Techniek & Toekomst:
Technologische ontwikkelingen op het gebied van privacy & security

Pim Koeman

Informatiebijeenkomst MRDM

17 mei 2018

Openbaar

Techniek & Toekomst

- Introductie
- Implementatie “Focus op verwerkingsverantwoordelijke”
- Privacy by design status / roadmap 2018
- Toekomst / R&D

Waar staan we, waar gaan we heen?

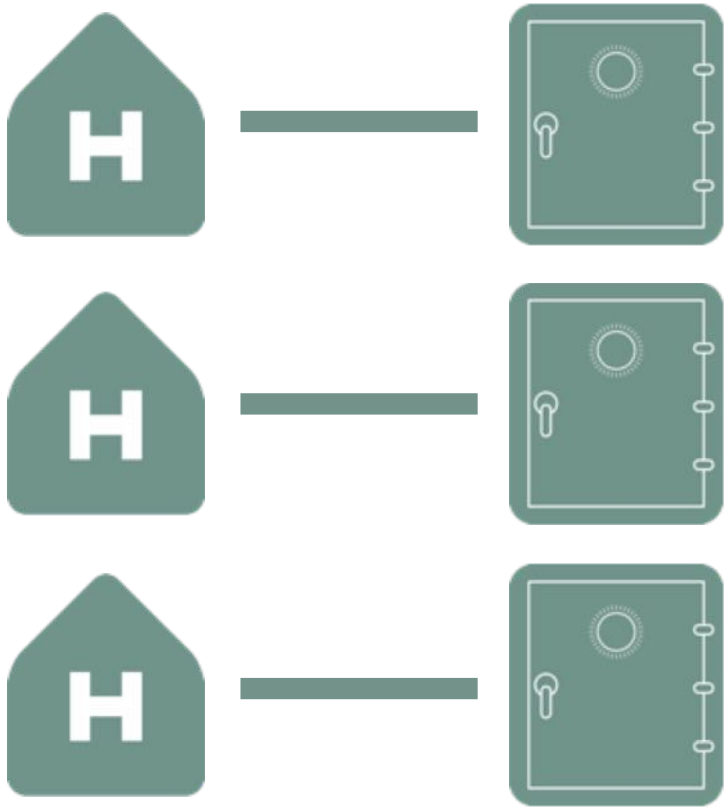
- MRDM Secure Platform (2012-heden)
- Alle persoonsgegevens encrypted at rest & in transit
- Datamanagement per project / registratie
- Techniek volgens ISO27001/NEN7510
- Klaar voor volgende fase
- Focus komende releases

Implementatie “Focus op verwerkingsverantwoordelijke”

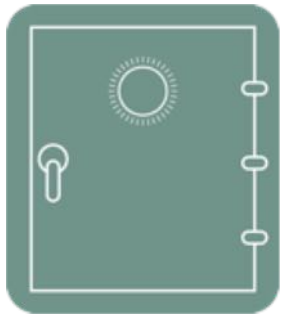
- Databeheer op organisatieniveau
- Pseudonimisatie voorafgaand aan aanleveren van data aan MRDM
- Verwerkingsverantwoordelijke in control
  - Volledig afgeschermde, eigen datakluis met secure inbox en -outbox
  - Volledige controle over eigen datakluis
  - Managementinformatie over eigen datakluis
  - Managementinformatie over gegevensverwerking

- Alle data typen
  - HL7 FHIR / CDA
  - CSV, XML, TXT en XLS

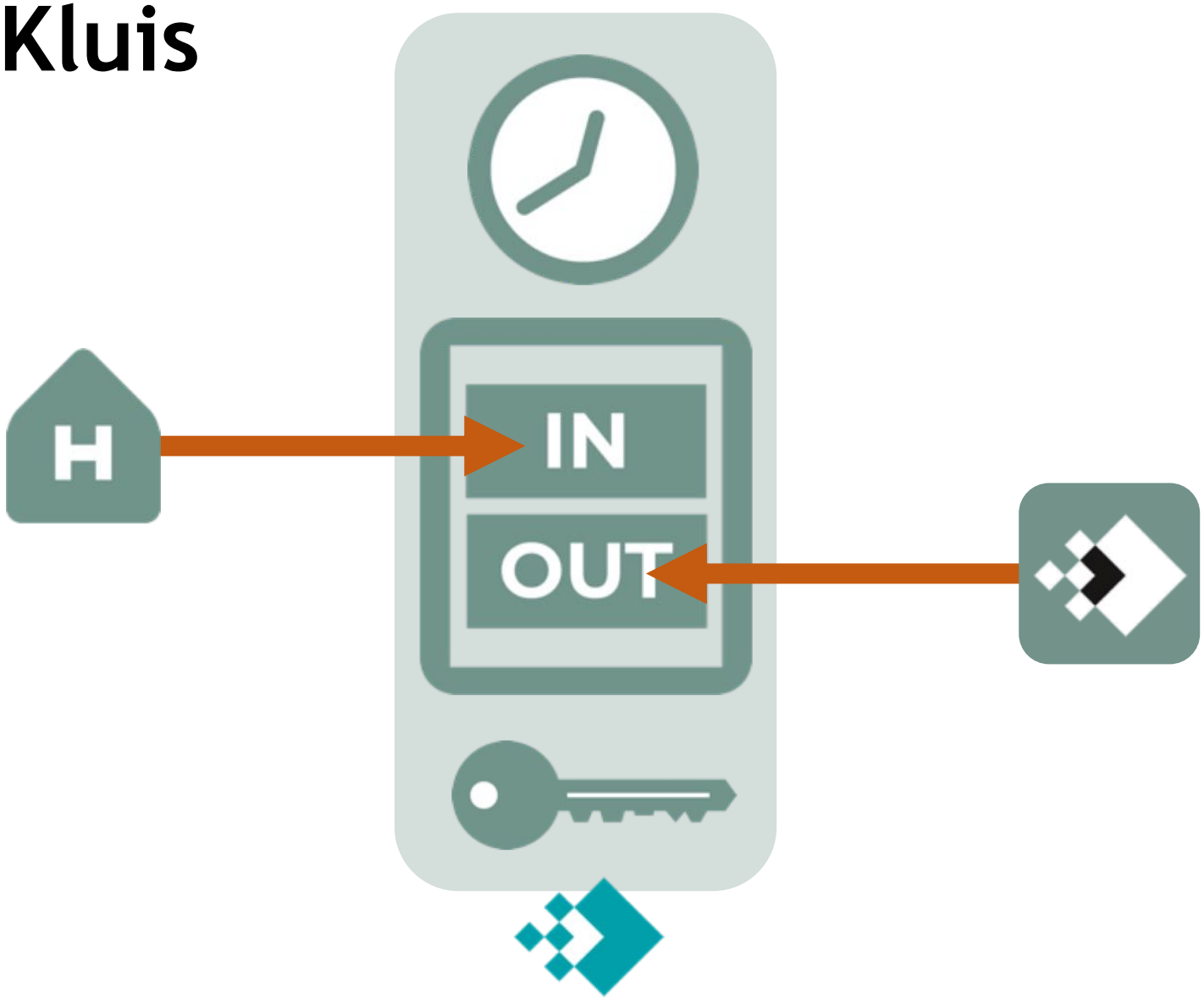
Databeheer op organisatieniveau: MRDM DataKluis



Databeheer op organisatieniveau: MRDM DataKluis



Databeheer op organisatieniveau: MRDM DataKluis



Databeheer op organisatieniveau: MRDM DataKluis

- Eigen beveiligde kluis per veranwoordelijke en processors
- Inbox en outbox voor aan- en uitlevering
- Toolkit voor invoerders, batchleveranciers en processors
- Privacy filtering bij elk gebruik van data
- Geautomatiseerd encryptiesleutel- en lifecyclemanagement

Pseudonimisatie voorafgaand aan aanlevering

- Uitvoer “binnen de muren” van de verantwoordelijke
- Patient volgen in de keten o.b.v. (tijdelijke) “M-Nummers”
- Zorgt voor ontkoppeling van het BSN

Privacy by design roadmap: Authenticatie en Authorisatie

- Onboarding medewerkers en data stakeholders
- Alle interne toegang via tweefactor authenticatie
- Alle interne toegang via hardware tweefactor sleutels
- Eigen “Multifactor” Smartphone app voor gebruikers
- Serviceaccounts met certificaten voor aan- en uitlevering
- Single Sign On voor EPD integratie

Privacy by design roadmap: Cryptografie & Sleutelbeheer

- Sleutel uitgifte-, rotatie en beheer per verantwoordelijke
- Alle data encrypted at rest & in transit
- Alle encryptiesleutels in Cloud (V)HSM (“Fort Knox”)
- Alle encryptiesleutels zijn non-exportable
- Automatische sleutelrotatie
- ”Kill switches” bij vermoeden concern

Privacy by design roadmap:
Data lifecycle management

- Geautomatiseerd beveiligd archiveren van data
- Geautomatiseerd beveiligd verwijderen van data
- Lifecyclepolicy controle via audit log
- GDPR lifecycle management tooling

Privacy by design roadmap: MRDM Software toolkit v1.0

- Functies
  - Configuratie & Certificaatuitgifte
  - Pseudonimisatie
  - DataKluis Secure upload
  - DataKluis Secure download
  - …
- Microsoft .NET Core technologie
- Start 8 Pilotcentra

Toekomst / R&D MRDM

- Self service portal voor verantwoordelijke en afnemers
- Extra externe certificering MRDM toolkit en proces
- (Near) Realtime HL7 FHIR berichtenverkeer via DataKluis

- Onderzoek inzet data loss prevention (DLP) systemen
- Onderzoek toepassing Polymorphic Encryption & Pseudonymisation (PEP)

Samenvatting

- Sterke focus op privacy by design
- Controle bij de verantwoordelijke
- Datakluis per verantwoordelijke
- Ondersteuning met softwaretoolkit

- Vragen en/of opmerkingen?

Informatiebijeenkomst MRDM

17 mei 2018

Openbaar