DaTreFo – Datentreuhänder mit geschützten Datenschätzen für die Forschung

Nationale Konferenz IT-Sicherheitsforschung

Berlin, 18. März 2025

Konstantin Knorr

Hochschule Trier

Informatik
Hauptcampus

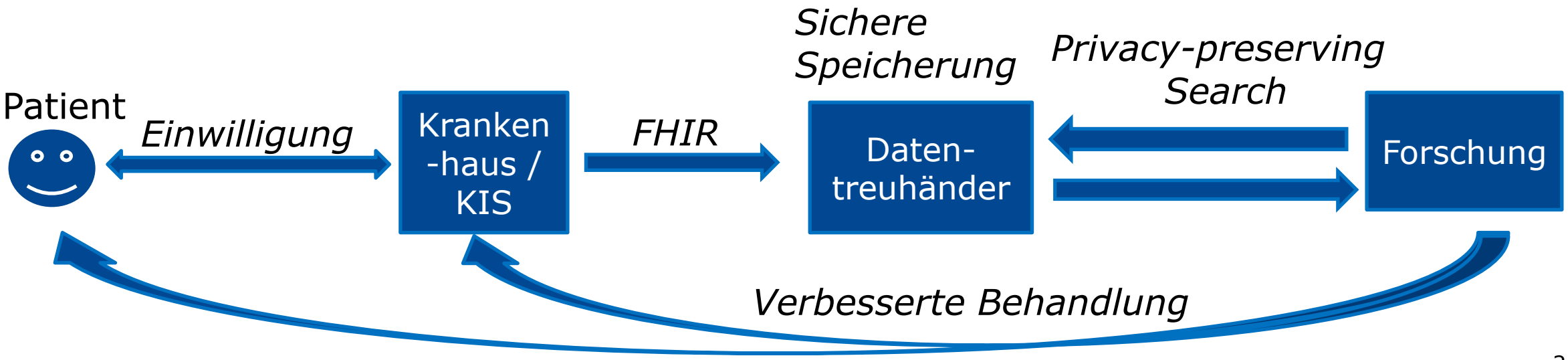
HOCHSCHULE TRIER

DaTreFo: Projektübersicht und Motivation

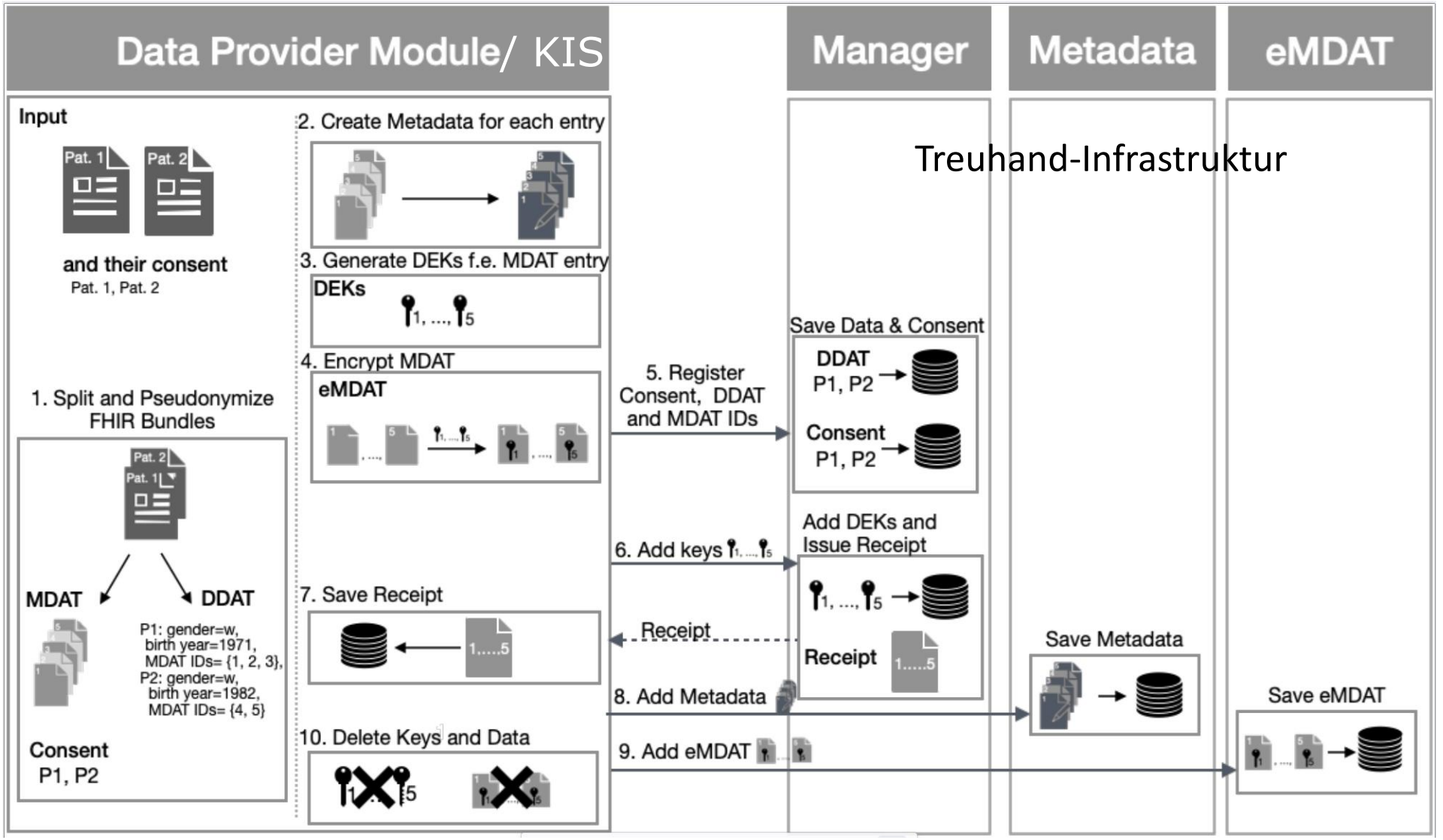
- Laufzeit: 2022-2025
- BMBF-Verbundprojekt mit folgenden Partnern:
  - Hochschule Trier
  - Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI)
  - Dedalus HealthCare GmbH
  - Gematik und Duria eG (beratend)

DaTreFo
Datentreuhänder mit geschützten Datenschätzen für die Forschung

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung



Upload der Daten aus dem KIS in die Treuhand-Infrastruktur nach [1]

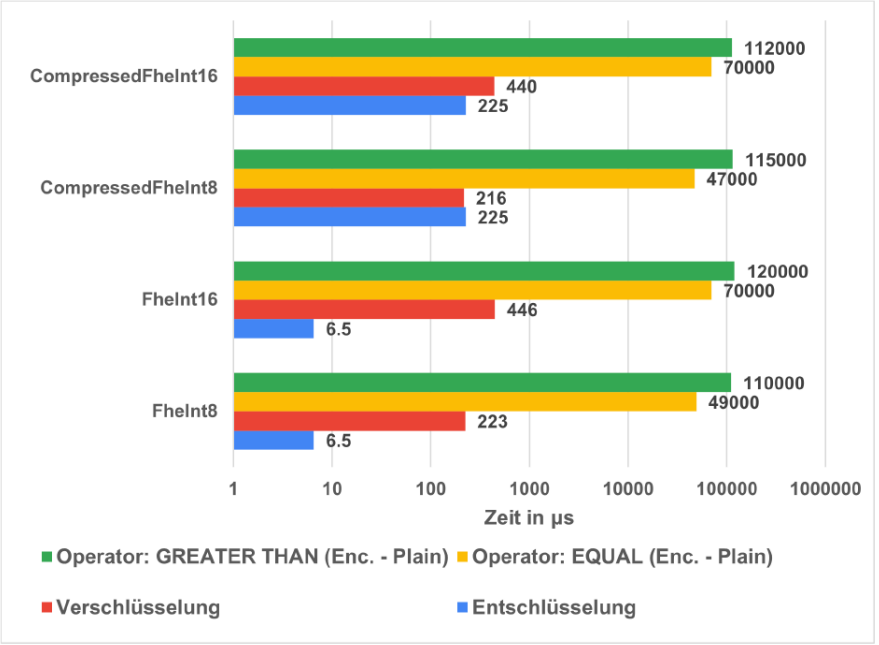


[1] Carolin Poschen, Britta Herres, and Konstantin Knorr. "A Threat-Driven Design of a Data-Trustee Infrastructure for Medical Data". 2024 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), Lisbon, Portugal, (2024)

Homomorphe Suche als Alternative

- Erstellung eines Prototyps auf Basis des TFHE-Verfahrens [2]
- Tests mit synthetischem Datensatz im FHIR-Format, bestehend aus 1.000 gebündelten Patientendatensätzen
- (Einfache) Suche in verschlüsselten Daten mittels =, <>, <,>,<=, >= in Kombination mit UND- und ODER-Verknüpfungen möglich
- Verwendete Implementierung: Rust, https://github.com/zama-ai/tfhe-rs
- Speicherplatzbedarf: Server Key 110 MB bzw. 24 MB komprimiert pro Ressource
- Berechnungszeiten:
  - Schlüsselgenerierung: ~ 1 s
  - Ver- und Entschlüsselung: ~ 1 ms pro Datensatz
  - Homomorphe Suche: ~ 1 s je Suche

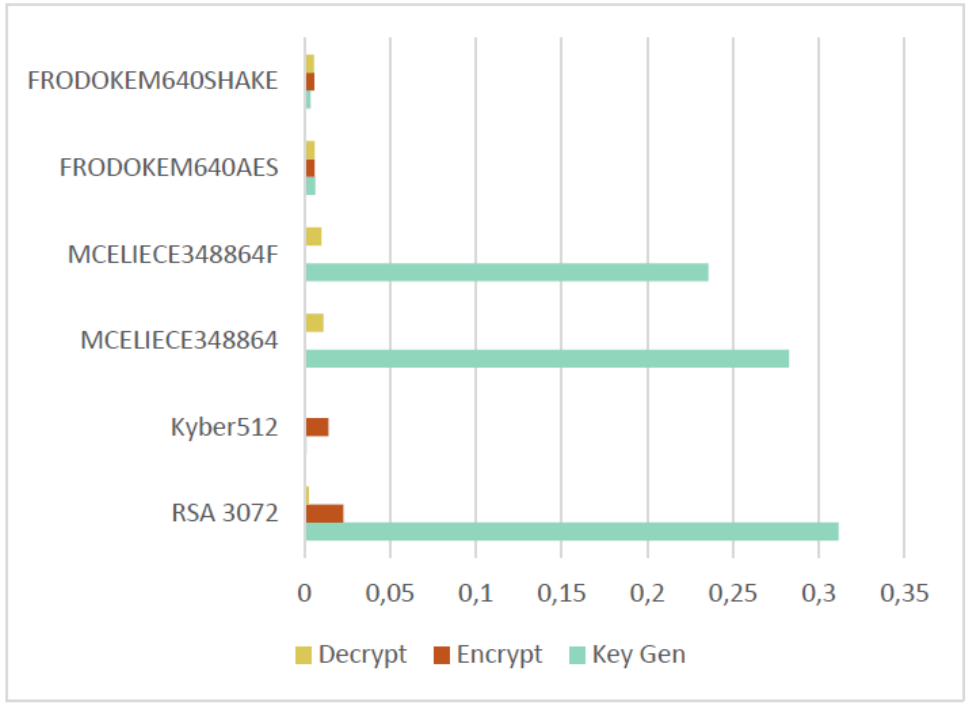
Datentyp	Platz	Einheit	Erklärung
FheInt8	65816	B	−128 bis 127
FheInt16	131624	B	−32768 bis 32767
CompressedFheInt8	**344**	**B**	−128 bis 127
CompressedFheInt16	**680**	**B**	−32768 bis 32767
ClientKey	**39**	**KB**	privater Schlüssel
ServerKey	110	MB	
CompressedServerKey	**24**	**MB**	



[2] Chillotti, I., Gama, N., Georgieva, M. *et al.* TFHE: Fast Fully Homomorphic Encryption Over the Torus. *J Cryptol* **33**, 34–91 (2020). https://doi.org/10.1007/s00145-019-09319-x

Anpassung der DaTreFo-Kryptographie auf Post-Quanten-Verfahren

- Tests unter Java mit BCPQC-Provider von Bouncy Castle
- PQ-KEMs teilweise schneller als RSA
- Signaturen mit CRYSTALS Dilithium schneller als RSA-Signaturen
- Speicherplatzbedarf für PQ-Schlüssel leicht bis stark höher als RSA
- Einbindung von PQ-Zertifikaten per EJBCA-PKI (https://www.ejbca.org/) angestrebt
- Standardisierung in FIPS 203, 204, 205



Vielen Dank für die Aufmerksamkeit.

https://www.hochschule-trier.de/informatik/forschung/projekte/datrefo

Fragen? Anmerkungen?

knorr@hochschule-trier.de