IHE EUROPE CONNECTATHON WEEK ONLINE BRUSSELS NOVEMBER 2-6 2020

HL7 FHIR in Belgium
Nov 5, 2020 – 2PM
Damien Giry

HL7® Belgium

IHE BELGIUM | Integrating the Healthcare Enterprise

Scope & purpose of the work

- Recommendations on HL7 FHIR usage regarding:
  - Data Exchange paradigms (Messaging vs Documents vs REST API …)
  - Security (End-to-end Encryption, Transport Layer Security/TLS, etc.)

- **Approach**:
  - Started an open Working Group within IHE/HL7 Belgium with participants from regions, industry, hospitals.
  - Looking abroad & collecting requirements and current proposals
  - Defining a common approach that allows variations imposed by the local requirements

Participants of ad-how working group

- IHE Belgium
- HL7 Belgium
- VAZG
- RSB
- RSW
- UZ Leuven

HL7® Belgium

IHE BELGIUM Integrating the Healthcare Enterprise

Data Exchange - Options

- Accessing any individual FHIR resources (e.g. Patient, Observations…) directly via the FHIR RESTful API

- Create Documents (composed of predefined set of FHIR resources) and make them available (i.e. “broadcast” mode) for any user for any purpose

- Create Messages (composed of predefined set of FHIR resources) and send them on a 1:1 basis (one message for one consumer), for one purpose

Data Exchange - Recommendations

- The different paradigms can coexist, if infrastructure is prepared
- Documents and Messages, if based on a web architecture, can be based on a FHIR RESTful API
- It is possible to make broader documents/messages from individual resources, the opposite is not guaranteed.
- Use FHIR REST API as a foundation; when we need documents/messages, we make FHIR documents/messages available on that infrastructure

Data Exchange impact - DataQ, WF, Security

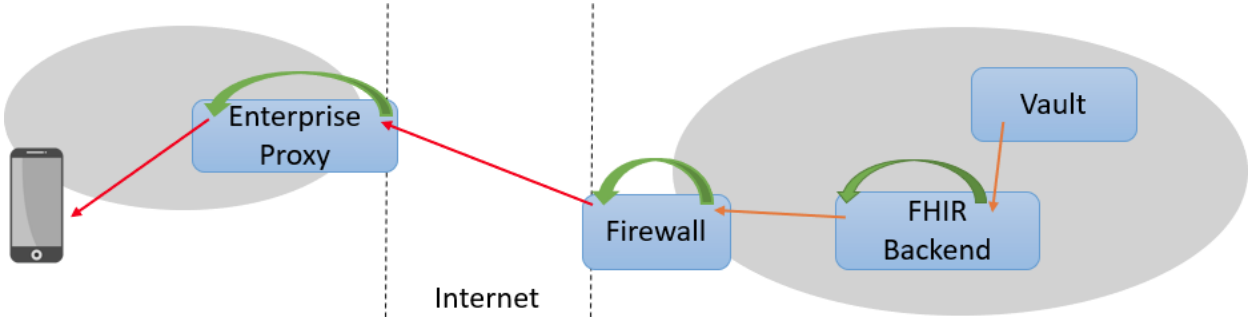
- The choice of Data Exchange paradigm is related to
  - Data quality
  - Workflow
  - Security and privacy:
    - Access control – on “Document level” or “Resource level”
    - User-level End-to-end Encryption indicates a 1:1 communication which is natural with messages, but not REST or Documents
    - The data may be meant to persist and be stored after exchange

Security - Options

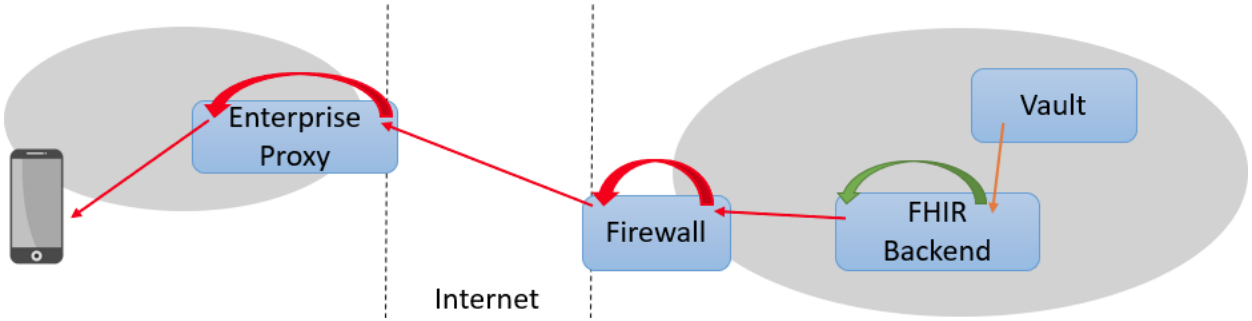
- Security is not only a Technical issue – Technical vs management solutions are needed
  - It's risk management – we add security mechanisms (technical or not) when we have an unacceptable risk (of intrusion, of misuse,..)
  - Delicate, continuous balance – "too secure" ⍰ "too difficult" ⍰ users will make shortcuts ⍰ less secure
- Has impact on functionality and expandability – e.g. End-to-end encryption prevents intermediaries to collect & reuse data
- Other countries have had similar challenges – before and after FHIR (and FHIR has some guidance)

Security - End-to-end / E2E Encryption

- TLS is channel point-to-point encryption
  - Easy to implement
  - No FHIR adaptation



- End-to-end encryption
  - Needs some work
  - FHIR adaptation required
  - PKI needed (already here in most cases)
  - Interesting for specific use cases



Certificate Based Mutual Authentication

- Between identified systems, we can require them to authenticate each other before data is exchanged
  - Prevents the global internet from exploiting applicative faults.
  - Prevents stolen authorization tokens from being used.
- Belgium currently already has a system in place for distributing eHealth certificates (users/apps/org) that can be leveraged to this purpose.
- It's still burdensome…
  - Low adaptation in current eHealth infrastructure
  - Web applications intended for patients / caregiver

Security - Alignment with Belgian scene

Belgium has made some advances in security, we can reuse them

- eHealth certificates can be used (for Mutual Auth & E2E encryption)
- On-the-fly certificates for when E2E encryption is needed

Security - discussions

- “One formula” is not a good goal –
  - For example, for simple, patient apps, we can use TLS (not even mutual auth)
    - But that may not be sufficient for bulk data transfers, or for more sensitive scenarios
  - for example E2E encrypted messages make sure that an intermediary cannot read content
    - So the intermediary cannot do format conversions, checks, or reuse data (analysis or other apps)
- We agreed on common parts and guidance, giving some freedom to projects to add their security mechanisms
  - Compatible with the baseline
  - Compatible with FHIR (i.e. no custom mechanisms)

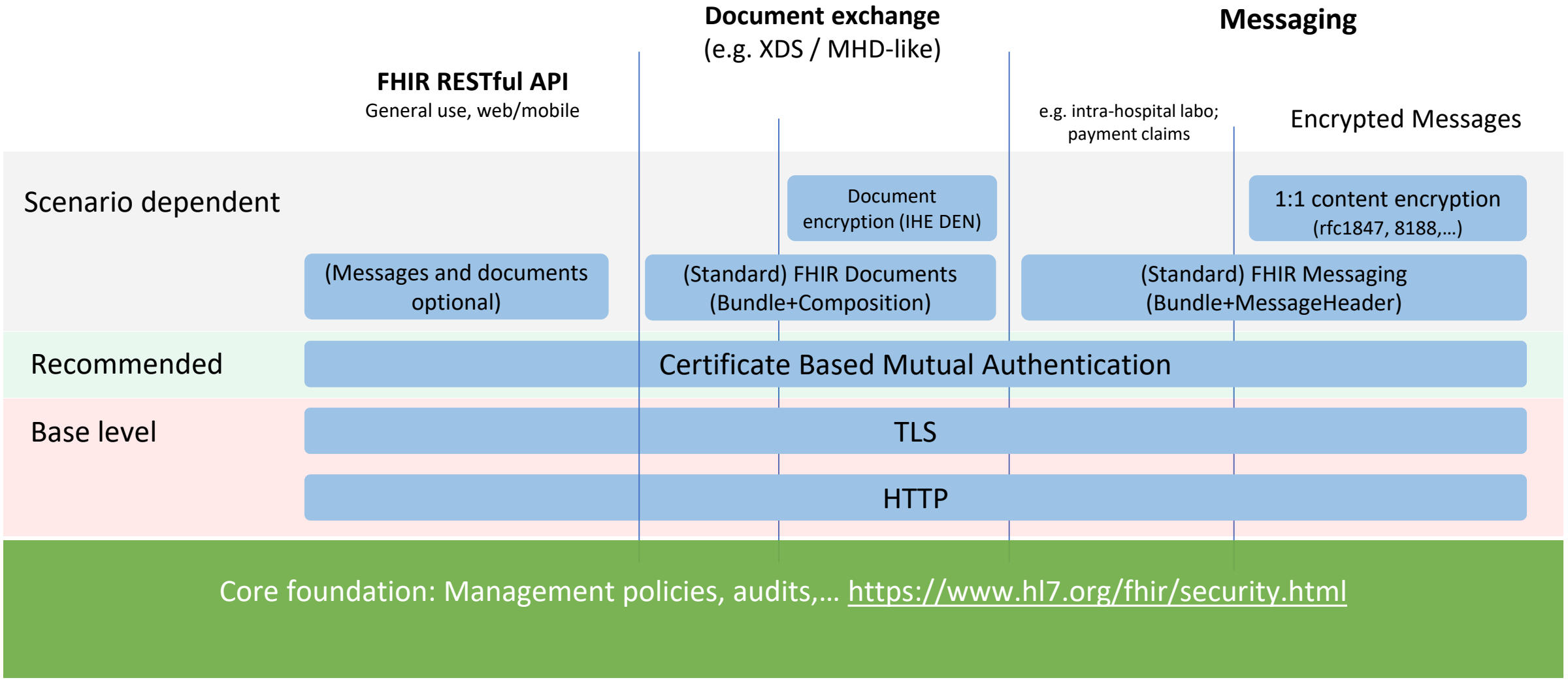
Security - Conclusions

No need to impose same security mechanism for all – depends on purposes and risks.

- E.g. RESTful API using “only” TLS may not be adequate for some cases
- Other cases may not be able to support E2E encryption

…But a decision is needed… Thus:

- **Baseline for all FHIR projects (MUST): Secure HTTP (TLS) + FHIR recommendations** - management policies, audit logs, search as POST payload (not GET), etc.
- **Recommended (SHOULD): Mutual Authentication + SMART on FHIR**
- **Depending on other use cases (MAY): E2E Encryption or other mechanisms**



HL7® Belgium

IHE BELGIUM Integrating the Healthcare Enterprise

- **Pieter Devolder**, IHE Belgium co-chair users
  pieter.devolder@uzgent.be
- **Karlien Erauw**, IHE Belgium co-chair vendors & HL7 Belgium co-chair
  karlien.erauw@agoria.be
- **José Costa Teixeira**, HL7 Belgium chair
  jose.a.teixeira@gmail.com