# SECURE

Secure Encryption Key Utilization and Reliable Exchange

| | | | |
|---|---|---|---|
| **Programm / Ausschreibung** | IWI, IWI, Basisprogramm Ausschreibung 2023 | **Status** | abgeschlossen |
| **Projektstart** | 01.01.2024 | **Projektende** | 30.09.2025 |
| **Zeitraum** | 2024 - 2025 | **Projektlaufzeit** | 21 Monate |
| **Keywords** | | | |

## Projektbeschreibung

fiskaly ist eine sehr forschungsorientierte Firma, die sich im Bereich der Cloud-Lösung zur Fiskalisierung auch international einen Namen gemacht hat. Basierend auf den Forschungsprojekten der Vorjahre soll nun das Kernstück, nämlich der Cryptographic Service Provider (CSP) für weitere, innovative Services wie z.B. bei E-IDs oder im E-Health-Bereich weiterentwickelt werden.
Die angestrebten verteilten CSPs müssen eine Vielzahl von Schlüsseln verwalten, die hochverfügbar vorgehalten werden müssen. Ebenso sind die Vorgänge stateful, sodass Logs über einen längeren Zeitraum vorgehalten werden müssen. Da Redundanz der Schlüssel und Logs aufgrund der Sicherheitsanforderungen keine Option ist, müssen Methoden und Prozesse entwickelt werden, um in einem Cloud-Szenario eine hohe Verfügbarkeit und Robustheit zu gewährleisten.
Die Entwicklung verteilter CSPs für den Einsatz in Cloud-Umgebungen unter Berücksichtigung der Sicherheitsanforderungen an solche kritischen Sicherheitsanker, steht also vor einer Vielzahl von Herausforderungen hinsichtlich Stabilität, Robustheit und Verfügbarkeit in verteilten Systemen, die in diesem mehrjährigen Forschungsprojekt gelöst werden sollen.
Ziel ist somit, eine Plattform und Services zu entwickeln, die den weit verbreiteten HSMs in Security-Fragen ebenbürtig ist, aber wesentlich performanter und mit mehr Funktionalitäten ausgestattet sein soll.

## Endberichtkurzfassung

Erfolgreiche Ermittlung, Anschaffung und Erprobung einer geeigneten Hardware-Plattform, die die notwendigen Sicherhheits- und Performanzkriterien erfüllt
Erfolgreiche prototypische Entwicklung und Erprobung eines CSPL-Clusters mit hybridem Replikationsansatz mit mehreren Slave-Instanzen
Optimierung der Performanz für das Critical Path des CSPL bei minimalem Datenverlust im Ausnahmefall eines katastrophalen Ausfalls der Master-Instanz
Leistung des Prototyps in Lasttests übertrifft beobachtete Last in existierenden Instanzen, daher Skalierbarkeit und

Performanz auch bei größeren Profuktionslasten erwartet, Ansatz bzw. Hardware-Plattform muss sich aber auch in der Praxis bewähren

Durch Einschränkungen aus Abstimmungen mit dem BSI konnte kein automatisierter Cluster-Management bzw. Failover-Prozess entwickelt werden. Die Master-Instanz ist für die Diagnose des Zustands der Slave-Instanzen zuständig und ein menschlicher Administrator für administrative Eingriffe. Ein (im Idealfall auch zertifizierbarer) automatisierter Prozess wäre Gegenstand weiterer Forschung.

Aktuelle Architektur und Prototyp sehen Implementierung im Rahmen desselben Rechenzentrums vor. Verteilung über mehrere Rechenzentren wäre Gegenstand weiterer Forschung.

## Projektpartner

- fiskaly gmbh