Autorisierungsschema mit Least-Privilege- und Separation-of-Duties-Prinzipien.

Fraunhofer FOKUS führte eine wissenschaftliche Analyse des Einsatzes von HE im Identitäts- und Zugriffsmanagement durch. Daraus leitete FOKUS Einsatzprinzipien für HE ab, die als Leitfaden für die Konzeption von HE-Projekten dienen können.

6.3.4 AP 3.4 Erforschung und Umsetzung von HE für weitere Datenbanken für weitere sensible Daten

Die Speicherung HE-verschlüsselter Daten auf den Storage-Komponenten der [ui!] UrbanPulse wurde sowohl auf lokalen als auch auf Cloud-Alternativen erprobt und validiert. Insbesondere wurde die Funktionalität zur Speicherung verschlüsselter Kennzeichen sowie verschlüsselter Ähnlichkeitsmatrizen für die Parkraumüberwachung umgesetzt.

[ui!] entwickelte ein auf HE angepasstes Data-Storage-Konzept und ermöglichte geeignete Queries, um Daten zuverlässig abzufragen und für die HE-Weiterverarbeitung aufbereitet bereitzustellen.

Fraunhofer FOKUS definierte die notwendigen Schnittstellen zur Ablage der Daten im Cloud-Storage und übernahm einen Teil der Implementierungsaufgaben.

6.3.5 AP 3.5 Erforschung und Umsetzung von Plattform- und logischen Services zur Nutzung der HE

Es wurden mehrere logische Services und Anwendungssichten konzipiert, umgesetzt und erfolgreich erprobt: ein verschlüsselter Abgleich für Parkverstöße, eine Bußgeldverwaltung, eine Verkehrsplanungssicht mit aggregierten Parkanalysen sowie ein Policy-Management. Der Demonstrator zeigt rollenabhängige Sichtbarkeit, K-Anonymität, Bußgeldvalidierung und Zeitraumbeschränkung.

[ui!] verantwortete die Ausmodellierung der Use Cases, die Interface-Modelle und die Anpassung der Plattform-Services zur Ertüchtigung der HE-Verfahren.

Fraunhofer FOKUS entwickelte eine Datenabgleichoperation auf Grundlage von HE-Daten sowie einen Service zur Erkennung einzelner Buchstaben in homomorph verschlüsselten Bildern mittels neuronaler Netze mit homomorphen Gewichten, der für die Parkraumüberwachung notwendig ist.

6.3.6 AP 3.6 Erforschung und Umsetzung von HE-Adaptern zur Ertüchtigung von Plattform- und logischen Services

Damit die erforschten Funktionalitäten wieder- und neuverwertet werden können, wurde ein

Adapter-Konzept erarbeitet, das je nach Art der Homomorphen Verschlüsselung die Einbettung verschlüsselter Daten in Verarbeitungsschritte ermöglicht. Da je nach Anwendungsfall unterschiedliche HE-Verfahren sinnvoll sind, etwa wenn nur Additionen benötigt werden, wurde die Konfigurierbarkeit des einzusetzenden HE-Verfahrens konzipiert und auf Basis der Vorarbeiten der übrigen Arbeitspakete umgesetzt.

[ui!] verantwortete, konzeptionierte die Adapter und hat sie in den HE-Layer integriert, sodass Policy-, Identitäts- und Schlüsselmanagement auch die Adapter unterstützen.

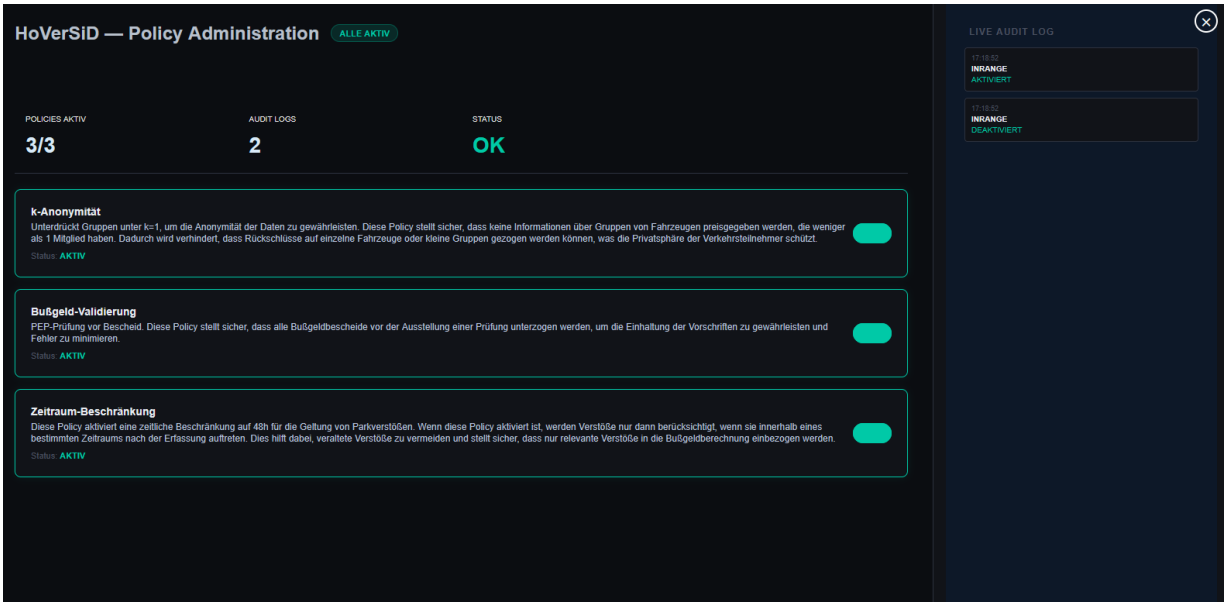
Fraunhofer FOKUS unterstützt die technische Umsetzung der notwendigen Adapter, so dass die im Rahmen von HoVerSiD umgesetzte HE für alle Komponenten verwendet werden kann.

6.4 AP 4 Validierung der theoretischen Konzepte

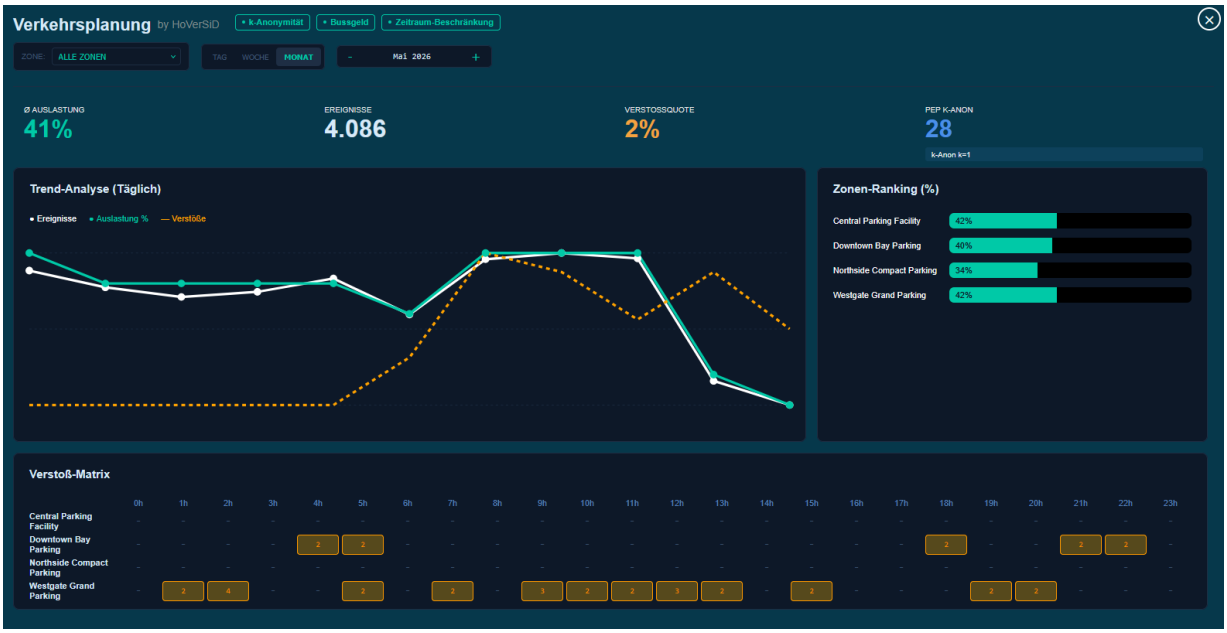
Angestrebte Ergebnisse laut Arbeitsplan: *Validierter Demonstrator und Einzelkomponenten; Erkenntnisse für den Einsatz Homomorpher Verschlüsselung auf OUPs; abgeschätzte Bedarfe für zusätzliche Rechenressourcen und daraus resultierende Mehrkosten; sichergestellte Lizenzkompatibilitäten.*

6.4.1 AP 4.1 Einrichtung der Validierungsumgebung und Definition von Test-Cases und Test-Verfahren

Im Rahmen von AP 4.1 wurde die auf der [ui!] UrbanPulse basierende HoVerSiD-Demonstrator- und Validierungsumgebung eingerichtet und so ertüchtigt, dass die im Projekt entwickelten theoretischen Konzepte nicht nur isoliert, sondern in einem anwendungsnahen Plattformkontext überprüft werden konnten. Die Umgebung war erforderlich, um die Ergebnisse aus den vorherigen Arbeitspaketen, insbesondere die HE-Kernkomponenten, den HE-Layer, das Identitäts- und Rollenmanagement sowie ergänzende Policy-Enforcement-Mechanismen, in eine zusammenhängende technische Umgebung zu überführen. Dadurch entstand eine belastbare Grundlage, um Test-Cases und Test-Verfahren nicht abstrakt, sondern anhand konkreter Smart-City-Szenarien wie der Parkraumüberwachung zu definieren. Die Demonstratorumgebung ermöglichte es, synthetische Daten, Rollenmodelle und verschiedene fachliche Perspektiven auf dieselben Daten innerhalb einer realitätsnahen UrbanPulse-Instanz zusammenzuführen. Damit konnte überprüft werden, ob die theoretisch konzipierten Sicherheits-, Datenschutz- und Zugriffskonzepte im Zusammenspiel der Komponenten grundsätzlich tragfähig sind und ob sie sich für eine spätere Nutzung in offenen urbanen Datenplattformen eignen. In der Konzeption und Umsetzung des Demonstrators wurde sich an dem Use Case 2 der Parkraumüberwachung orientiert. Ziel war es den Use Case auf seine technische Readiness aber auch seine praktische Anwendung zu testen. Der Demonstrator unterstützte die Validierung, indem er unterschiedliche Rollenperspektiven sichtbar machte. Im Admin-Bereich können Policy-Management und Rollen-/Identitätsaspekte betrachtet werden. In der Admin-Perspektive sieht man demnach vor allem Verwaltungs- und Konfigurationsfunktionen wie Policy-Verwaltung, Rollen-/Nutzerverwaltung über Keycloak und API-bezogene Management-Funktionen. Dem Admin ist es in erster Linie möglich Policies zu definieren als auch in Bezug auf die anderen Rollen des Demonstrators ein- und auszuschalten.

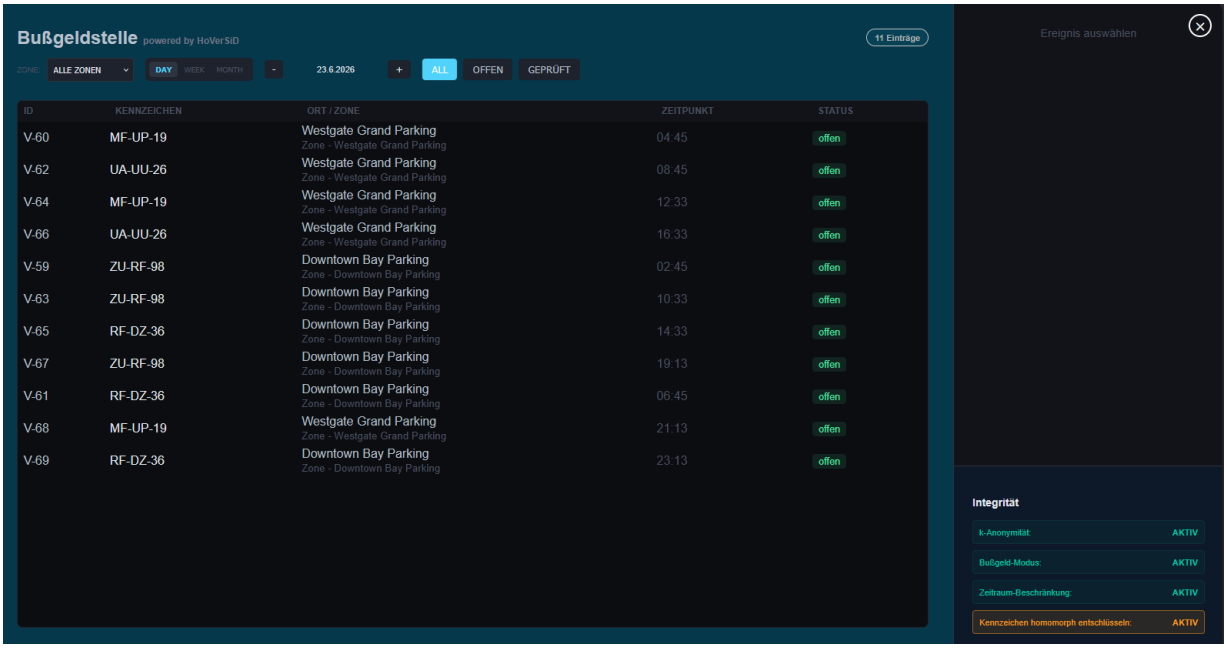


Das Verkehrsplanungs-Dashboard zeigt aggregierte Analysen der Verkehrskamera als auch des Parkscheinautomaten für die Planungsrolle. Hierbei werden die Daten der Parkraumüberwachung genutzt, um klassische Verkehrsanalysen durchzuführen, wie beispielsweise Häufigkeit von Falschparkenden, die Belegungsdauer und Belegungszeiten. Um die Datensicherheit der Parkenden weiter zu erhöhen, wurde neben der Policy der Kennzeichenunterdrückung eine Policy zur k-Anonymität hinzugefügt. Diese besagt, dass Analysen die <3 Fahrzeuge als Datenpunkte nutzen vom System unterdrückt werden sollen, um die Ergebnisse nicht auf einzelne Fahrzeuge zurückzuführen.



Das Bußgeld-Dashboard ist für die Fallbearbeitung vorgesehen. Sie enthält eine Falltabelle, Filter nach Zeitraum, Zone und Bearbeitungsstatus, ein Detail-Panel mit Ereignisdaten, sowie Bearbeitungsbuttons. Kennzeichen der Parksünder sind hierbei zunächst durch das Policy Enforcement unterdrückt und nicht einsehbar. Wird diese Policy ausgeschaltet sind die Kennzeichen letztlich zusätzlich homomorph verschlüsselt. Für den Bußgeld-Nutzer ist eine

spezielle Funktion zum „homomorphen Entschlüsseln“ bzw. decodieren der Nummernschilder vorhanden, um die Daten an der Stelle der Fallbearbeitung zu entschlüsseln. Um die Einsicht der Daten vor unbefugtem Zugriff weiter zu schützen, wurde darüber hinaus eine Policy entwickelt, welche es nur erlaubt Verstöße der letzten drei Tage ein zusehen. Sollte eine historische Inspektion der Kennzeichen notwendig sein, beispielsweise durch die Kriminalpolizei kann diese Policy wir auch die anderen durch den Administrator aufgehoben werden.



[ui!] verantwortete Konzeption und vollständige Umsetzung der Validierungsumgebung. Auf Basis der Messungen konnte gezeigt werden, dass HE-basierte Verfahren im Vergleich zu unverschlüsselten Prozessen einen erhöhten Ressourcenbedarf verursachen. **Fraunhofer FOKUS** definierte die Testverfahren mit den zugehörigen Testfällen und -daten mit Fokus auf der Korrektheit der spezifizierten Funktionalität sowie auf Performanz- und Lasttests.

6.4.2 AP 4.2 Anwendung der Test-Cases und Test-Verfahren unter Nutzung der Validierungsumgebung

Die Test-Cases und Test-Verfahren wurden systematisch angewendet und ausgewertet und belegen die Funktionsfähigkeit der Lösung. Für den Wohnberechtigungsschein lag die DGK-Server-Side-Berechnung bei nicht-trivialen Vergleichen im Schnitt bei etwa 300 ms; die clientseitige Schlüsselgenerierung erwies sich als rechenintensiver und in der Dauer stark schwankend. Für die Parkraumüberwachung wurden rund 23 Sekunden Verarbeitung auf der Plattform und etwa 5,5 Sekunden Weiterverarbeitung bei der Behörde gemessen, also rund 28 Sekunden pro Bild. Das Verarbeitungswachstum verhielt sich bei steigender Zahl von Aufrufen und Tickets linear, womit der Ansatz skalierbar und für Szenarien ohne harte Echtzeitanforderung einsatzfähig ist. Die Kennzeichenerkennung mittels CNN erreichte eine Genauigkeit von 93 Prozent, die durch die homomorphe Verschlüsselung der Gewichte gegenüber der unverschlüsselten Variante unverändert blieb. Die Gesamtsystemgenauigkeit lag bei 77 Prozent und stieg bei bereinigter Datengrundlage auf rund 84 Prozent.

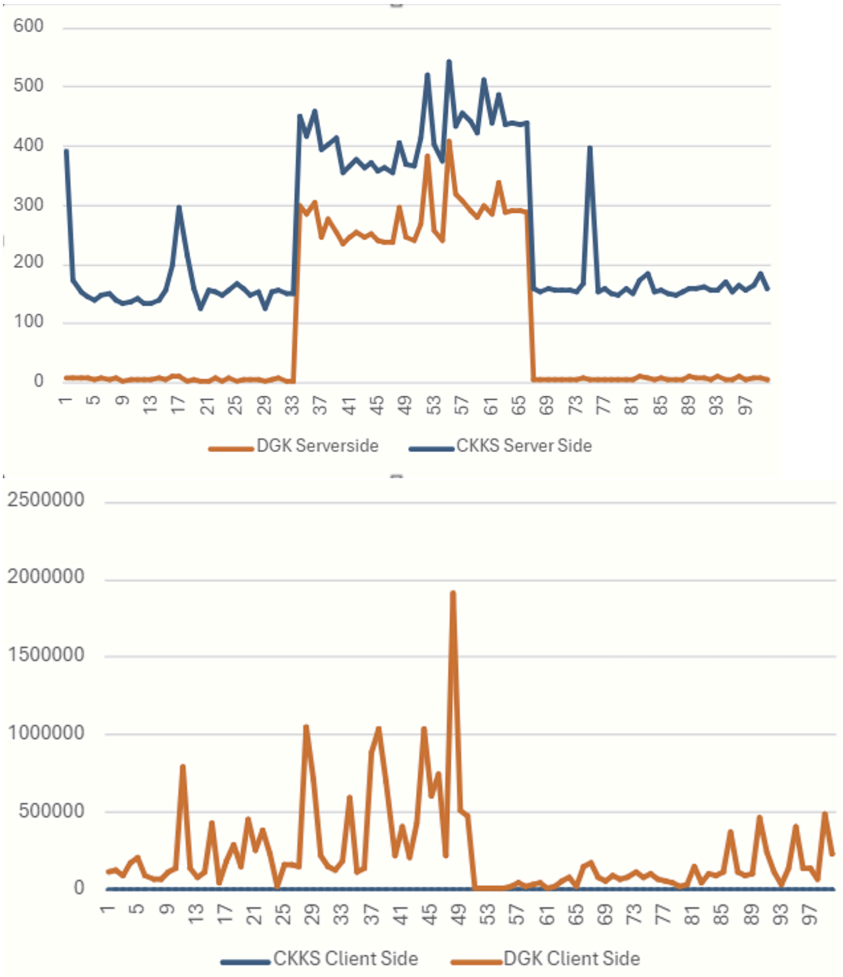


Abbildung 4: Performanzmessungen Wohnberechtigungsschein. DGK- und CKKS-Berechnungszeiten server- und clientseitig; die clientseitige Schlüsselgenerierung schwankt stark.

TABLE II
RESULTS OF THE ACCURACY EVALUATION.

Metric	**Value**
CNN accuracy, unencrypted weights	93%
CNN accuracy, encrypted weights	93%
System accuracy	77.00%
System accuracy, cleaned data	84,27%

Abbildung 5: Genauigkeitsevaluation der Kennzeichenerkennung. Die CNN-Genauigkeit bleibt mit homomorph verschlüsselten Gewichten unverändert bei 93 Prozent.

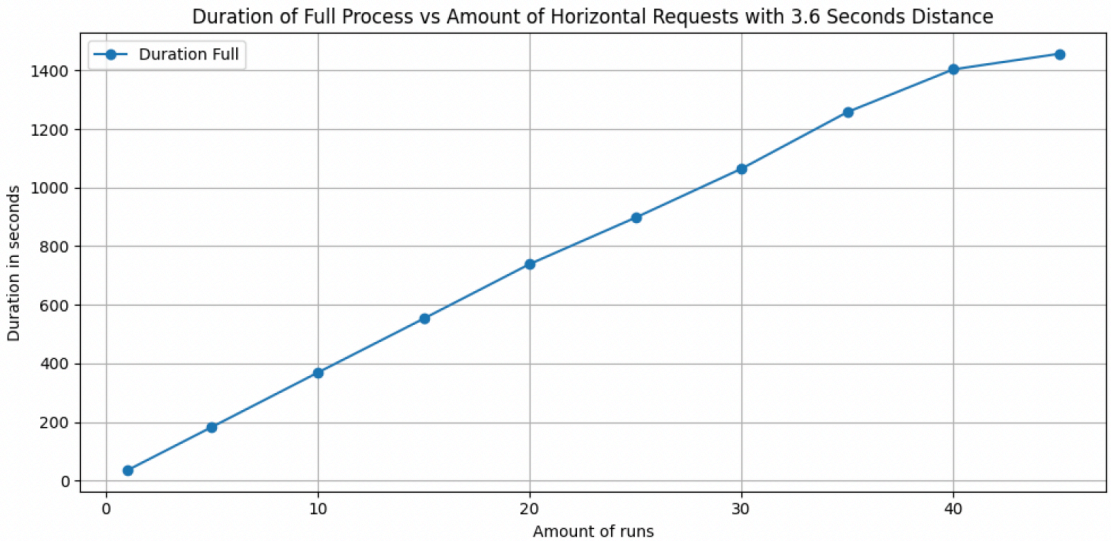


Abbildung 6: Lineares Skalierungsverhalten der Gesamtverarbeitungszeit der Parkraumüberwachung bei steigender Zahl von Anfragen.

Fraunhofer FOKUS implementierte die funktionalen sowie die Performanz- und Lasttests durch; die gewonnenen Erkenntnisse führten zu iterativen Verbesserungen der Komponenten und einer Einschätzung des Potentials von HE für die Kommunen. **[ui!]** führte die Test-Cases aus und verbesserte die Validierungsumgebung und hat Lizenzkompatibilität der Komponenten geprüft.

6.4.3 AP 4.3 Fehlerbehebung, technische Verstetigung und abschließende Validierung

Die Lösung wurde durch eine cloud-native und demonstratornahe technische Verstetigung robuster und einsatzfähiger gemacht. Eingesetzt wurden Open Policy Agent als zentrale Governance-Engine mit formal definierten, nicht hartkodierten Rego-Policies und dynamisch änderbaren Schwellwerten für die K-Anonymität, Quarkus 3.32.1 mit minimalem Ressourcen-Footprint, ein Single-Container-Deployment, Kubernetes-native Deployments mit Argo CD, Keycloak für die Enterprise-Authentifizierung, WebSockets für die unmittelbare UI-Aktualisierung, OpenSearch für eventbasierte Zeitreihendaten und H2 für Demo und Entwicklung. Die Demonstratorumgebung spielte dabei eine zentrale Rolle, weil sie nicht nur als Präsentationsoberfläche, sondern als Proof-of-Concept für das Zusammenspiel der im Projekt entwickelten Konzepte genutzt wurde. Auf Basis der Tests konnten technische Schwachstellen und Integrationsbedarfe sichtbar gemacht werden, etwa hinsichtlich der Wirkung von Policy-Konfigurationen auf die unterschiedlichen Dashboards, der Konsistenz der Datenvisualisierung oder der Robustheit einzelner Komponenten. Die Umgebung unterstützte somit die iterative Verbesserung der Lösung und ermöglichte eine abschließende Bewertung, ob die theoretischen Konzepte zur Homomorphen Verschlüsselung, zu rollenbasiertem Zugriff, Policy Enforcement und datenschutzwahrender Analyse in einer UrbanPulse-basierten Plattform praktisch umgesetzt und nachvollziehbar demonstriert werden können.

Fraunhofer FOKUS hat iterativ die Komponenten anhand der Testergebnisse verbessert. Für den WBS-Anwendungsfall wurde die notwendige Zeit zur Schlüsselgenerierung und für die Parkraumüberwachung die Skalierungsmöglichkeiten untersucht. Für den zweiten Anwendungsfall hat man eine Mehrzahl an Fehler in den Trainingsdaten beim Testen festgestellt, welche dann behoben wurden, was zu einer messbaren Steigerung der Systemgenauigkeit geführt hat. Eine weitere Verbesserung bei der Parkplatzüberwachung

entstand, nachdem FOKUS synthetisch den Trainingsdatensatz erweitert hat. Die durchgeführten Maßnahmen haben zur Verbesserung der funktionalen und nichtfunktionalen Eigenschaften der Systeme geführt. **[ui!]** führte Fehlerbehebungen am Demonstrator durch und validierte den Demonstrator in Bezug auf Verstetigung und Anschlussfähigkeit.

7 Wichtigste Positionen des zahlenmäßigen Nachweises

Die mit Abstand wichtigste und größte Position ist „0837 Personalkosten“ und die damit verbundenen Fördermittel sind zu 100% abgerufen worden. Die tatsächlichen Kosten lagen geringfügig über den geplanten Kosten. Grund hierfür waren sich während der Umsetzungsphase entstandene Chancen, um ein höherwertiges Ergebnis zu erzielen und diese wurden wahrgenommen.

8 Notwendigkeit und Angemessenheit der geleisteten Arbeit

[ui!] hat das AP1 und AP4 geleitet und in allen anderen APs mitgewirkt. **Fraunhofer FOKUS** hat AP2 und AP3 geleitet und in allen anderen Aps mitgewirkt. Die erzielten Ergebnisse hätten nicht von einem Partner allein erzielt werden können, wodurch die Zusammenarbeit im Konsortium notwendig und zielgerichtet war. Die zukunftsträchtige Themenfeld der IT-Sicherheit birgt ebenfalls hohe Risiken bezüglich der wirtschaftlichen Verwertung, dessen Abschätzungen zwar vorläufig, aber noch nicht final bewertet werden konnten. Alle Arbeiten wurden gemäß Zeit- und Arbeitsplan durchgeführt und die angestrebten Ziele und Ergebnisse erreicht.

9 Voraussichtlicher Nutzen

Projektergebnis/ Inhalt	**Nutzen/ Verwertung**
HE-fähige Erweiterung der [ui!] UrbanPulse (HE-Layer, HE-fähige Konnektoren, HE-Kernkomponenten mit CKKS und DGK)	**Verwertungspotenzial:** Die [ui!] UrbanPulse ist nun vorbereitet für die Verarbeitung homomorph verschlüsselter Daten und schützt sensible Daten auch im Public-Cloud-Betrieb vor unbefugter Einsicht, etwa durch fremde Rechtsräume nach dem CLOUD Act. **Marktpotenzial:** Erhöhte Sicherheitsstandards als Alleinstellungsmerkmal gegenüber Wettbewerbern und Grundlage für die Gewinnung neuer Kunden unter Kommunen und kommunalen Unternehmen.
Privatsphäreerhaltende Parkraumüberwachung (Use Case 2)	**Verwertungspotenzial:** Prototypisch umgesetzter, DSGVO-konformer Ordnungswidrigkeitenprozess mit homomorph verschlüsselter Kennzeichenverarbeitung; Kennzeichen mit gültigem Ticket werden zu keinem Zeitpunkt entschlüsselbar.

	Marktpotenzial: Schnellere und häufigere Erfassung von Falschparkenden, dadurch höhere Gebühreneinnahmen für Kommunen; auf weitere kommunale Anwendungsfälle übertragbar.
Digitaler Wohnberechtigungsschein mit HE (Use Case 1)	**Verwertungspotenzial:** Nachgewiesene Eignung der HE für digitale Verwaltungsleistungen mit Einkommensprüfung (DGK für sichere Vergleiche, CKKS für Berechnungen) bei vollem Schutz personenbezogener Daten. **Marktpotenzial:** Blaupause für die datenschutzkonforme Digitalisierung weiterer Verwaltungsverfahren.
Policy Enforcement als zusätzlicher Sicherheitslayer (Open Policy Agent)	**Verwertungspotenzial:** Ermöglicht die kontrollierte Weiternutzung HE-geschützter Daten über den unmittelbaren Anwendungsfall hinaus, etwa für die Verkehrsplanung, unter Wahrung der K-Anonymität. **Marktpotenzial:** Unmittelbar produktisierbar und bei Bestandskunden etablierbar; deutlicher Mehrwert für hoheitliche Aufgaben und Entscheidungen.
IAM- und Key-Management-Konzept für HE	**Verwertungspotenzial:** Regelt rollen- und policybasiert, welche Stellen HE-Ergebnisse entschlüsseln dürfen, und sichert die durchgängige Nachvollziehbarkeit. **Marktpotenzial:** Wiederverwendbarer Baustein für sichere kommunale Plattformlösungen.
HoVerSiD-Demonstrator	**Verwertungspotenzial:** Lauffähiger Proof of Concept auf Basis der DIN SPEC 91357, der die Machbarkeit für den Verwaltungsalltag belegt. **Marktpotenzial:** Grundlage für Pilotprojekte und den Transfer in produktreife, einsatzfähige Lösungen.
Konzept für privatsphäreerhaltende Origin-Destination-Analysen und HE-Testprotokoll	**Verwertungspotenzial:** Technisches Konzept, Datensatz und Werkzeugansatz für verschlüsselte Bewegungsanalysen; aus den Erkenntnissen ging das wissenschaftlich verwertete Verfahren der strukturellen Testbarkeit unter Homomorpher Verschlüsselung hervor. **Marktpotenzial:** Anschlussforschung und Stärkung der wissenschaftlichen Positionierung beider Partner.
Wissenschaftliche Publikationen und Nachwuchsförderung	**Verwertungspotenzial:** Mehrere wissenschaftliche Beiträge und eine betreute Masterarbeit erweitern das Portfolio und fördern den Wissenstransfer. **Marktpotenzial:** Erhöhte Sichtbarkeit und Akquise von Folgeprojekten und Industriekooperationen.

9.1 [ui!]

Die [ui!] erweitert ihr Portfolio um belastbare Erkenntnisse und Technologiebausteine zur Homomorphen Verschlüsselung und hat die technische Readiness der [ui!] UrbanPulse für

deren Einsatz deutlich vorangetrieben. Besonderes Verwertungspotenzial bietet das Policy Enforcement, das die Nutzung bislang ausgeschlossener Daten in weiterführenden Analysen ermöglicht und im Anschluss an das Projekt produktisiert werden kann. [ui!] strebt an, die Ergebnisse bis zur robusten, einsatzfähigen Reife zu verstetigen, Adapter für weitere Datenbanken und Dienste zu ergänzen und die Lösung durch einen unabhängigen Dritten prüfen und möglichst zertifizieren zu lassen. Daraus entsteht unmittelbarer wirtschaftlicher Nutzen, da der kostenintensive Hybrid-Cloud-Betrieb entfallen kann und zugleich die Sicherheit der Plattform steigt. Der Vertrieb erfolgt zusätzlich über den Smart-City-Marktplatz [ui!] AGORA. Die erhöhten Sicherheitsstandards stärken die Marktposition der UrbanPulse und begünstigen die Gewinnung neuer Kunden, darunter Kommunen, kommunale IT-Dienstleister sowie Unternehmen des Finanz- und Versicherungssektors.

9.2 FOKUS

Fraunhofer FOKUS erweitert sein wissenschaftlich-technisches Portfolio um Methoden, Techniken und Werkzeuge für Homomorphe Verschlüsselung und privatsphäreerhaltende Datenanalysen. Im Rahmen von HoVerSiD wurden die im Verwertungsplan angestrebten Ziele erreicht. Es wurden wissenschaftliche Beiträge veröffentlicht und der wissenschaftliche Nachwuchs durch betreute Masterarbeiten gefördert. FOKUS festigt damit seine Stellung als wissenschaftlicher Partner für privatsphäreerhaltende Datenanalysen und schafft die Grundlage für die Akquise weiterer Forschungs- und Entwicklungsprojekte sowie für direkte Kooperationen mit der Industrie. Die enge Anbindung an die Berliner Universitäten unterstützt den nachhaltigen Wissenstransfer.

10 Bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Die Forschungsarbeiten in HoVerSiD erfolgten in einem ausgesprochen dynamischen Feld. Während der gesamten Projektlaufzeit wurden die externen wissenschaftlichen und technischen Entwicklungen kontinuierlich beobachtet.

Die Forschung zur homomorphen Verschlüsselung konzentriert sich derzeit stark auf Performanzverbesserungen, insbesondere auf die Reduktion des durch Bootstrapping verursachten Rechenaufwands, häufig im Kontext der ML-Inferenz. Beispielhafte Arbeiten sind:

- Zhang, Chuan; Hu, Chenfei; Wu, Tong; Zhu, Liehuang; Liu, Ximeng: *Achieving Efficient and Privacy-Preserving Neural Network Training and Prediction in Cloud Environments.* IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 5, pp. 4245-4257, 1 Sept.-Oct. 2023
- Pang, Qi; Zhu, Jinhao; Möllering, Helen; Zheng, Wenting; Schneider, Thomas: *BOLT: Privacy-Preserving, Accurate and Efficient Inference for Transformers.* 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2024, pp. 4753-4771
- Kim, Dongwoo; Guyot, Cyril: *Optimized Privacy-Preserving CNN Inference With Fully Homomorphic Encryption.* IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2175-2187, 2023
- Fan, Shengyu; Wang, Zhiwei; Xu, Weizhi; Hou, Rui; Meng, Dan; Zhang, Mingzhe: *TensorFHE: Achieving Practical Computation on Encrypted Data Using GPGPU.* 2023 IEEE International Symposium on High-Performance Computer Architecture (HPCA), Montreal, QC, Canada, 2023, pp. 922-934

Die Ergebnisse dieser Arbeiten sind häufig performante Forschungsprototypen. Diese weisen jedoch (sofern sie überhaupt zugänglich sind) Defizite hinsichtlich Verlässlichkeit und Wartbarkeit im Vergleich zu etablierten Bibliotheken auf, was ihre Integration erheblich erschwert. Daher wurde entschieden, im Rahmen des Projekts maximal auf bestehende Bibliotheken zurückzugreifen.

Die Projektteilnehmer wurden im Kontext der OD-Analysen zudem auf folgende Arbeiten aufmerksam:

- Koll, Charles; Hang, Preston Tan; Rosulek, Mike; Abbas, Houssam: *Monitoring in the Dark: Privacy-Preserving Runtime Verification of Cyber-Physical Systems.* arXiv preprint arXiv:2505.16059 (2025).
- Heinzinger, Thomas A.; Karimi, Mahyar; Thejaswini, K.S.: *Privacy-Preserving Runtime Verification.* Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25). Association for Computing Machinery, New York, NY, USA, 2774–2787.
- Waga, Masaki; Matsuoka, Kotaro; Suwa, Takashi; Matsumoto, Naoki; Banno, Ryotaro; Bian, Song; Suenaga, Kohei: *Oblivious Monitoring for Discrete-Time STL via Fully Homomorphic Encryption.* Runtime Verification. RV 2024. Lecture Notes in Computer Science, vol 15191. Springer, Cham.

Obwohl der Anwendungskontext dieser Arbeiten im Monitoring liegt, werden Verkehrsdaten in einem Format verarbeitet, das dem in diesen Arbeiten diskutierten, entspricht. Die darin vorgestellten Ansätze wurden bei der Konzeption des dritten Use-Cases in hohem Maße berücksichtigt.

Im Unterschied zu Arbeiten, die sich ausschließlich der homomorphen Verschlüsselung widmen, fokussierte sich das HoVerSiD-Konsortium auf eine DIN-SPEC-91357-konforme Offene Urbane Datenplattform sowie auf konkrete Verwaltungs-Use-Cases. Dabei zeigte sich, dass auf thematisch einschlägigen Konferenzen (IEEE ISC2, IET SCS, ACM BuildSys) und in relevanten Zeitschriften (IET Smart Cities, Smart Cities, Urban Informatics) lediglich nur eine weitere Arbeit zur homomorphen Verschlüsselung erschienen ist:

- Sasaki, Yusuke; Segawa, Tomoka; Michikata, Takashi; Koshizuka, Noboru: *Architecture for Privacy-Preserving Greenhouse Gas Emissions Calculation Among Multiple Organizations Using Homomorphic Encryption.* 2023 IEEE International Smart Cities Conference (ISC2), Bucharest, Romania, 2023, pp. 01-07

Die Projektpartner verfolgten mit Interesse die Entwicklung der Norm ISO/IEC DIS 28033-1 „Information Security – Fully Homomorphic Encryption“. Da die Norm jedoch während der Projektlaufzeit nicht in finaler Fassung erschienen ist, wurde sie im Projekt nicht genau berücksichtigt.

11 Erfolgte oder geplanten Veröffentlichungen des Ergebnisses

Im Rahmen von HoVerSiD wurden die folgenden wissenschaftlichen Beiträge erarbeitet und veröffentlicht:

Barlage, Katharina; Aleksandrov, Andrei; Lämmel, Philipp: *Privacy-Preserving Parking Lot Surveillance Utilizing Homomorphic Encryption.* 2025 IEEE International Smart Cities Conference (ISC2). IEEE, 2025.

Darius, Paul; Lämmel, Philipp; Tcholtchev, Nikolay: *Quantization and Pruning Under FHE Constraints: Enabling Encrypted Anomaly Detection in Smart City IoT.* 2025 IEEE International Smart Cities Conference (ISC2). IEEE, 2025.

Aleksandrov, Andrei: *Structural Testing with Homomorphic Encryption.* 2026 International Conference on Relational and Algebraic Methods in Computer Science. Springer, 2026.

Darius, Paul; Lämmel, Philipp; Tcholtchev, Nikolay: *Topology-aware quantization and pruning for FHE-based anomaly detection in smart city IoT*. Internet of Things, 38, 101981. Elsevier, 2026.

Darüber hinaus wurde im Rahmen des Vorhabens zwei Masterarbeiten betreut und damit der wissenschaftliche Nachwuchs gefördert:

Darius, Paul: *Privatsphäre-erhaltende Anomalieerkennung vo IoT Traffic mithilfe von homomorpher Verschlüsselung.* Technische Universität Berlin, 2026.

Barlage, Katharina: *Konzeption, Entwicklung und Evaluation einer Privatsphäre erhaltenden automatisierten Parkraumüberwachung.* Humboldt-Universität zu Berlin, 2025.