การวิเคราะห์ประสิทธิภาพการจัดความปลอดภัย ในระดับ MLS บนกริดสารสนเทศ
Performance Analysis of Message Level Security on "Information Grid": A Comprehensive Study

NECTEC-ACE 2010

23 กันยายน 2553

สุริยะ อุรุเอกโอฬาร เจษฎา เพ็งสุวรรณ

คำรณ อรุณเรื่อ และ นัยนา สหเวชชภัณฑ์

หน่วยปฏิบัติการวิจัยการจำลองขนาดใหญ่
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ประเทศไทย

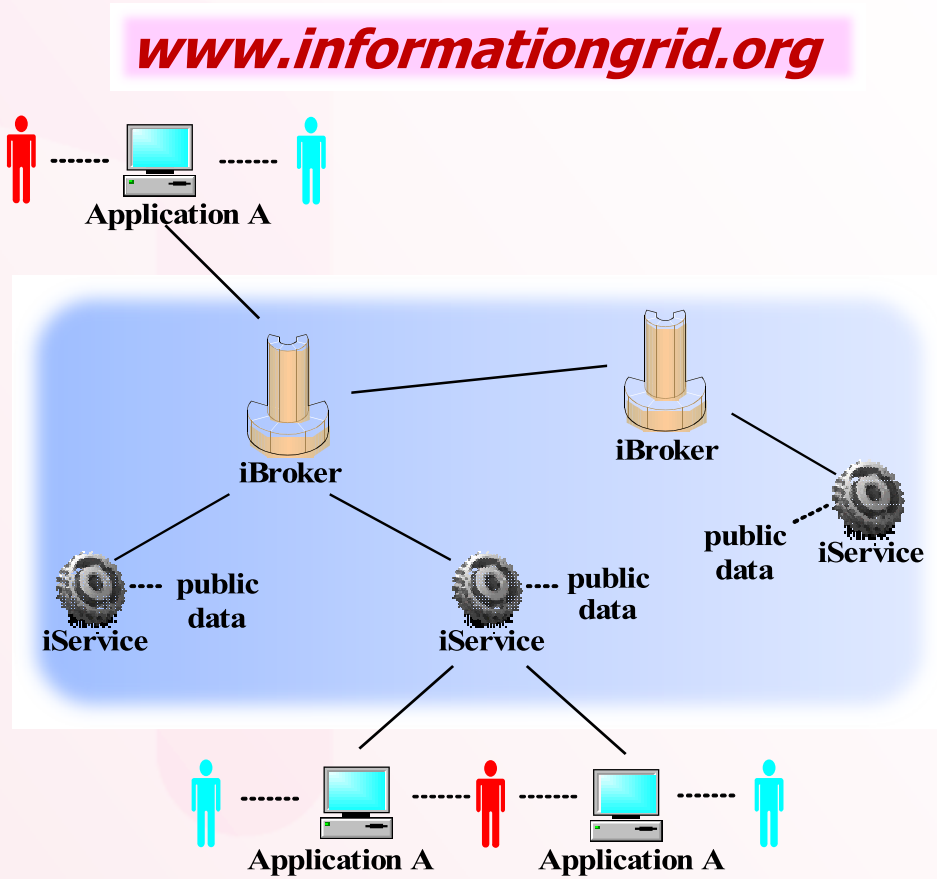
หัวข้อนำเสนอ

- บทนำ และการจัดการความปลอดภัยบนกริดสารสนเทศ
- เป้าหมาย และวัตถุประสงค์
- งานวิจัยที่เกี่ยวข้อง
- เทคโนโลยีที่เกี่ยวข้อง
- การออกแบบและพัฒนา
- การเตรียมการทดสอบ และการวัดประสิทธิภาพ
- ผลการทดสอบ
- สรุป

บทนำ

กริดสารสนเทศ

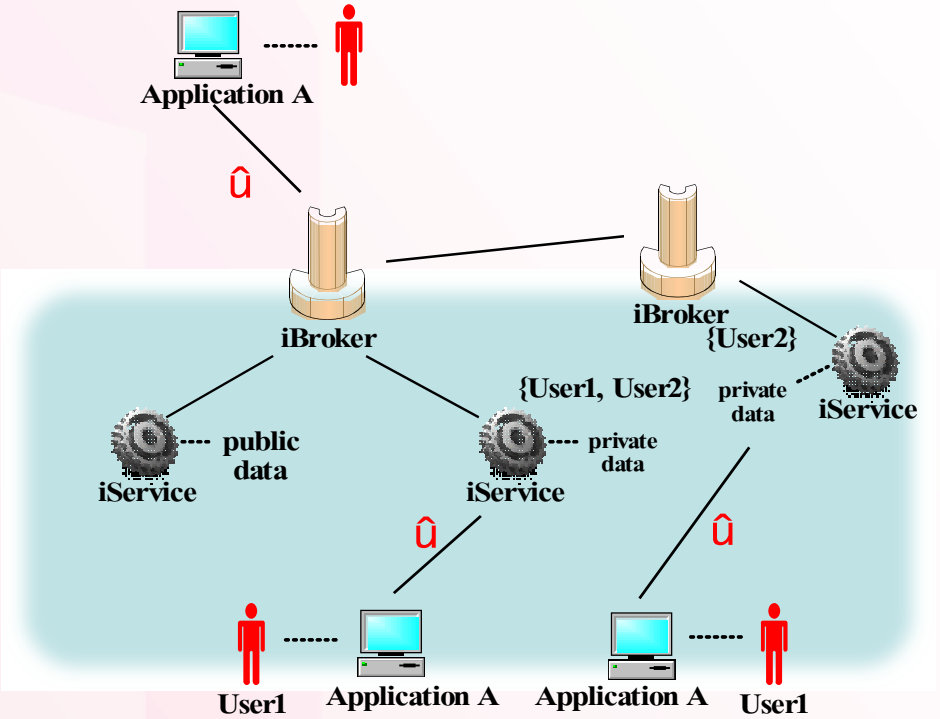
- โครงสร้างพื้นฐานที่ทำหน้าที่ในการสร้างแหล่งข้อมูลเสมือน และให้บริการการสืบค้นข้อมูล
  - ประกอบด้วยเครื่องแม่ข่ายอย่างน้อย 2 เครื่อง
    - เครื่องแม่ข่ายที่เป็นนายหน้าสำหรับสืบค้นข้อมูล (iBroker)
    - เครื่องแม่ข่ายที่ให้บริการจากแหล่งข้อมูลหนึ่งๆ (iService)
  - พัฒนาอยู่บนพื้นฐานของเทคโนโลยีเว็บเซอร์วิส
  - ข้อมูลที่ให้บริการเป็นข้อมูลแบบสาธารณะ (public data)



บทนำ

กริดสารสนเทศ

- แหล่งข้อมูลบางประเภทสามารถเปิดเผยได้เฉพาะกลุ่มบุคคลเท่านั้น
  - ข้อมูลสุขภาพ
  - ข้อมูลสิ่งแวดล้อม
- จำเป็นต้องเพิ่มขีดความสามารถของกริดสารสนเทศให้รองรับกับข้อมูลที่ไม่สามารถเปิดเผยแบบสาธารณะ (private data)



การจัดการความปลอดภัยบนกริดสารสนเทศ

	TLS/SSL	MLS
สภาวะแวดล้อม	point to point	endpoint to endpoint
การกำหนดข้อมูลที่ทำการเข้ารหัส	ทุกส่วน	ทุกส่วนและเฉพาะส่วน
ความน่าเชื่อถือของข้อมูล	ไม่มี	มี
ระดับการการันตีความลับ	Transport	Message
ประสิทธิภาพการทำงาน	ดี	ปานกลาง

เป้าหมาย และวัตถุประสงค์

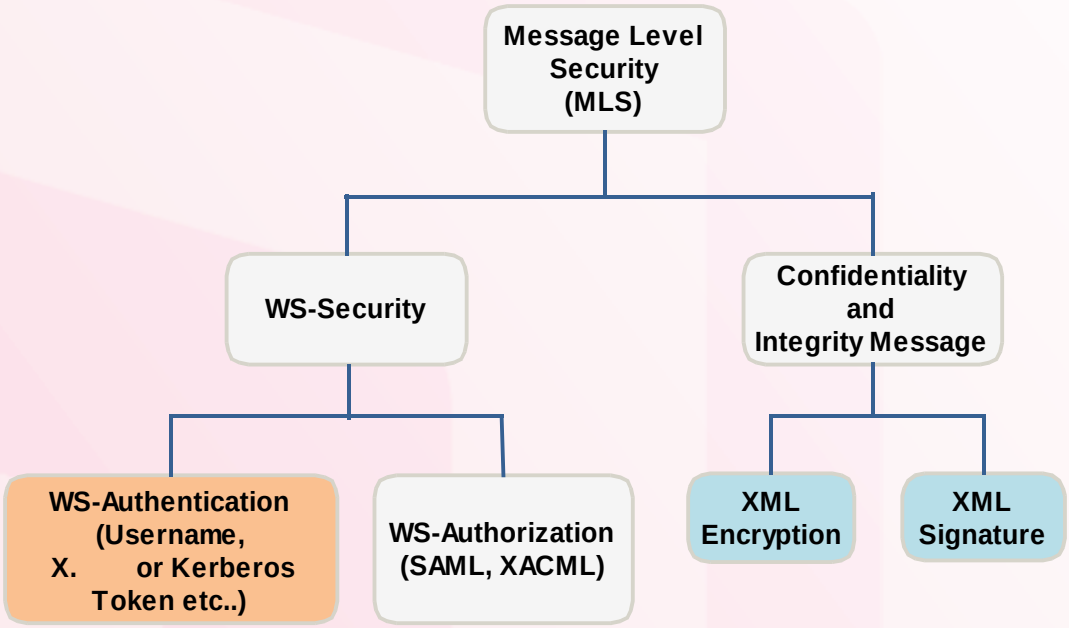
- **กริดสารสนเทศ**
  - **พัฒนาระบบความปลอดภัย MLS (Message Level Security) บนพื้นฐานของกริดสารสนเทศ**
    - การพิสูจน์ตัวตน (Authentication)
    - การอนุญาตเข้าใช้ทรัพยากร (Authorization)
    - การสร้างความน่าเชื่อของข้อมูล (Integrity)
    - การรักษาความลับของข้อมูล (Confidence)
- **บทความ**
  - **ศึกษาประสิทธิภาพการทำงานของกริดสารสนเทศ ร่วมกับการจัดการความปลอดภัยในระดับ MLS**
    - บนสภาพแวดล้อมแบบ endpoint to endpoint
    - มีการทำงานร่วมกับ IdP (Identity Provider)
      - การพิสูจน์ตัวตนในระดับข้อความโดยใช้ Security Token
      - การรักษาความลับและสร้างความน่าเชื่อถือของข้อมูลโดยใช้ XML-Encryption และ XML-Signature ตามลำดับ
    - รองรับการทำงานแบบ Single Sign-On (SSO)

งานวิจัยที่เกี่ยวข้อง

- A. Moralis, V. Pouli, M. Grammatikou, S. Papavassiliou and V. Maglaris, "Performance Comparison of Web Services Security: Kerberos token profile against X.509 token profile", In Proceedings of the Third International Conference on Networking and Services (ICNS), 2007, pp. 28-34.
  - ทดสอบประสิทธิภาพของ Security Token ระหว่าง X.509 กับ Kerberos
- K. Tang, S. Chen, D. Levy, J. Zic and B. Yan, "A Performance Evaluation of Web Services Security", In Proceedings of the 10th IEEE International Enterprise Distributed Object Computing Conference (EDOC'06), 2006, pp. 67-74.
  - การศึกษาประสิทธิภาพของอัลกอริทึมที่ใช้ในการสร้างลายเซ็นดิจิตอล และการเข้ารหัส-ถอดรหัสข้อมูลบนเทคโนโลยีเว็บเซอร์วิส
- *ไม่เพียงพอต่อการตัดสินใจ* เพื่อกำหนดเป็นแนวทางในการพัฒนาระบบความปลอดภัยในระดับ MLS บนกริดสารสนเทศ
  - มีการดำเนินการทดสอบอยู่สภาวะแวดล้อมแบบหนึ่งเครื่องแม่ข่ายต่อหนึ่งเครื่องลูกข่าย (point-to-point)
  - ไม่ได้มีการทำงานร่วมกับระบบ IdP
  - ไม่ได้มีสภาวะการทำงานแบบ SSO

เทคโนโลยีที่เกี่ยวข้อง

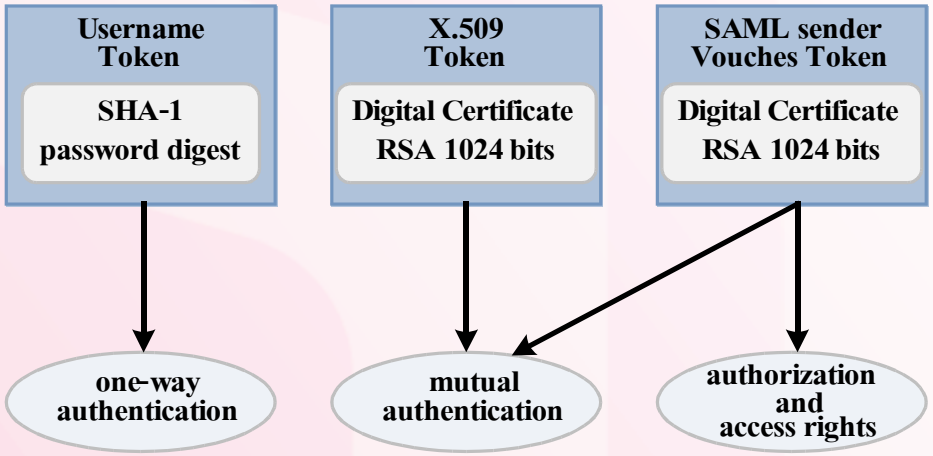
- ความปลอดภัยในระดับ MLS (Message Level Security)



- WS-Authentication ในส่วนของ Security Token กำหนดมาตรฐานโดย OASIS
- XML-Signature และ XML-Encryption กำหนดมาตรฐานโดย W3C

เทคโนโลยีที่เกี่ยวข้อง

- ความปลอดภัยในระดับ MLS (Message Level Security)
  - WS-Authentication: ***Security Token***



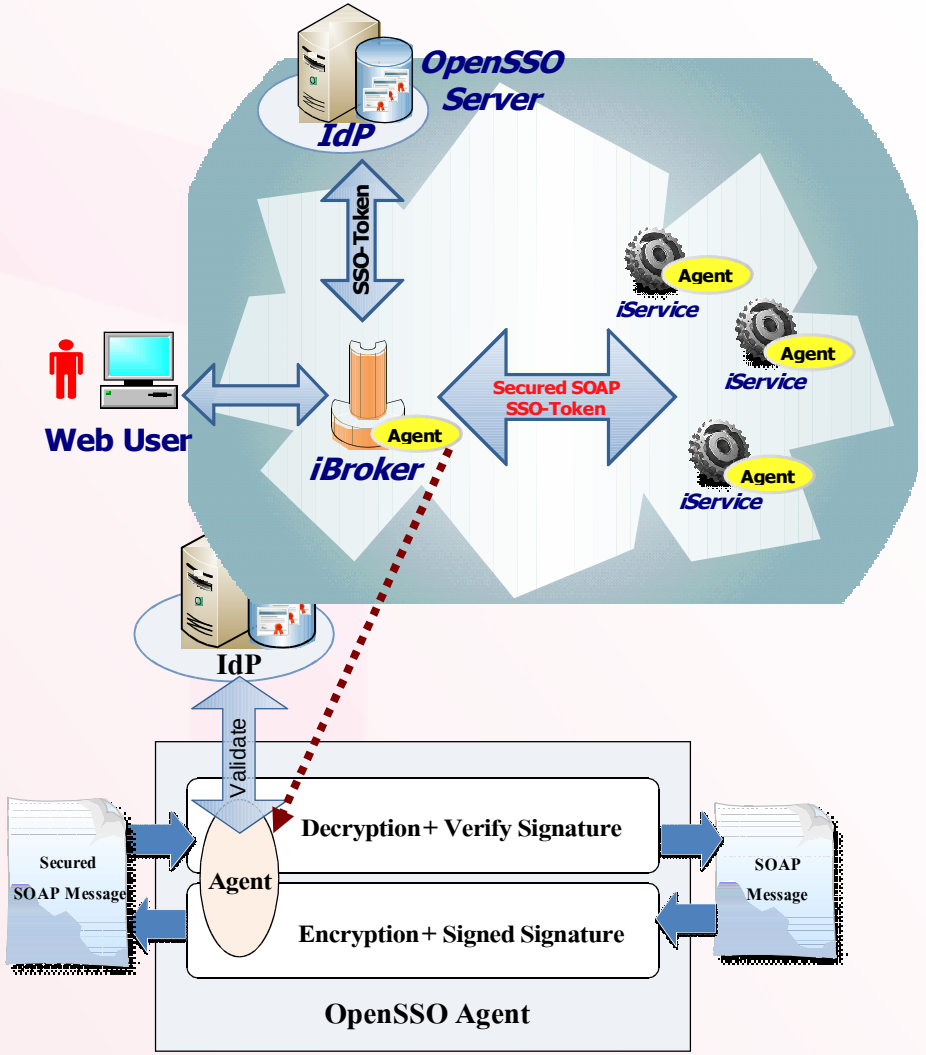
- อยู่ในส่วนของ *<soapenv:Header>*
- ป้องกันการปลอมตัวและการเลียนแบบครีเดนเชียล แต่ไม่รองรับการป้องกันการรักษาความลับและการบิดเบือนข้อมูล
- ใช้ XML-Encryption และ XML-Signature สำหรับรักษาความลับและการป้องกันการบิดเบือนข้อมูล ตามลำดับ

เทคโนโลยีที่เกี่ยวข้อง

- **ระบบ IdP (Identity Provider)**
  - บริหารจัดการ identity ของผู้ใช้งาน
  - มีกลไกการพิสูจน์ identity ของผู้ใช้งานแบบศูนย์กลาง
  - รองรับการจัดการความปลอดภัยในระดับ MLS
  - รองรับการกระบวนการทำงานแบบ SSO
  - สร้างกระบวนการความน่าเชื่อถือระหว่างเอนทิตี้ในระบบ
  - เครื่องมือสำหรับจัดการระบบ IdP
    - Shibboleth
    - JOSSO
    - OpenSSO

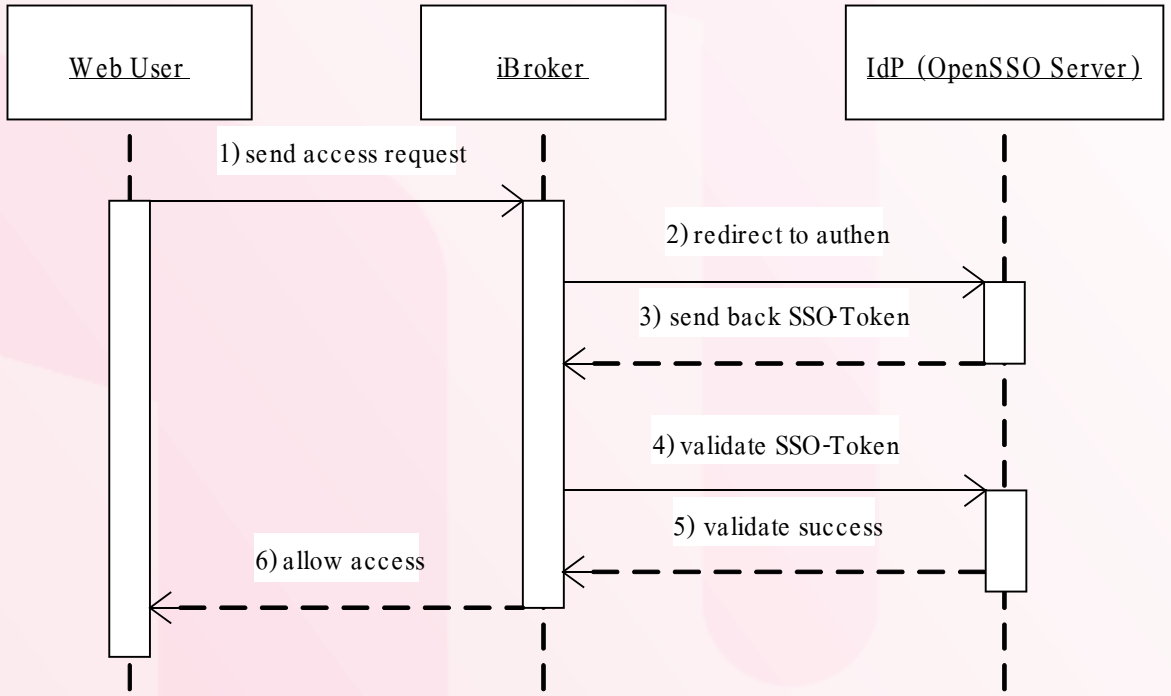
การออกแบบและพัฒนา

- **เลือกใช้ OpenSSO ทำหน้าที่เป็นระบบ IdP ซึ่งประกอบด้วย**
  - OpenSSO Server
    - บริหารจัดการและตรวจสอบ identity ของผู้ใช้งาน
    - สร้าง SSO-Token (user identity, sessionID, security token,encryption, signature และ timestamp)
  - OpenSSO agent
    - ตรวจสอบความถูกต้องของ SSO-Token
    - เข้ารหัส-ถอดรหัสข้อมูล
    - สร้างและตรวจสอบความถูกต้องของลายเซ็นดิจิตอล
    - ติดตั้งอยู่บน iBroker และ iService



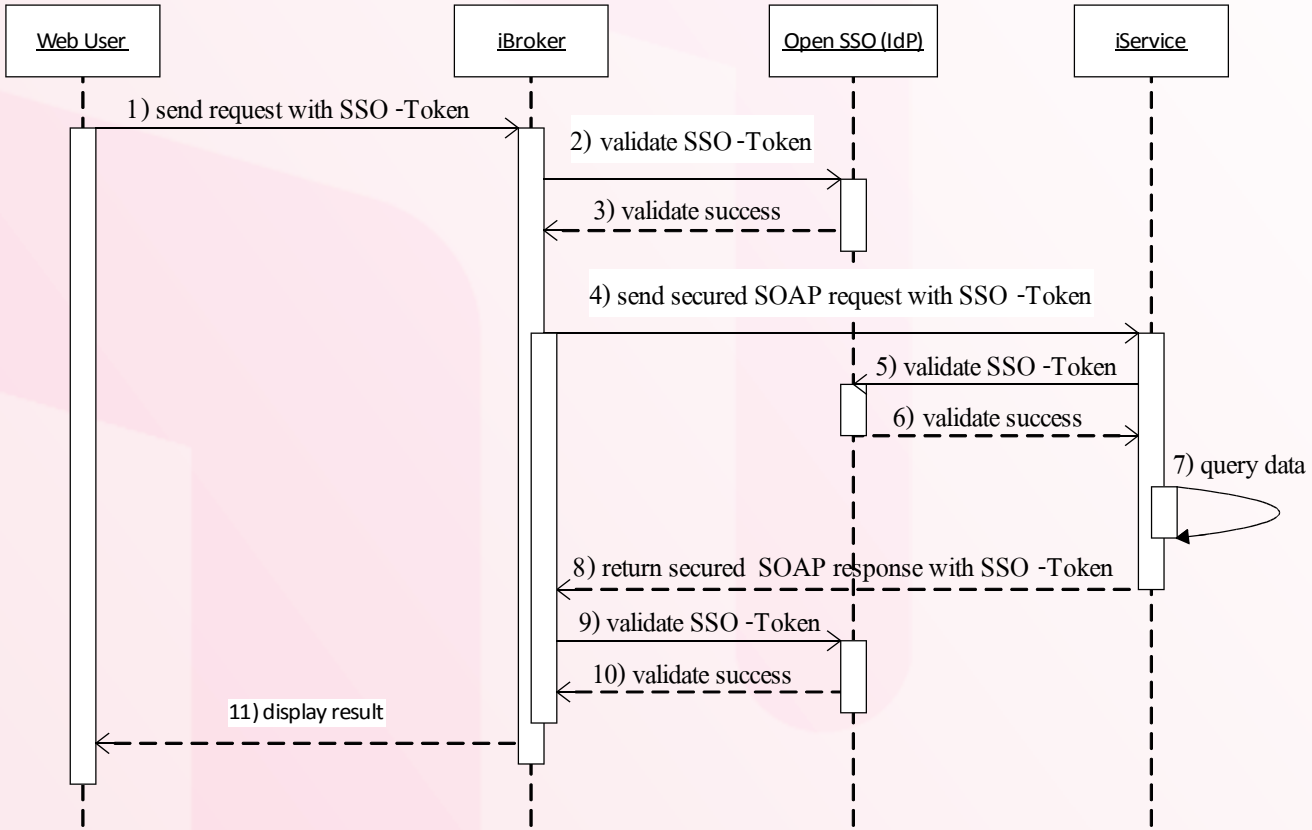
การออกแบบและพัฒนา

- **การทำงานของกริดสารสนเทศร่วมกับ OpenSSO Server และ Agent**
  - การพิสูจน์ตัวตน



การออกแบบและพัฒนา

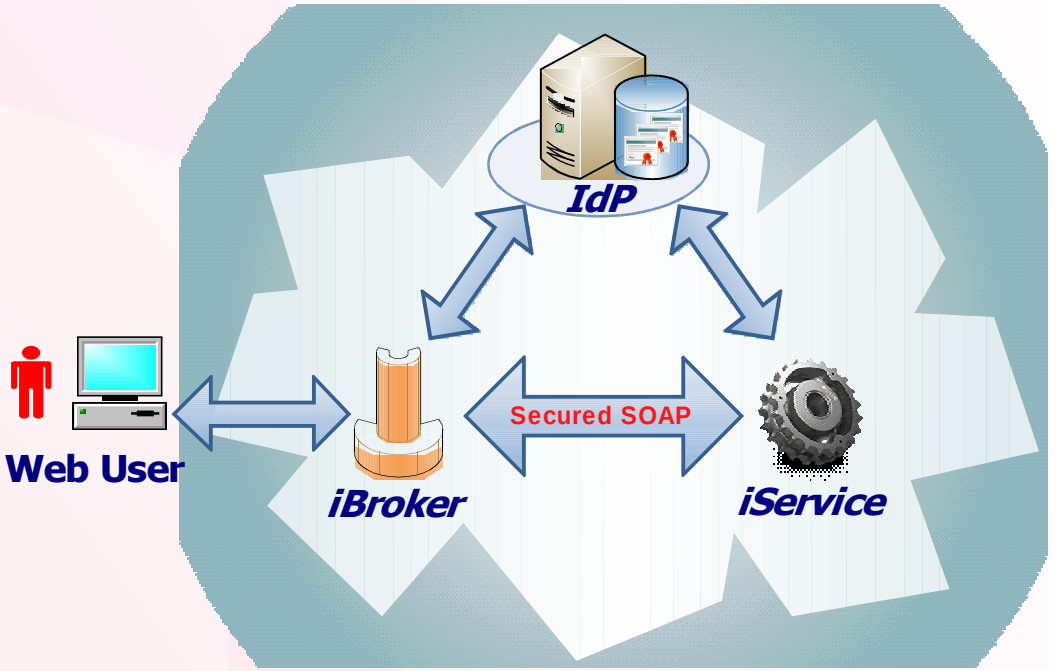
- **การทำงานของกริดสารสนเทศร่วมกับ OpenSSO Server และ Agent**
  - การเข้าถึงข้อมูล



การเตรียมการทดสอบประสิทธิภาพ

รายละเอียดฮาร์ดแวร์

ทรัพยากร	หน่วยประมวลผล	หน่วยความจำ	ความเร็วเครือข่าย
IdP (OpenSSO)	P4 3.0 GHz	1 GB	100 Mbps
Web User	P4 1.6 GHz	512 MB	
iBroker	P4 3 GHz	1GB	
iService	Xeon 1.6 GHz	256 MB	



รายละเอียดซอฟท์แวร์

- JAVA SE version 1.6
- Apache Axis 2 version 1.5.1
- OpenSSO version 8.1

การทดสอบประสิทธิภาพ

- ทดสอบประสิทธิภาพการทำงานของกริดสารสนเทศร่วมกับระบบ IdP บนสภาวะการทำงานแบบ SSO
- ประเมินการถดถอยประสิทธิภาพการทำงานของกริดสารสนเทศใน 5 กรณีดังนี้
  - Security Token
  - Security Token กับ XML-Signature
  - Security Token กับ XML-Encryption *<soapenv:Body>*
  - Security Token กับ XML-Encryption *<soapenv:Header,Body>*
  - Security Token กับ XML-Signature+XML-Encryption
- ขนาดของข้อมูลที่ให้บริการโดย *iService*
  - 1K, 10K และ 100K

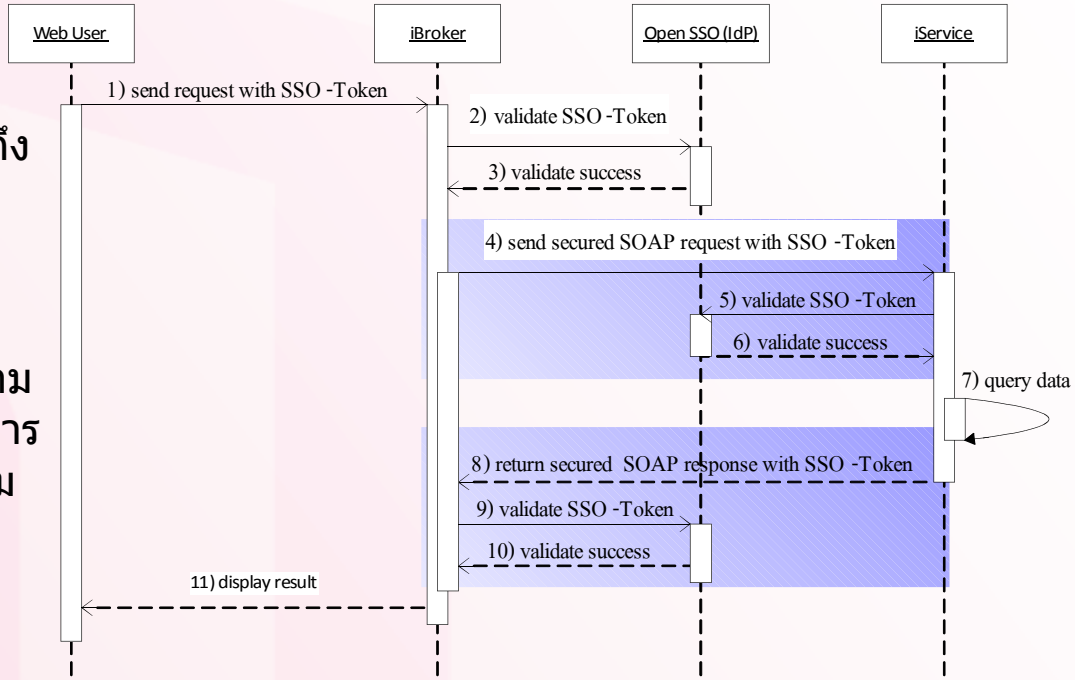
การวัดประสิทธิภาพการทำงาน

พิจารณาสองตัวชี้วัด

- เวลาในการเข้าถึงข้อมูล
  - เป็นเวลาที่ *iBroker* ใช้ในการเข้าถึงข้อมูล *iService*

- การถดถอยของประสิทธิภาพ
  - การเข้าถึงข้อมูลที่มีการจัดการความปลอดภัยในระดับ MLS เทียบกับการเข้าถึงข้อมูลที่ไม่มีการจัดการความปลอดภัยในระดับ MLS

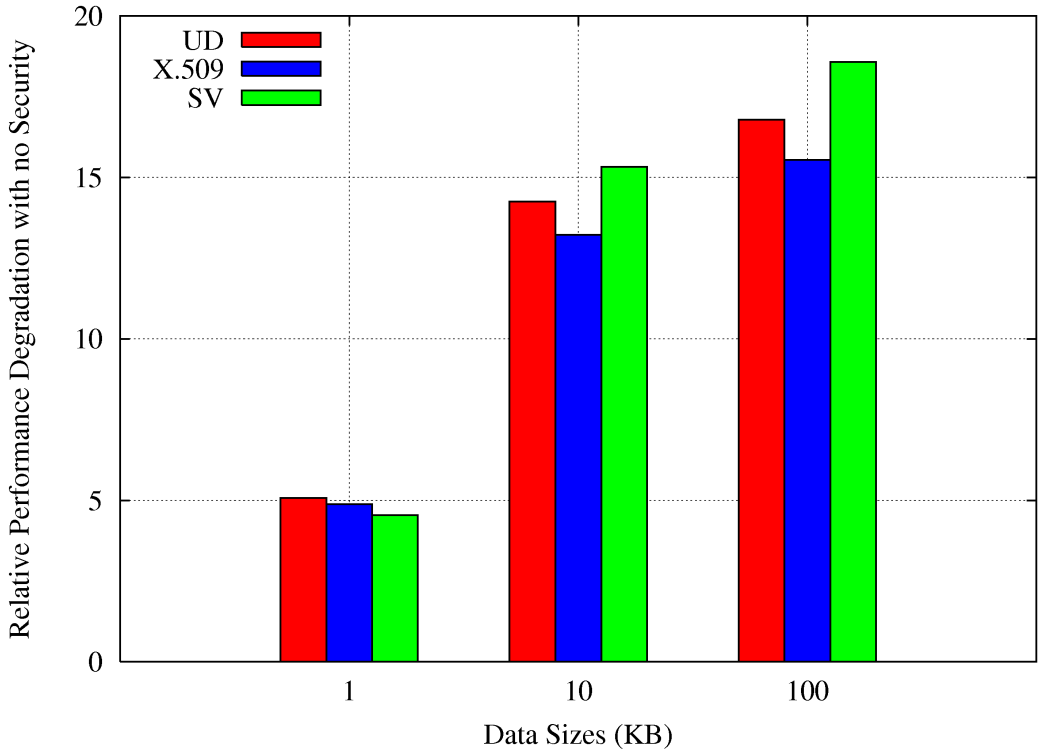
$$RTT_{\deg rade} = \frac{RTT_{\sec}}{RTT_{no\sec}} - 1$$



ผลการทดสอบประสิทธิภาพ

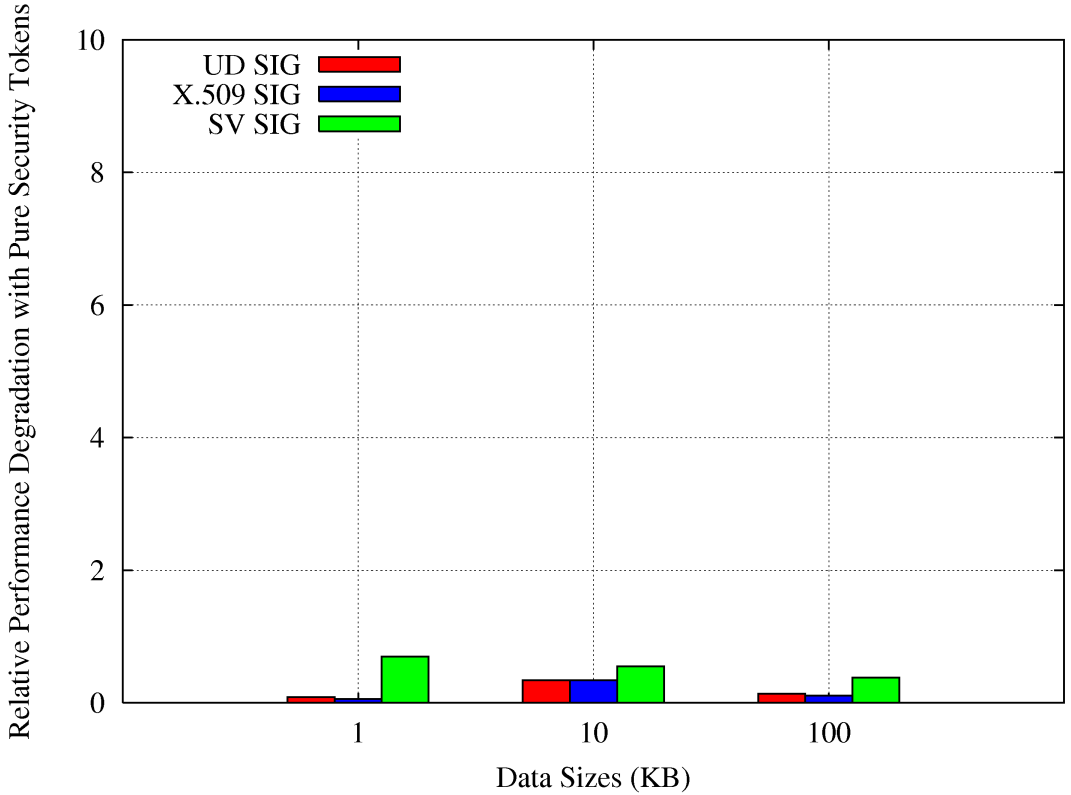
NECTEC
a member of NSTDA

» **กรณีที่ 1** การถดถอยของประสิทธิภาพการทำงานของกริดสารสนเทศ
  - **ทำงานร่วมกับ IdP และ Security Token**
  - **โดยประสิทธิภาพที่ได้สัมพัทธ์กับการทำงานของกริดสารสนเทศที่ไม่มีการจัดการความปลอดภัยในระดับ MLS**



ผลการทดสอบประสิทธิภาพ

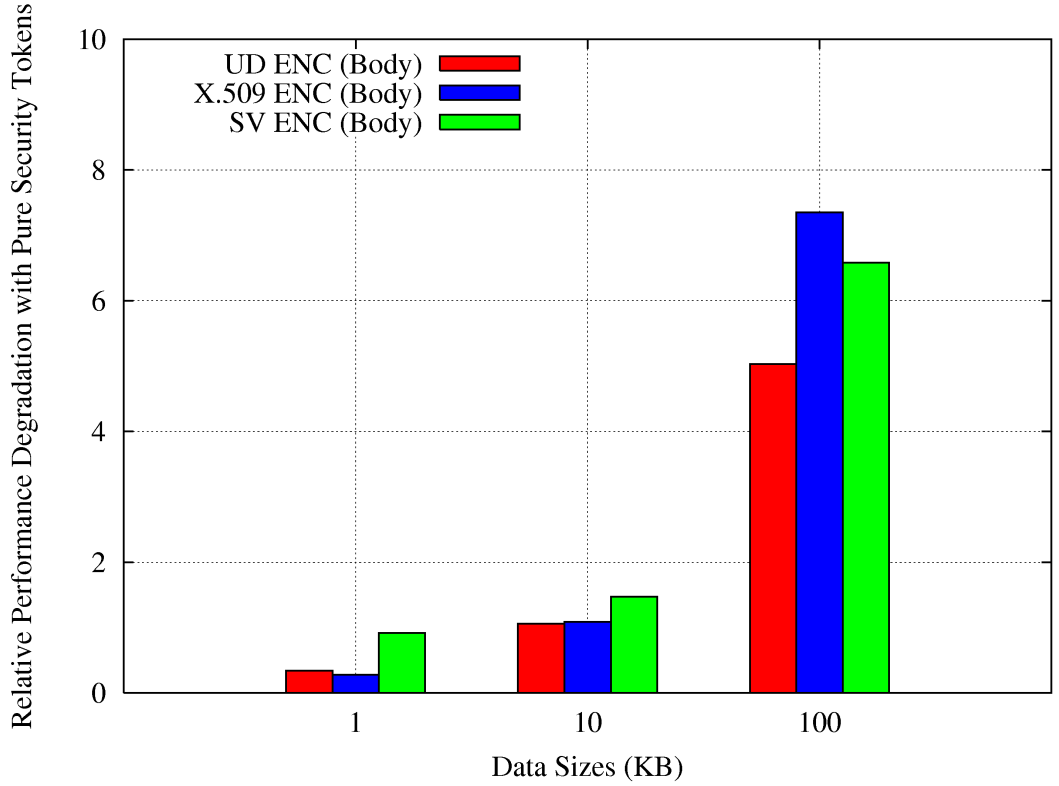
- **กรณีที่ 2** การถดถอยของประสิทธิภาพการทำงานของกริดสารสนเทศ
  - ทำงานร่วมกับ **IdP,Security Token** และ **XML-Signature**
  - โดยประสิทธิภาพที่ได้สัมพัทธ์กับการทำงานของกริดสารสนเทศใน ***กรณีที่ 1***



ผลการทดสอบประสิทธิภาพ

NECTEC
a member of NSTDA

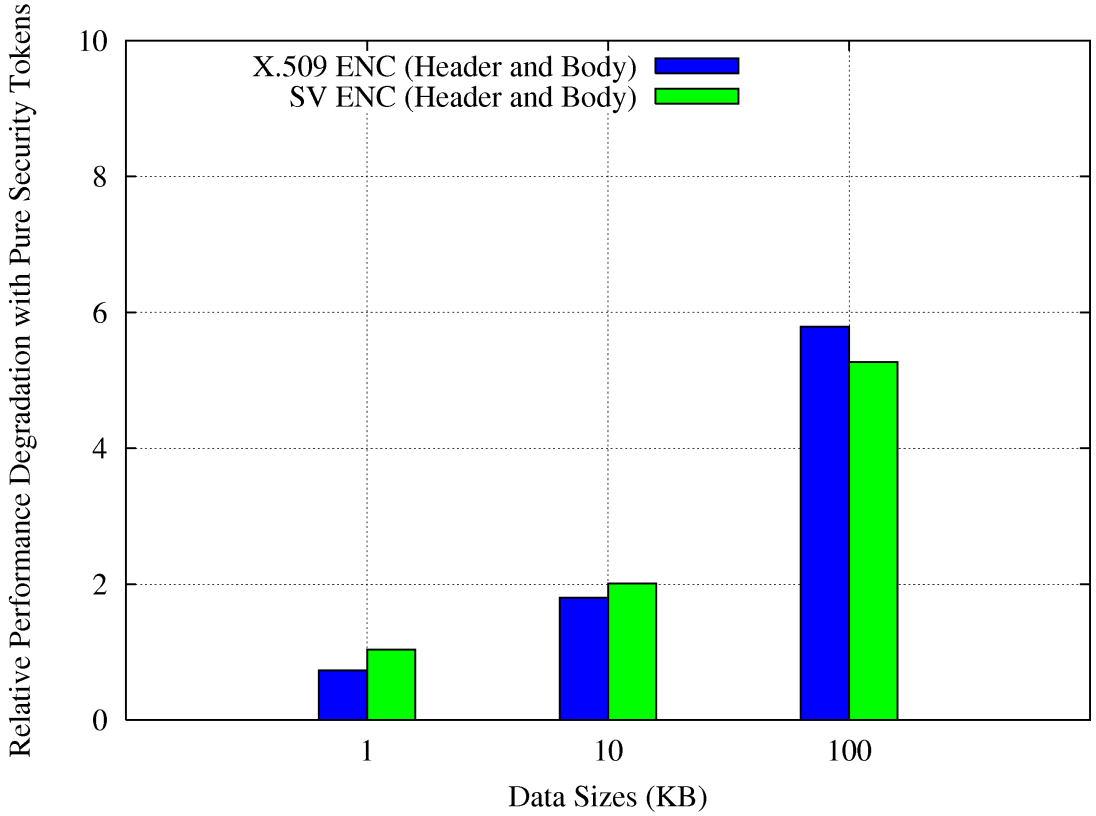
» **กรณีที่ 3** การถดถอยของประสิทธิภาพการทำงานของกริดสารสนเทศ
- ทำงานร่วมกับ **IdP, Security Token** และ **XML-Encryption** ***<soapenv:Body>***
- โดยประสิทธิภาพที่ได้สัมพันธ์กับการทำงานของกริดสารสนเทศใน ***กรณีที่ 1***



ผลการทดสอบประสิทธิภาพ

NECTEC a member of NSTDA

» **กรณีที่ 4** การถดถอยของประสิทธิภาพการทำงานของกริดสารสนเทศ
- ทำงานร่วมกับ **IdP,Security Token** และ **XML-Encryption** ***<soapenv:Header,Body>***
- โดยประสิทธิภาพที่ได้สัมพันธ์กับการทำงานของกริดสารสนเทศใน ***กรณีที่ 1***

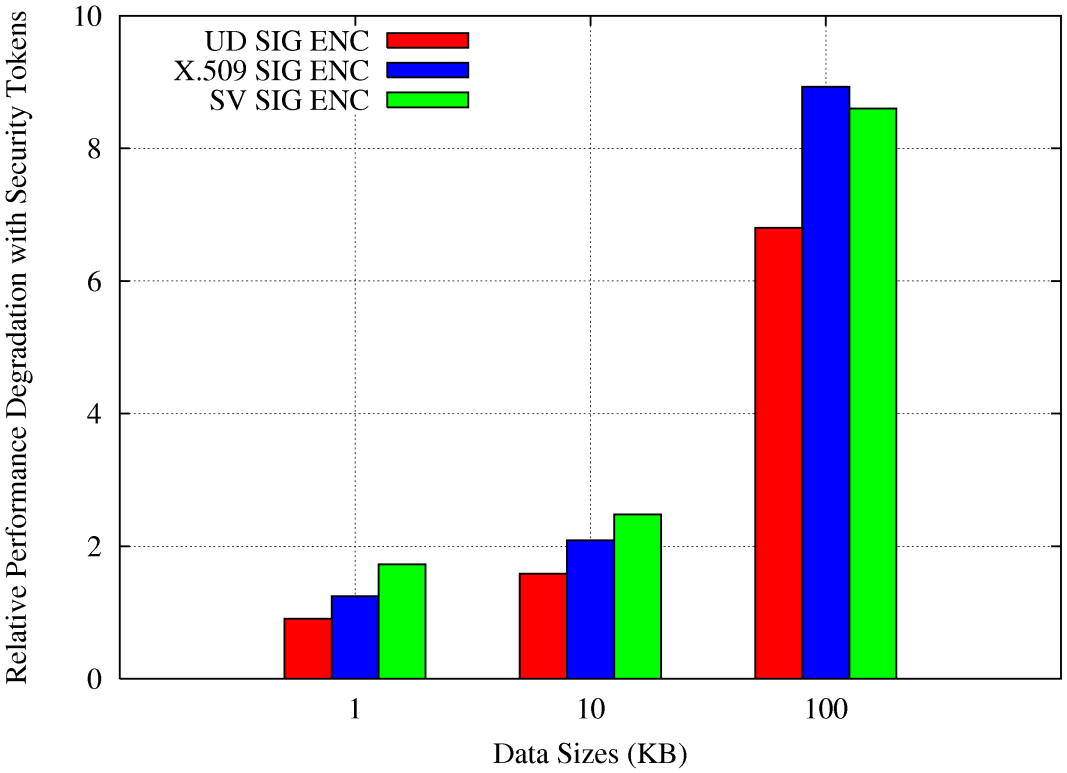


ผลการทดสอบประสิทธิภาพ

NECTEC a member of NSTDA

» **กรณีที่ 5** การถดถอยของประสิทธิภาพการทำงานของกริดสารสนเทศ

- ทำงานร่วมกับ **IdP,Security Token, XML-Signature และ XML-Encryption**
- **โดยประสิทธิภาพที่ได้สัมพัทธ์กับการทำงานของกริดสารสนเทศใน *กรณีที่ 1***



สรุป

- ออกแบบพัฒนาและประเมินประสิทธิภาพของกริดสารสนเทศร่วมกับการจัดการความปลอดภัยในระดับ MLS
  - ภายใต้สภาพแวดล้อมแบบ endpoint to endpoint และ SSO ที่มีการทำงานร่วมกับระบบ IdP
  - ทดสอบการใช้งาน Security Token ร่วมกับ XML-Signature และ XML-Encryption
    - Security Token แบบ SAML sender Vouches มีคุณภาพที่เหมาะสมสำหรับใช้ในการพิสูจน์ตัวตนมากกว่าแบบ UD และ X.509
      - ส่งผลกระทบต่อการทำงานของกริดสารสนเทศโดยรวมไม่ต่างจากแบบ UD และ X.509
      - รองรับการอนุญาตและสิทธิ์ในการเข้าใช้ข้อมูลในระดับ Token
      - สามารถทำลายเซ็นดิจิตอลในระดับ Token ได้
    - XML-Encryption ทำให้ประสิทธิภาพการทำงานของกริดสารสนเทศถดถอยมาก แต่สำหรับ XML-Signature ส่งผลกระทบเพียงเล็กน้อย