|  |  |
| --- | --- |
| **เอกสารผลการปฏิบัติงานแบบ On Site Service** | |
| **โครงการ :** | งานจ้างบำรุงรักษาระบบ SAP ด้าน Basis และ Function เลขที่ จท.81/2559 |
| **สถานที่ :** | การประปานครหลวง |
| **วัน/เดือน/ปี :** | 20 ตุลาคา 2560 |
| **เวลาที่ปฏิบัติงาน:** | 13:00-17:30 น. |
| **ชื่อ-นามสกุล :** | นาย เสกสรร มณี |
| **Module :** | ABAP |
| **Incident No. :** | MWA-MA02-000104 |

**ผลการปฏิบัติงาน :**

ให้คำปรึกษาเกี่ยวกับการกำหนดรูปแบบการรักษาความปลอดภัยของ Web Services ดังนี้

1. อธิบายเกี่ยวกับการรักษาความปลอดภัย การรับส่งข้อมูล ของ Web Services

**ความต้องการ :** ต้องการทราบวิธีการเลือกใช้รูปแบบการรักษาความปลอดภัยของ Web Services ที่เหมาะสม

การรักษาความปลอดภัย การรับส่งข้อมูล ของ Web Services จะมีอยู่ด้วยกัน 2 ระดับคือ

1. **Transport Level Security** จะเป็นการรักษาความปลอดภัยของข้อมูลในระดับของการส่งข้อมูล โดยสามารถใช้งานโปรโตคอล HTTP หรือ HTTPS ส่งข้อมูลผ่าน Transport Layer
2. **Message Level Security**  จะเป็นการรักษาความปลอดภัยของข้อมูลในระดับข้อความ โดยทุกๆ ข้อความจะมีรูปแบบการรักษาความปลอดภัยตามมาตรฐาน WS-Security

**Communication Security**

เป็นการกำหนดเกี่ยวกับรูปแบบการรักษาความปลอดภัยข้อมูล

* **Non ( HTTP )** เป็นการส่งข้อมูลที่ไม่มีการเข้ารหัส
* **SSL ( HTTPS, Transport Channel Security )** เป็นการส่งข้อมูลที่มีการเข้ารหัส
* **Symmetric Message Signature / Encryption** เป็นการส่งข้อมูลที่มีการเข้ารหัส โดยทั้งผู้รับ และ ส่งจะต้องมี Public Key ตรงกัน จึงจะสามารถรับส่งข้อมูลกันได้
* **Asymmetric Message Signature / Encryption** เป็นการส่งข้อมูลที่มีการเข้ารหัส โดยทั้งผู้รับ และ ส่งไม่จำเป็นต้องมี Public Key ตรงกัน ก็สามารถรับส่งข้อมูลกันได้

**คำแนะนำ**  **:**

การกำหนดเกี่ยวกับรูปแบบการรักษาความปลอดภัยข้อมูล ควรเป็นแบบ Non (HTTP) เนื่องจากเป็นมาตรฐานที่ใช้งานกันทั่วไป และ ง่ายต่อการนำ Web Service ไปใช้งาน ส่วนรูปแบบอื่นๆ จะมีความซับซ้อนในการนำไปใช้งานมากกว่า

**Authentication Method**

**No Authentication** คือ เป็นการกำหนด Authentication โดยระบุค่า User Name/Password ไว้

**Transport Channel Authentication**

เป็นการกำหนดรูปแบบการตรวจสอบความถูกต้อง ในระดับ Transport Level Security โดยจะมีข้อมูลสำหรับตรวจสอบความถูกต้องไว้ที่ HTTP Header

* + User ID/password ใช้ User ID/Password ในการยืนยันความถูกต้อง
  + X.509 SSL client certificate ใช้ certificate ในการยืนยันความถูกต้อง
  + Single Sign On using SAP Assertion Ticket ใช้ Single Sign On ในการยืนยันความถูกต้อง ( Single Sign On เป็น SAP Security Product ที่ใช้สำหรับการตรวจสอบสิทธิ์การใช้งานระบบ )

**Message Authentication**

เป็นการกำหนดรูปแบบการตรวจสอบความถูกต้อง ในระดับ Message Level Security โดยจะมีข้อมูลสำหรับตรวจสอบความถูกต้องไว้ที่ SOAP Header ของแต่ละ Message ที่มีการรับส่ง

* + User ID/password ใช้ User ID/Password ในการยืนยันความถูกต้อง
  + X.509 certificate ใช้ certificate ในการยืนยันความถูกต้อง
  + Single Sign On using SAML ใช้ Single Sign On ในการยืนยันความถูกต้อง ( Single Sign On เป็น SAP Security Product ที่ใช้สำหรับการตรวจสอบสิทธิ์การใช้งานระบบ )

**คำแนะนำ**  **:**

การกำหนดรูปแบบการตรวจสอบความถูกต้อง ควรเป็นแบบ Transport ChannelAuthenticationเนื่องจากผู้ใช้งานไม่จำเป็นต้องมีความรู้ความเข้าใจเกี่ยวกับ มาตรฐานความปลอดภัยของ Web Services ( WS-Security ) แต่ Message Authentication ผู้ใช้งานจะต้องมีความเข้าใจ เกี่ยวกับ มาตรฐานความปลอดภัยของ Web Services ( WS-Security )

สำหรับการเลือกวิธีการยืนยันความถูกต้อง ควรเป็นแบบ User ID/Password เนื่องจาก X.509 certificate จะต้องมีการใช้ certificate ซึ่งจะมีขั้นตอนในการกำหนดยุ่งยากซับซ้อน (จำเป็นจะต้องศึกษาเพิ่มเติม) และ Single Sign On จะต้องมีการติดตั้ง Product ของ SAP เพิ่มเติมจึงจะสามารถใช้งานได้

**สรุปจากคำถามที่ส่งมา**

การเลือกใช้ Communication Security เป็น Non ( HTTP ) และ Authentication Method เป็น การเลือกใช้ Transport Channel Authentication โดยใช้ User ID/Password ในการยืนยันความถูกต้อง เป็นการเลือกใช้ที่เหมาะสมแล้ว

**คำแนะนำอื่นๆ เพิ่มเติม :**

……………………………………………………………………………………………………………………………………..

……………………………………………………………………………………………………………………………………..

……………………………………………………………………………………………………………………………………..