Common message security workflow

Overview

Description: This workflow describes how authentication and authorisation of systems making use of the HIE is done through the HIM. This workflow provides the security underpinning for many other workflows that rely on a secure connection and authorised message delivery.

Sponsor: Ryan Crichton, with the IL (HIM) community

Status: Completed

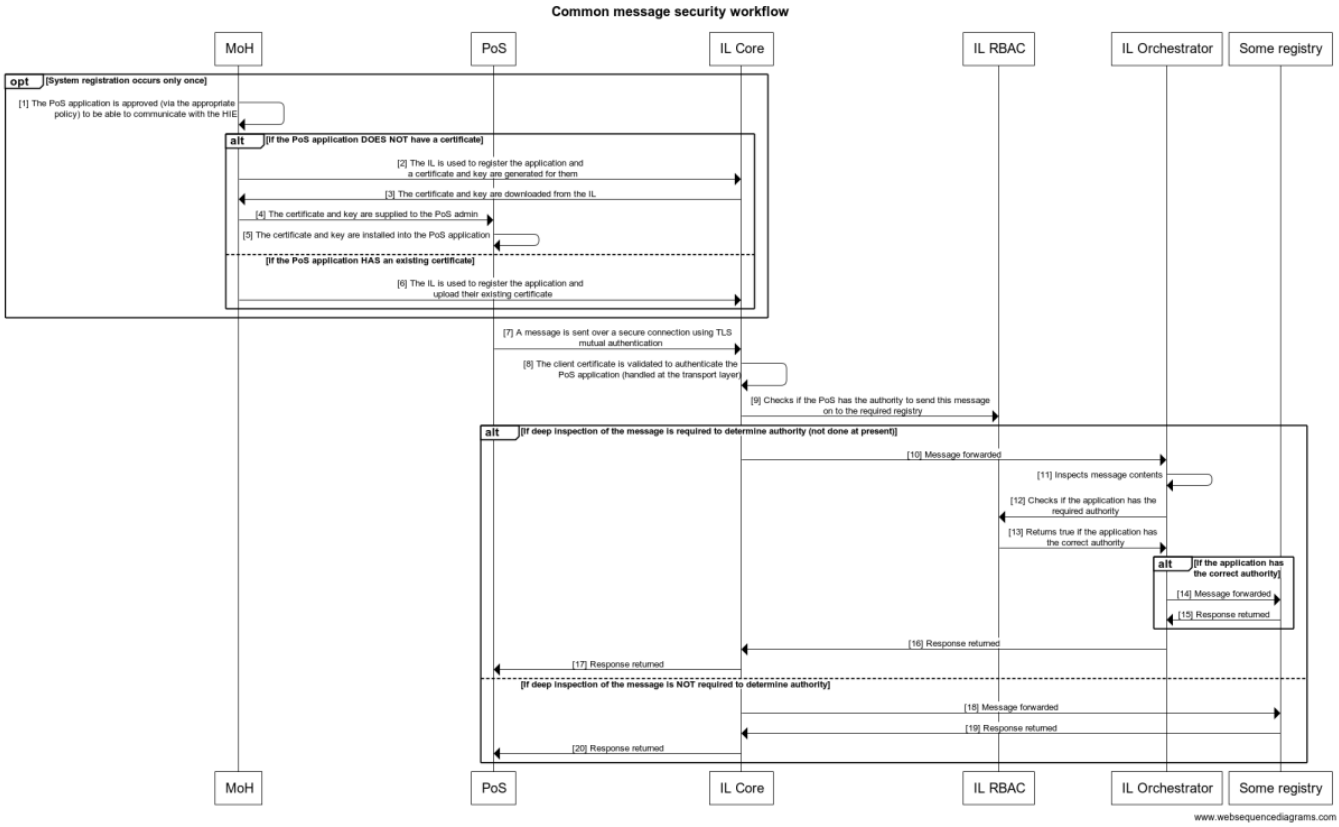
Last Modified: 12rd March 2015

Referenced Standards and APIs:

- IHE ATNA

Actors

- MoH - This actor represents the authority that controls access to the HIE. This is likely a Ministry of Health or a Department of Health.
- PoS - The Point of Service application that is connecting to the HIE.
- IL Core - The Interoperability layer core component that provides a single entry point for message destined for systems within the HIE, it provides security, audit and logging capabilities.
- IL RBAC - The interoperability layer role-based authentication control (RBAC) component.
- IL Orchestrator - This is a message specific orchestrator that is able to process and orchestrate a particular message based on the messages contents.
- Some registry - This represents one of the other registry components of the HIE.



Technical details

Ref	Interaction	Endpoint	Data	Transaction Specification
1	The PoS application is approved (via the appropriate policy) to be able to communicate with the HIE		policy	
2	The IL is used to register the application and\n a certificate and key are generated for them		details about the application	
3	The certificate and key are downloaded from the IL		in .pem format	
4	The certificate and key are supplied to the PoS admin		in .pem format	Sneaker-net
5	The certificate and key are installed into the PoS application			
6	The IL is used to register the application and upload their existing certificate			
7	A message is sent over a secure connection using TLS mutual authentication			ATNA Node Authentication
8	The client certificate is validated to authenticate the PoS application			
9	Checks if the PoS has the authority to send this message on to the required registry			
10	Message forwarded			
11	Inspects message contents			
12	Checks if the application has the required authority			
13	Returns true if the application has the correct authority			
14	Message forwarded			
15	Response returned			
16	Response returned			
17	Response returned			
18	Message forwarded			
19	Response returned			
20	Response returned			