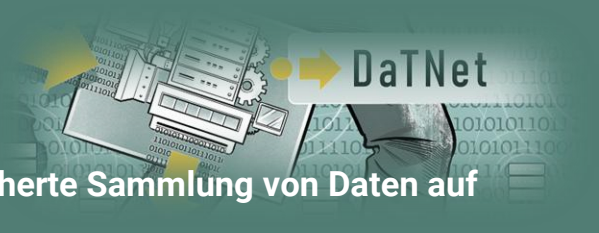
Datentreuhand Kompetenz Netzwerk DaT Net



TRESOR – eine technische Lösung für kryptografisch abgesicherte Sammlung von Daten auf mobilen Endgeräten

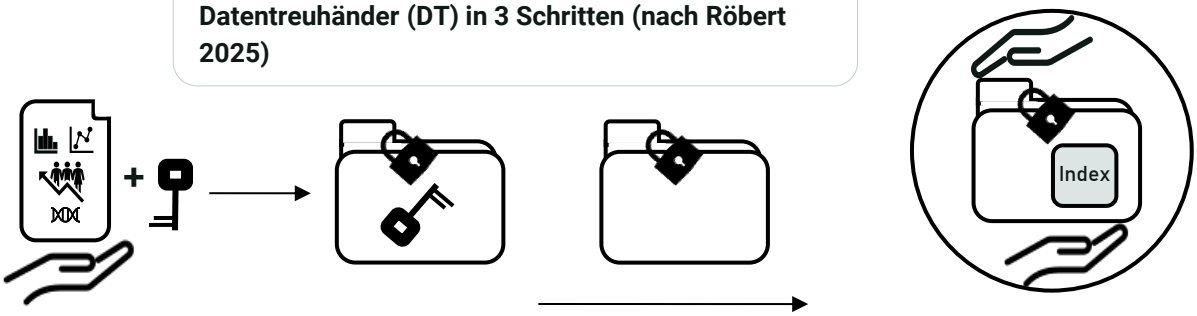
Kategorien:
Workflows: Kontrolle der Datengebenden durch granulare Freigabe
Architekturen: kryptografisch abgesicherte Infrastruktur
Tools: Data Vault App

https://tresor-projekt.de/

Dr. Lisa Eggerichs (wiss. MA, DaTNet, TU Dresden) und Kevin Röbert (wiss MA, TRESOR, Universität Hamburg)

Kurzbeschreibung des Projektes: TRESOR entwickelt u.a. technische Lösungen für die kryptographisch abgesicherte und privatsphäreschützende Sammlung, Speicherung und Vermittlung von auf mobilen Geräten erhobenen Daten. Durch eine Data Vault App können Datengebende (DG) ihre Daten gezielt an authentifizierte Datennutzende (DN) freigeben.

Datenübertragung vom Datengebenden (DG) hin zum Datentreuhänder (DT) in 3 Schritten (nach Röbert 2025)



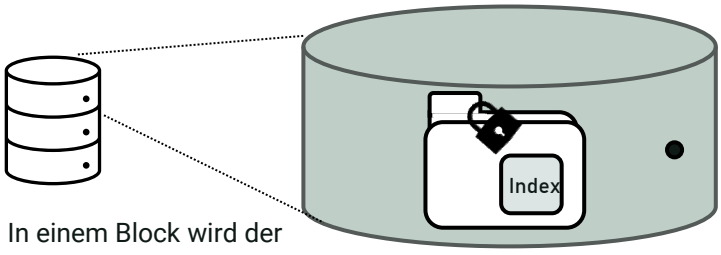
1) DG generiert und speichert einen zufälligen Schlüssel (symmetrischer Schlüssel, z.B. AES-256), der zur Verschlüsselung der Klartextdaten dient. Nur DG kann die Entschlüsselung vornehmen.

2) DG sendet verschlüsselten Block an DT.

3) DT speichert die verschlüsselten Daten unter einer Referenz-ID. Der Index (I) dafür wird gleichverteilt zufällig gewählt. DT erhält damit keinen Zugang zum Klartext.

Datenverwaltung beim Datentreuhänder (nach Röbert et al. 2025)

Die Datenbank besteht aus n verschlüsselten Blöcken. Jeder Block hat eine Standardgröße von 128 Bit. Große Datensätze werden auf mehrere Blöcke aufgeteilt, um zu verhindern, dass der DT Rückschlüsse auf die Daten anhand der Größe der Blöcke ziehen kann.



In einem Block wird der verschlüsselte Datensatz und der zugehörige Index gespeichert.

Literatur

Röbert, Kevin, Dominik Kaaser, and Mathias Fischer. 2025. "Unlinkable Data Sharing with Dynamic Access Control." In Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing (SAC), Catania, Italy, March 2025.

Gefördert durch:
Bundesministerium für Forschung, Technologie und Raumfahrt
Finanziert von der Europäischen Union NextGenerationEU
TECHNISCHE UNIVERSITÄT DARMSTADT
TECHNISCHE UNIVERSITÄT DRESDEN
RWTH AACHEN UNIVERSITY
Universität Marburg

Datentreuhand Kompetenz Netzwerk DaTNet

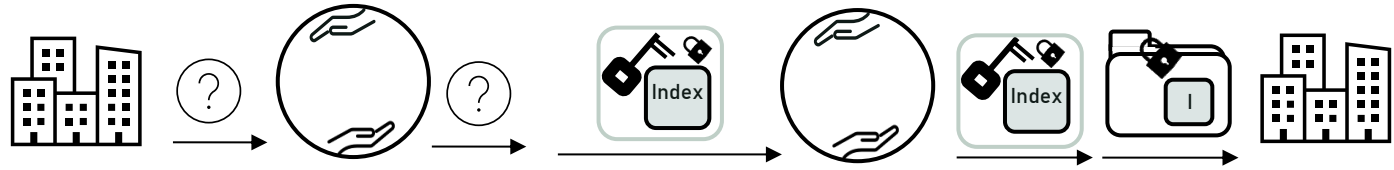
TRESOR – eine technische Lösung für kryptografisch abgesicherte Sammlung von Daten auf mobilen Endgeräten

Kategorien:
Workflows: Kontrolle der Datengebenden durch granulare Freigabe
Architekturen: kryptografisch abgesicherte Infrastruktur
Tools: Data Vault App

https://tresor-projekt.de/

Dr. Lisa Eggerichs (wiss. MA, DaTNet, TU Dresden) und Kevin Röbert (wiss MA, TRESOR, Universität Hamburg)

Datenbereitstellung an den Datennutzenden (DN)



1) Daten liegen beim DG bereits vor Anfrage durch einen DT in verschlüsselter Form vor (Data Vault App)

2) DT identifiziert zur Anfrage des DN geeignete DG mit Hilfe von Privatsphäre-wahrenden Lokalisierungstechniken

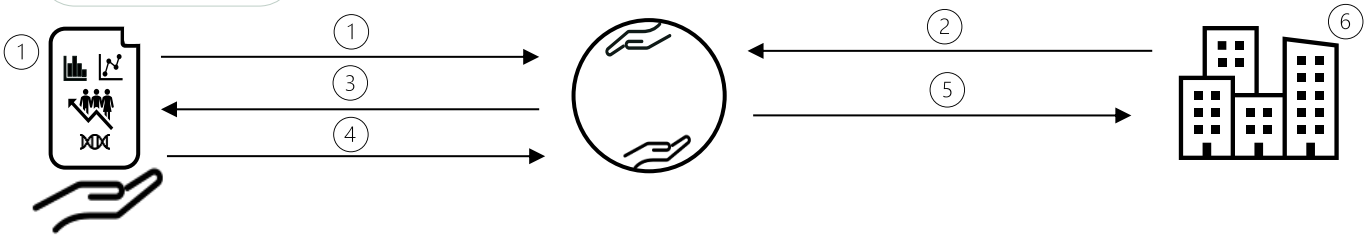
3) DG verschlüsselt das Schlüssel-Index-Paar und sendet Index und Schlüssel an DT

4) DT leitet das verschlüsselte Schlüssel-Index-Paar weiter an DN. DN erfragt den verschlüsselten Datenblock beim DT und entschlüsselt den Klartext.

Privatsphäre-wahrende Lokalisierungs-techniken (nach Röbert 2025)

Dieser Mechanismus schützt die Privatsphäre des DG, indem

- seine echten Interessenslagen in einer größeren Gruppe (Anonymitätsmenge) versteckt sind und
- der DT keine Rückschlüsse auf die Identität der echten Kategorien ziehen kann. Umgesetzt wurde dies mit Hilfe von Differential Privacy.



1) Differential Privacy: DG bildet eine Anonymitätsmenge aus verschiedenen Themen, in dem er eine Menge von Themen erstellt, in die das echte Thema eingebettet ist (Verrauschen) und sendet diese zum DT.

2) DN stellt eine Anfrage für ein bestimmtes Thema an DT. 3) DT leitet die Anfrage die DG weiter, in deren Anonymitätsmenge das angefragte Thema vorhanden ist. 4) Alle DG, die das angefragte Thema in ihrer Anonymitätsmenge haben, antworten. 5) DT leitet die Antworten weiter. 6) Der DN erhält nun verschiedene Antworten zum angefragten Thema ohne diese zum DG konkret zuordnen zu können.

Literatur

Röbert, Kevin, Dominik Kaaser, and Mathias Fischer. 2025. “Unlinkable Data Sharing with Dynamic Access Control.” In Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing (SAC), Catania, Italy, March 2025.

Gefördert durch: Bundesministerium für Forschung, Technologie und Raumfahrt
Finanziert von der Europäischen Union NextGenerationEU
TECHNISCHE UNIVERSITÄT DARMSTADT
TECHNISCHE UNIVERSITÄT DRESDEN
RWTH AACHEN UNIVERSITY
Universität Marburg