31st July 2008, National ICT Australia, 7 London Circuit, Canberra

Web Services Forum - Summary of Outcomes

Background:

A Web Service Forum was jointly offered by IHE Asia-Pacific, HL7 Australia, MSIA and HISA. With the anticipation of the broad development and implementation of web services in Australia to achieve integration between health information systems in line with NEHTA guidelines, the challenge is:

How does the health information system industry build web services such that they will:

- Interoperate with other health information systems
- Be built and deployed with low implementation and support costs
- Meet privacy requirements
- Support efficient provider workflow
- Increase safety for patients

Many vendors are grappling with these issues. The forum explored these issues from many perspectives and provided an opportunity for discussion of specific WSDL specifications provided by industry which stimulated frank and open round table discussion of these challenges. The forum increased the understanding of industry with regard to the challenges, and informed the consideration of appropriate profiles for development and implementation of interoperable web services.

Outcomes:

The following is a summary of the key points noted in the discussion:

- If keys and certificates are to be used to secure web services, it was agreed a dual key system is necessary for individual certificates/keys given the appropriateness of separating the business functions of signing and de-securing. For example the function of signing is typically not delegated to other entities when the entity that owns a key is not available, where as it makes sense to delegate the function of decryption to another entity when the entity that owns the key is not available.

- If WS-Security is to be used to secure web services using keys and certificates, the following points were noted:

    - All existing development environments (Microsoft, Java, etc) are limited to performing asymmetric encryption to achieve certificate based WS-Security.
    - Current Medicare Australia keys and certificates do not support this sort of encryption so different keys and certificates will be required.

- Microsoft's WCF development environment currently does not support certificate based WS-Security with dual keys (single key must be used for both signing and decrypting). NEHTA acknowledged they are working with Microsoft to address this issue, however there is no expected resolution date.
- Asymmetric encryption is slower than symmetric encryption and has been demonstrated to be able to process far fewer transaction per minute than symmetric encryption. Medicare Australia advised their CPAP processes 4000 authority transactions per minute and would struggle with the transaction load if using asymmetric encryption.
- Can only reliably encrypt content up to a size of about 1.5 MB. This would not support the delivery of radiology images.

- If sign and encrypt is the preferred order, WS-Addressing could be used to persist information required to route communications through the intermediary points/servers that do not have access to keys to decrypt communications. This includes the persistence of such data as: destination (eg organisation, provider, etc), source (eg organisation, provider, etc) and message identifier.

- Some participants at the forum were unclear as to whether NEHTA would require keys belonging to individuals and/or organisations to be used to secure communications using web services. Such a decision would benefit from an assessment of the relative merit of using individual or location certificates in light of the impact on patient safety and efficiency. For example would requiring a clinician to use an individual key to decrypt a communication result in the inefficient use of clinical time? Could this present a business continuity issue that may impact on patient safety if that clinician were not present to decrypt the communication?

- Some participants at the forum were unclear as to whether NEHTA are specifying web services that can be used to secure communications for any type of clinical document, or whether a different web service specification will be required for every different type of clinical document (eg pathology, medication, referrals, etc).

Thank you to all those who attended the Forum, particularly David Bunzli and Larry Singer for presentations on their successes and challenges with the development of web services. These presentations were most informative and provided the basis for a worthwhile and productive discussion.