LISA-MKD

Entwicklung einer rollenbasierten Lösung für eine beweisbar 100%ige Datensicherheit für Dateien und Datenbanken auf PCs

Programm / Ausschreibung	IWI 24/26, IWI 24/26, Basisprogramm Ausschreibung 2026	**Status**	laufend
Projektstart	01.01.2026	**Projektende**	30.09.2026
Zeitraum	2026 - 2026	**Projektlaufzeit**	9 Monate
Keywords			

Projektbeschreibung

LISA: In offenen IT-Arbeitsplätzen (PCs, Laptops etc.), IoT-Geräten, Maschinen etc., wo Anwendungen inklusive einer gemeinsamen Datenbasis über mehrere Arbeitsplätze bzw. einer Zentrale verarbeitet werden, können ein logisches Zugriffsberechtigungssystem und eine Berechtigungsverwaltung, wie in einem Hostumfeld üblich, aus Sicherheitsgründen nicht eingesetzt werden. Doch der Stand der Technik, insbesondere das heutige Lösungsangebot am Markt, liefert dazu keine ausreichend geeignete Lösungen für eine komplexere Berechtigungsverwaltung und feingliedrigen Zugriffskontrolle, wie im Hostumfeld bei Datenbanken bzw. Dateien üblich.
Die Ergebnisse des Projekts LISA liefern erstmalig eine komplette Lösung für eine ausreichend sichere Dezentralisierung. Dabei werden die Anwendungen direkt am IT-Arbeitsplatz des Benutzers (Berechtigten) verarbeitet und die Daten sofort nach der Verarbeitung noch am IT-Arbeitsplatz feingliedrig bei Datenbanken (bis auf einzelne Datenelemente) und Dateien rollenbasierend mit dem mathematischen Verfahren AES-256 verschlüsselt. LISA enthält dazu ein neuartiges kryptografisches Zugriffskontrollsystem und Schlüsselmanagement sowie eine sichere, kryptografische Berechtigungsverwaltung.

LISA-MKD: Sehr hohe Datensicherheit ist für Behörden, bei medizinischen Daten, Unternehmensdaten wie Forschungsdaten, strategischen Daten, Angeboten etc. sehr wichtig. Doch die Sicherheitsbeurteilungen der mathematischen Kryptografie bauen auf Vermutungen auf und können noch nicht veröffentlichte Angriffsmethoden nicht berücksichtigen. Dies führte zur physikalischen Kryptografie und den verstärkten Einsatz des One-Time Pads mit einer beweisbar 100%igen Sicherheit. Dabei ist heute QKD (Quantum Key Distribution) der große Treiber. Doch QKD ist extrem teuer (über € 100.000 pro Endgerät) und kann nur an festen Standorten verwendet werden und ist daher im Umfeld von Laptops etc. praktisch nicht verwendbar. Datensicherheit und Kryptografie müssen aber immer end-to-end betrachtet werden und da spielen eben PCs eine wichtige Rolle. Die meisten sensiblen Daten entstehen heute auf PCs und daher müssen schon dort die Daten hochsicher verschlüsselt werden.
LISA-MKD garantiert eine durchgängig beweisbar 100%ige Datensicherheit, von der Erzeugung und Verteilung der kryptografischen Schlüssel bis zur Datenverschlüsselung und MAC-Berechnung am PC. Und das Ganze vollständig integriert in die PC-Betriebssysteme um einen, mit QKD verglichen, sehr günstigen Preis. Eine beweisbar absolute (100%ige)

Sicherheit für die gesamte Telekommunikation und Datenspeicherung für Dateien und Datenbanken für PCs, Laptops, Tabletts etc. um einen in diesem Umfeld vertretbaren Preis wäre weltweit einzigartig. Außerdem handelt es sich dabei um eine europäische und österreichische Lösung, was bei der Datenverschlüsselung, wo Vertrauen eine besondere Rolle spielt, ein großes zusätzliches Plus darstellt.
LISA-MKD kann noch mit einer weiteren einzigartigen Spezialität aufwarten. In den Rollen der Berechtigungsverwaltung kann auch angegeben werden, ob im kryptografischen Zugriffskontrollsystem die Ver-/Entschlüsselung der Daten mit einem mathematischen oder mit einem physikalischen Verfahren erfolgen soll. Die mathematischen Verfahren der Kryptografie inklusive Berechtigungsverwaltung sind schon durch LISA abgedeckt.
Das heißt LISA-MKD erweitert die Dezentralisierung von LISA um die beweisbar 100%ige Datensicherheit. Und diese mit einem rollenbasierenden Berechtigungssystem und einem in die Betriebssysteme integrierten kryptografischen Zugriffskontrollsystem.

Bei Lösungen, die heute schon am Markt verfügbar sind, muss die Verschlüsselung der Daten vom Benutzer gezielt durchgeführt werden und erfolgt im Hochsicherheitsbereich meist in spezialisierten HW-Boxen und mit dem AES-256, einem mathematischen Verfahren ohne beweisbare Sicherheit. Bei LISA-MKD erfolgt eine automatische Verschlüsselung im Hintergrund. Und das Ganze basiert als Folge des Vorprojektes LISA zusätzlich auf Rollen basierend für Dateien und Datenbanken.
Eine Datenverschlüsselung mit einem One-Time Pad in diesem Umfeld erfordert spezielle Mechanismen und eine Logistik, für die im Jahr 2025 an der FH St. Pölten (heute Hochschule für Angewandte Wissenschaften St. Pölten) im FFG-KIRAS-Projekt „Kryptovergleich“ (Projektleiter Ernst Piller) schon umfangreiche Forschungstätigkeiten erfolgten und in LISA-MKD fertig gestellt und in eine praxisgerechte Softwarelösung übergeführt werden sollen.

Projektpartner

- insitu software gmbh