

A Reference Architecture for Healthcare Benefit Exchange

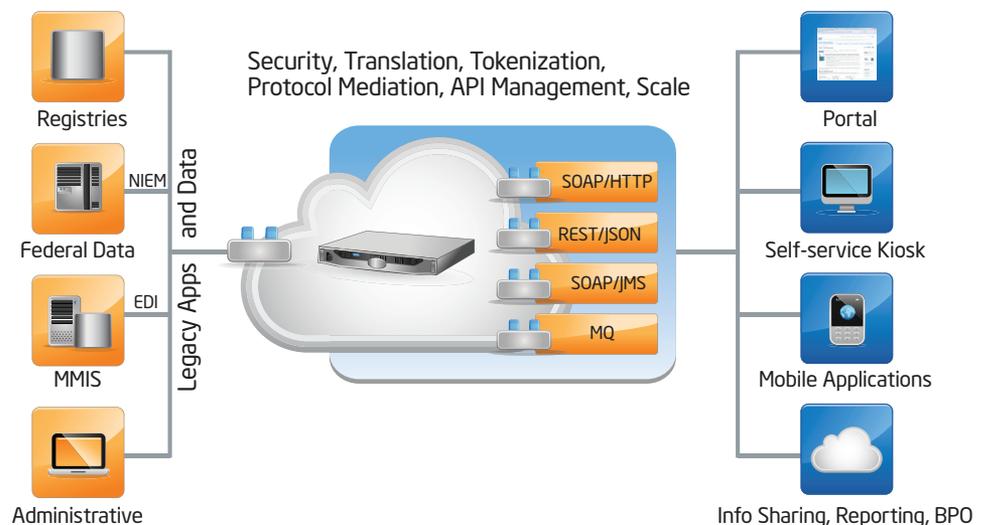
Given the looming deadline of 2014 under the Patient Protection and Affordable Care Act, and the fact that the states have existing Medicaid architecture that already provides many of the components required in an HBE, not leveraging this existing infrastructure ... would be a costly duplication of effort and not even an option for many budget constrained states.

Abstract

Health Information Technology for Economic and Clinical Health (HITEC) and Patient Protection Affordable Care Act (PPACA) are fueling the requirement for and subsequent growth of, interoperable Healthcare IT systems in the US. A common thread between initiatives such as Accountable Care Organizations (ACO), Health Information Exchange (HIE) and Healthcare Benefit Exchange (HBE) is the use of SOA (Service Oriented Architecture) for loosely coupled, interoperable architectures. In this solution brief we take a look at how this plays out in the HBE healthcare ecosystem and recommend a reference architecture that can be implemented with Intel® Expressway Service Gateway for Healthcare (Intel® ESG for Healthcare) - reflecting the unique legacy protocols in healthcare, the services required for the exchanges, and the impact of strict security laws on the overall architecture.

This paper is intended for healthcare solution specialists, technology architects, business analysts in the healthcare industry, Healthcare SMEs, executives, state level health and human services implementers, system integrators who are looking to build state HBE systems, and other potential customers.

Figure 1: Service Gateway as Proxy in HBE



Introduction

PPACA mandates all states to establish an HBE where individuals will be able to shop and purchase competitive health insurance and be enrolled in public healthcare programs based on their eligibility. Consuming and presenting information from the disparate health plans and checking for eligibility with Medicaid and state run healthcare programs will require integration of heterogeneous systems.

The states have been given a choice to either:

1. Build an HBE.
2. Coordinate with other states to form an interstate HBE.
3. Default to an HBE that is being built by the Federal government.

This paper is limited to a discussion of the technical aspects of the data integration and security components of an HBE as they can be implemented with Intel® ESG for Healthcare. It does not address other components of the exchange such as rules engines, data stores or user interfaces such as portals. It is, however, designed to integrate with these components through standards based interfaces as part of a loosely coupled architecture.

The following are the specific deadlines for the HBE mandate,

Certification : January 1, 2013

Operations : January 1, 2014

Self-Sustaining : January 1, 2015

Given the looming deadline of 2014 and the fact that the states have existing Medicaid architecture that already provides many of the components required in an HBE, not leveraging this existing infrastructure but rather standing up yet another silo, would be a costly duplication of effort and not even

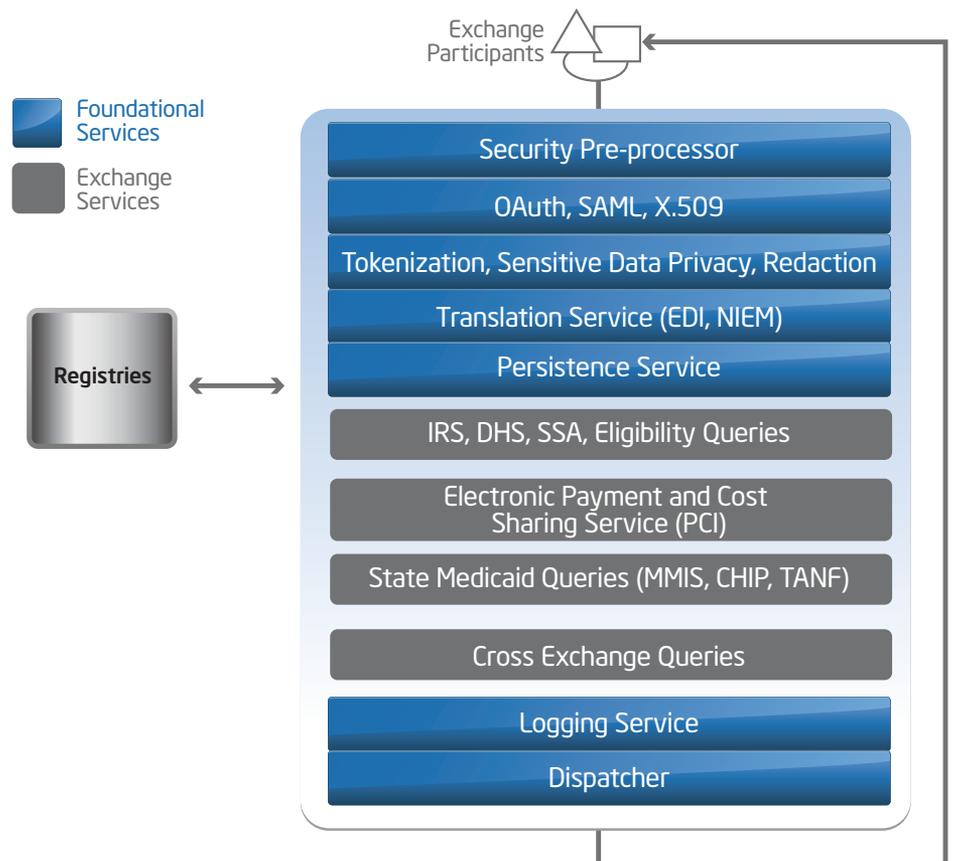
an option for many budget constrained states. Instead, Intel® recommends that the existing MMIS infrastructure components be leveraged along with the use of a Service Gateway, such as the Intel® ESG for Healthcare.

Taking this approach will reduce development time, provide ample agility to support the changes that are bound to emerge in this nascent environment, deliver the performance to process all exchange services with a manageable foot-print, provide a HIPAA compliant security capability for protection of Federal Tax Information (FTI), Personal Health Information (PHI), and be strong enough to withstand cyber attacks.

HBE Reference Architecture

The reference architecture depicted below illustrates the functional components that are required to enable the exchange of data between applications hosted by the HBE and applications hosted by the exchange participants. The architecture adheres to the CCIIO/CMS Guidance for Exchange and Medicaid Information Technology (IT) Systems and the Technical Architecture defined in the Medicaid Information Technology Architecture (MITA) Framework for a secure, SOA based and scalable exchange. The individual services will be described on the following pages.

Figure 2: HBE Reference Architecture



Security Preprocessor

A Healthcare Benefit Exchange has to be HIPAA compliant and protect Personal Identifiable Information, such as Federal Tax Information and Personal Health Information. Therefore, we recommend the use of a policy enforcement point as a security preprocessor at the ingress and egress of the exchange, to protect requests to and from exchange participants, whether they are mobile applications or legacy MMIS systems.

It is then the responsibility of the security preprocessor service to manage security and routing for each request. Transport security is implemented using two-way, mutual authentication between the Exchange Participant and Intel® ESG for Healthcare. Public key certificates supporting node-level authentication are configured using the built-in certificate store in Intel® ESG for Healthcare, which is configured using the security configuration available from the web-based administration tool. The security preprocessor service verifies the signature and SAML assertion of the certificate embedded in the request header. If the exchange participant is a mobile application, a third-party federation component can be used to return SAML assertions to web mobile applications in support of single-sign-on (SSO) and Intel® ESG for Healthcare can enforce authentication, authorization and OAuth processing for non-trusted clients. Intel® ESG for Healthcare can also enforce perimeter security to protect against denial of service attacks and content threats.

Intel® ESG for Healthcare provides additional protection of sensitive data, through PII protection. Intel® ESG for Healthcare has a PII data privacy option (currently on the product roadmap, due

to be released in 2013) that allows for traditional message level security as well as format preserving encryption (FPE)* of sensitive data that is flowing through the system. This could include protecting information such as Name, DOB, SSN, Address, Zipcode, Medical records, tax information and other sensitive data records. The use of format preserving data encryption mitigates the risk of accidental or malicious data exposure and insulates back-end systems from changes. While there are other systems in the market which provide similar functionality, Intel® ESG for Healthcare can modify data in-transit over disparate protocols without relying on an integration SDK.

Privacy policies may be expressed through encryption of PII data, redaction of PII data or data tokenization for credit card information and PCI DSS compliance. Privacy may also entail OAuth 2.0, which protects user credentials from third parties. All of these types of privacy and security policies may be specified on requests or responses, and the level of control can vary based on the calling client and can be enforced in the security preprocessor, based on identity and location of the client along with time of day or day of the week.

Intel® ESG for Healthcare integrates with most existing IDM (Identity Management) systems. The integration connectors are already pre-built so the integration with any identity system (including identity directories such as AD, LDAP) is a configuration step, not a task requiring custom development. You can set access control policies around a specific application and data that are being accessed. This can be at a very high level or be very granular. Intel® ESG for Healthcare can evaluate every transaction based on the identity of the user and

make decisions based not only off the identity + policy but also overlay a location based component that can restrict a type of usage pattern (i.e. from a more secure device to a less secure device, such as desktop vs mobile device).

When you expose your services on the Internet, as with an HBE, whether from a cloud or from an on-premise deployment, you need to provide protection for your exposed services. Intel® ESG for Healthcare has declarative policies that include CAP (Content Attack Prevention), AAA (authentication, authorization, access control), Message Routing, QoS (Quality of Service), Transformation (XSLT), Validation (XSD), and WS-Security. Further, many policies can be updated and cached dynamically without the need for a system restart. This means that an administrator can update certain policies on an external server or location and Intel® ESG for Healthcare can dynamically apply them to live running traffic without taking the system down or stopping processing. The policies to which this applies include: content based routing, content-attack-prevention policy, XSLT stylesheet, XSD (schema), and XML processing parameter set (XML documents).

Finally, policy enforcement is applied to any part of the incoming data over standard SOAP or REST APIs: This includes the transport (e.g. client IP address), protocol data (e.g. URL, query, headers, and queue name), protocol type, protocol meta-data, message headers, message body, and attachments. This is possible due to the high performance architecture that converts the entire request into a binary stream and makes access to it available using the policy design tool.

*The FPE implemented by Intel is based on AES-FFX.

Translation Service

The Translation Service is responsible for translating incoming messages to and from legacy formats - such as HIPAA EDI and Cobol Copybook, to XML, which are prevalent in MMIS architectures before handing the messages over to the security preprocessor. The Intel® ESG for Healthcare translation service in conjunction with the security preprocessor will, for example, handle an EDI receive step, validate how well-formed the message is, and provide a response to the sender prior to translating to a format that the back end claims systems can support, such as Cobol Copybook, in effect offloading these steps from the backend system where processing tend to be more expensive.

Persistence Service

For long running transactions and guaranteed delivery, the role of the persistence service is to interact with message queues, databases and caches. Intel® ESG for Healthcare has native support for the IBM Mqueue client and JDBC which makes this a configuration step in the overall work flow.

IRS/DHS/SSA Eligibility Queries

CMS requires eligibility queries be sent to the IRS for income verification, to the DHS for lawful presence verification, to the SSA for citizen verification and to CMS for program eligibility verification. CMS has defined NIEM as the preferred method for these sets of queries. Intel® ESG for Healthcare supports NIEM IEPDs, but none has been made available by CMS at the time of the writing of this solution brief. For a description of the NIEM support in Intel® ESG for Healthcare please see: <http://cloudsecurity.intel.com/solutions/government/niem-national-information-exchange-model>

Electronic Payment and cost sharing service (PCI DSS)

For a Healthcare Benefit Exchange to process electronic payments, the HBE will need to adhere to the Payment Card Industry Data Security Standard, or PCI DSS. PCI DSS is enforced through annual audits. Intel® Expressway Tokenization Broker, replaces the Primary Account Number (PAN) with a token at the ingress to the exchange, thereby reducing the PCI DSS scope and the cost of the audit. For more information regarding Intel® Expressway Tokenization Broker, please see <http://cloudsecurity.intel.com/solutions/tokenization-broker-reduce-pci-scope>

State Medicaid Queries

Existing state programs such as TANF and CHIP will need to be queried for eligibility as well. We are recommending that the existing MMIS be extended to provide BHE services as well. Integration with programs such as TANF and CHIP might be within the same domain, but this will vary from state to state based on their current MMIS implementation. Intel® ESG for Healthcare can mediate eligibility queries to the state programs, eliminating the requirement for any API changes to the existing systems.

Cross Exchange Queries

In the case of movement between states, an HBE should have the ability to query other exchanges. The IHE profiles typically describe how CDA documents are exchanged, but the profiles could conceivably be used for the exchange of other payloads. One method that might be employed for this purpose is the IHE XCA/XCPD profile. Intel® ESG for Healthcare has support for this profile as well as the IHE PIX/PDQ, XDS.B, ATNA and CT, should the exchange wish to exchange data with a Healthcare Information Exchange or the NwHIN. For more information regarding

IHE profile support and how to apply SOA to IHE Profiles, please see http://www.ihe.net/Technical_Framework/upload/IHE_ITL_TF_WhitePaper_A-Service-Oriented-Architecture_SOA_2009-09-28.pdf and <http://cloudsecurity.intel.com/white-papers/interoperable-health-information-exchange/>

Performance and Scale

A core mandate from CMS is that the Healthcare Benefit Exchanges must be scalable. Intel® ESG for Healthcare was created from the ground up to process messages at wire speed, with the following design features:

- **Optimized XML processing and policy execution** - Intel® ESG for Healthcare provides a native software XML acceleration layer with specific optimizations for the very latest world-class microprocessor optimizations without requiring a third-party add-on board.
- **High concurrency I/O processing tied to Intel® Multi-Core** - Intel® ESG for Healthcare supports thousands of connections with low latency for SSL and non-SSL traffic.
- **High performance hardware I/O processing** - Intel® ESG for Healthcare supports hardware acceleration of I/O calls, a key requirement for service gateways. Intel® ESG for Healthcare ships with Intel® I/O Acceleration Technology in the standard hardware appliance and supports I/O AT in the software and virtual appliances.
- **Large Message Handling** - Intel® ESG for Healthcare has demonstrated large message handling for streaming XML security and EDI claims files, up to 2GB running in customer deployments.
- **Real-time Policy Updating** - Intel® ESG for Healthcare supports remote updating of security policies and artifacts with zero service downtime.

▪ **Back-End Load Balancer** – Intel® ESG for Healthcare supports back-end load distribution across HTTP based SOAP or REST services using round robin or least request algorithms with server stickiness support and automatic retry capabilities.

Data Analysis, Big Data, Business Intelligence

Intel® ESG for Healthcare's analytics and Big Data interfaces allow you to connect multiple sources of high volume data. This enables you to correlate and analyze patient and consumer specific correlated information such as drug correlation, fraud detection, payer information etc. to build a consumer profile that will help making knowledgeable decisions about specific consumer or a group based analysis. For more information about Big Data integration, please see <http://cloudsecurity.intel.com/solutions/security-for-big-data-deployments>

Total Cost of Ownership (TCO)

Intel® ESG allows you to develop, deploy, maintain and monitor your HBE interfaces from a consolidated interface. Intel® ESG for Healthcare provides an Eclipse based development platform, Services Designer, which allows you to develop policies using a visual work flow environment. There is no need to code for hours and test the code for weeks before deploying updates to a solution. This means your development costs are reduced; your upgrade costs are reduced, along with your maintenance and administrative costs. In addition, Intel® ESG for Healthcare workflows are completely parallel and the highest performing in the healthcare middleware class, which results in an HBE that can process a lot more transactions with a minimal foot print. This results in a reduced TCO (Total Cost of Ownership) and increased ROI (Return on Investment) while providing a quicker time to deployment. Furthermore, faster development times will lead to getting your solution out to the market more quickly.

Conclusion

Healthcare Benefit Exchanges are a core IT component of the health care reform. It is mandated that they are implemented using a SOA that can meet both current and future needs. In this solutions brief we have described how Intel® ESG for Healthcare can be used to handle the application to application message exchange in a secure and scalable manner, with support for legacy data formats.

Intel® ESG for Healthcare is a proven, reliable, scalable, highly secure, ready to use gateway built to be the healthcare middleware solution that connects multiple healthcare systems. Intel® ESG for Healthcare is standards based, yet flexible enough to integrate with newer healthcare standards as they emerge. In addition, Intel® ESG for Healthcare does not require any coding, but rather provides a graphical development environment, with a drag, drop and configure approach which increases developer productivity, and allows for a faster time to production to meet the HBE timelines.

SOLUTION PROVIDED BY:



More Information:

Web: cloudsecurity.intel.com

Americas: 1-855-229-5580

E-mail: asipcustomeercare@intel.com

All other geographies: 1-425-888-0426

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web site at www.intel.com.

Copyright © 2012 Intel Corporation. All rights reserved. Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Printed in USA

Please Recycle

