



DGI Update: Your Guide to Interoperability & Conformance Test Services

July 2007

Industry Profiles: ebMS XML Encryption

Last month in our newsletter, we looked at the need for industry profiles. While B2B standards, like AS2, meet the needs for most business transactions, certain industry groups may have unique requirements which are not specified in the standard. The solution is industry profiles. Industry and supply chains find great value in having software meet their needs with test profiles and having those products certified "interoperable." This newsletter will focus on the XML Encryption profile within ebMS.

In 2003, the Centers for Disease Control and Prevention (CDC) approached Drummond Group about testing a profile for using XML encryption within ebXML Messaging Service v.2 (ebMS). CDC was working on a long term project known as PHIN, the Public Health Information Network. PHIN required secure messaging transport of ebMS and the use of XML encryption. CDC believed an industry profile was needed to clarify the exact requirements for implementing XML encryption in PHIN.

CDC came up with the specific requirements for the profile. These included only synchronous messaging, using one and only one payload, HTTP with SSL must be used and SSL Client Authentication is required along with other requirements. As DGI conducted ebMS testing with this industry profile, different interoperability issues were found and resolved creating best practices which were added into the profile with the approval of the CDC. Examples of these best practices are the choice of digitally signing the payload first before applying XML encryption and the content-type for the XML attachments either by application/xml or text/xml. These best practices are not part of the XML Encryption Profile requirements but consensus on these issues is

critical in order to achieve interoperability. The full XML Encryption profile with its requirements and best practices can be found at

<http://www.drummondgroup.com/html-v2/XML-encryption.html>

This profile has been tested by Drummond Group for several years within the ebMS interoperability tests and proven to be a valuable addition to ebMS adoption. While the profile was developed for PHIN by CDC, other industry groups, including automotive, felt this was a beneficial profile and adopted it as well. Next month, we will look at another ebMS profile which was developed for automotive retail industry.