Enhancing Patient Privacy and Security via Complex Event Processing (CEP) and Legitimate Relationships Service (LRS)

Raed A. Haltam

UMIT - University for Health Sciences, Medical Informatics and Technology; Hall in Tyrol, Austria

Abstract

We present a solution and a methodology that enhances patient's privacy and security in cross-organizational, regional and national healthcare provisioning models. The research was accomplished in the context of the Legitimate Relationship Service that is part of the United Kingdom's National Programme for IT (NPfIT). The solution monitors access requests issued by clinicians to patient information clinicians from multiple different organizations and issues alerts and notifications based on modeled event patterns. The solution employs Complex Event Processing (CEP) which stems from Event-driven SOA. HL7 messages are used are canonical event model and CDA documents as canonical Entities. We describe the solution in form of a logical view as a Reference Architecture(1) that can be reused in independent of the implementation and technologies. The reference implementation utilized hl7:QUPA_IN010000UK01 message as input basic event.

Keywords:

Hospital information systems, Multihospital information systems, Automated pattern recognition, Service Oriented Architecture (SOA).

Methods

The first step review the detailed requirements for the Legitimate Relationships Service (LRS) that were used by the National Programme for IT (NPfIT) (2) to determine the functional components of the LRS Service

The second step defined the Reference Architecture of the Legitimate Relationship Service and described the architecture using the logical view according to the (4+1) Model (1).

The third step developed a Reference Implementation which executed two event patterns, detected their occurrence and raised respective events.

Results

A Reference Architecture that was proven via a Reference Implementation. The implementation detected two event patterns: The 1st pattern: Suspicion of Identity Theft. The 2nd pattern: Suspicion of Inappropriate Access to Patient Information By a specific Clinician

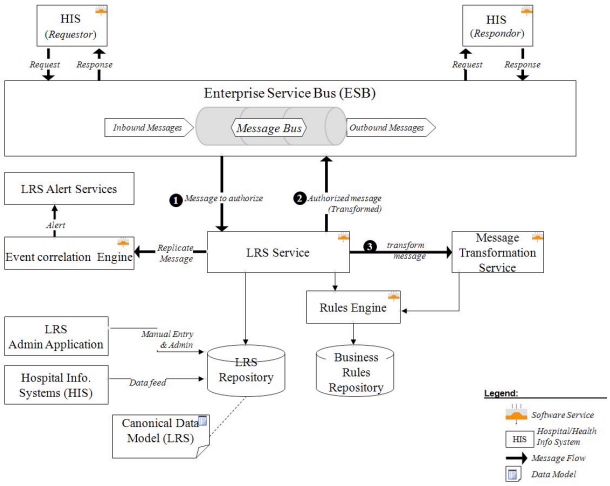

Figure 1-LRS-Reference Architecture–eBooking-NPfIT

Conclusion

Based on the results we conclude the following:

1. Patient's Privacy and Security can be enhance via Legitimate Relationship Service (LRS).
2. LRS is possible for regional and national implementations.
3. The CEP engine is non-intrusive. It does not require modification of source systems.

References

[1] Kruchten P. Architectural Blueprints—The "4+1" View Model of Software Architecture IEEE Software. 1995;12(6):42-50.

[2] NPfIT (Part 3) N. Integrated Care Records Service, Part III - Common Requirements. In: Technology NPfI, editor. Second Iteration ed: National Health Service (NHS) - United Kingdom; 2002.

[3] StreamBase. StreamBase Documentation. 2007 [cited; Available from: http://www.streambase.com