แนวทางการเข้าถึงระบบบริการอิเล็กทรอนิกส์แบบรวมศูนย์ (Single Sign-On)

EGA
e-Government Agency

การเข้าถึงระบบบริการอิเล็กทรอนิกส์แบบรวมศูนย์ (Single Sign-On) คืออะไร?

- คือ ความสามารถของระบบการยืนยันตัวบุคคล (Authentication Service) ที่รองรับการให้ผู้ใช้งานลงชื่อเข้าใช้งานระบบ (Login) ครั้งเดียว แล้วสามารถเข้าใช้งานระบบหลายระบบได้ โดยไม่ต้องลงชื่อเข้าใช้งานซ้ำอีก

EGA
e-Government Agency

การเข้าถึงระบบบริการอิเล็กทรอนิกส์แบบรวมศูนย์ (Single Sign-On) คืออะไร?

- ประชาชน และเจ้าหน้าที่หน่วยงานภาครัฐสามารถเข้าถึงระบบสารสนเทศต่าง ๆ ของรัฐ ทั้งที่เป็นระบบบริการอิเล็กทรอนิกส์ภาครัฐ (e-Services) และระบบงานภายในของรัฐ (Back Office) ได้โดย Login เพียงครั้งเดียว แล้วสามารถเข้าใช้งานระบบหลายระบบได้โดยไม่ต้องลงชื่อเข้าใช้งานซ้ำอีก

เป้าหมาย

- ผู้ใช้งานทั้งที่เป็นประชาชนทั่วไป และเจ้าหน้าที่หน่วยงานภาครัฐ สามารถเข้าถึงบริการอิเล็กทรอนิกส์ต่างๆ ของหน่วยงานภาครัฐได้ โดยอาศัยหลักฐานอ้างอิง (Authentication Credential) ชุดเดียว โดยหลักฐานอ้างอิงดังกล่าวอาจเป็น Login/Password หรือ (ในอนาคต) Smart Card, ใบรับรองอิเล็กทรอนิกส์ ฯลฯ

เป้าหมาย

- ก้าวหนึ่งใน e-Government Cloud: Authentication Service

  หน่วยงานภาครัฐไม่จำเป็นที่จะต้องพัฒนาระบบสำหรับยืนยันตัวบุคคลด้วยตนเอง

  ลดค่าใช้จ่ายในการพัฒนาและดูแลรักษาฐานข้อมูลผู้ใช้งาน และระบบการ

EGA
e-Government Agency

แนวทางการเข้าถึงระบบบริการอิเล็กทรอนิกส์แบบรวมศูนย์ (Single Sign-On)

ลักษณะการทำงานของระบบ

EGA
e-Government Agency

องค์ประกอบหลักที่เกี่ยวข้อง

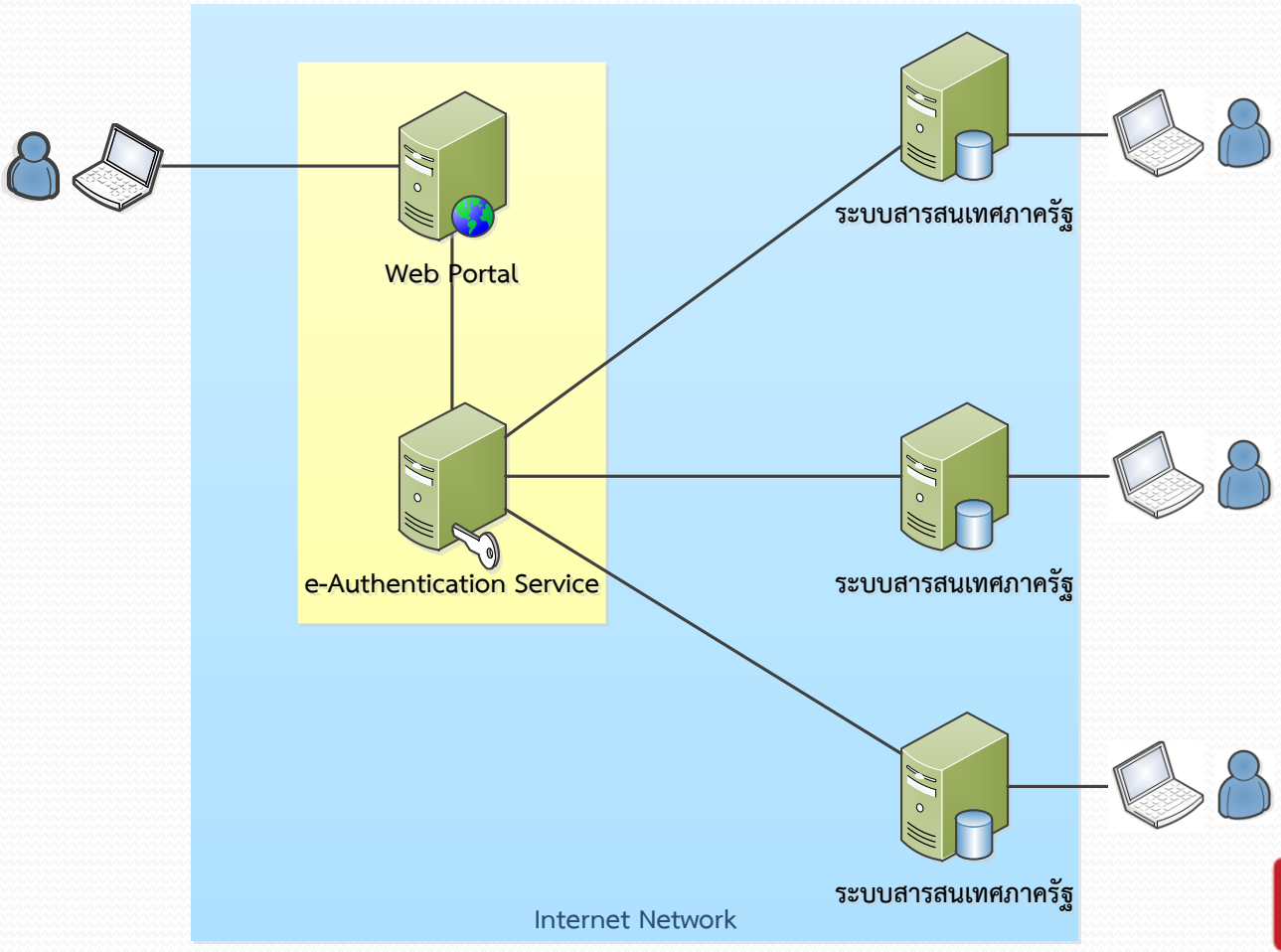
- **เว็บไซต์ท่าสำหรับเข้าเข้าถึงข้อมูลและระบบงานต่าง ๆ ของภาครัฐ (Web Portal)**
  - ระบบเว็บไซต์กลางบริการอิเล็กทรอนิกส์ภาครัฐ (e-Government Portal) ซึ่งรวบรวมข้อมูลและบริการต่าง ๆ สำหรับประชาชนทั่วไป (http://www.egov.go.th)
  - เว็บไซต์หน่วยงาน ซึ่งมักจะรวบรวมลิงค์ไปยังระบบงานต่าง ๆ ที่เจ้าหน้าที่ของหน่วยงานนั้น ๆ จำเป็นต้องใช้ อาทิเช่น ระบบเว็บเมล์ ระบบอินทราเน็ต หรือระบบงานภายในอื่น ๆ เป็นต้น
- **ระบบยืนยันตัวบุคคลกลาง (e-Authentication Service)**
  - เป็นระบบที่ใช้ในการยืนยันตัวบุคคล**โดยอาศัยหลักฐาน**อ้างอิง (Authentication Credential) ที่เหมาะสม โดยหลักฐานอ้างอิงดังกล่าวอาจเป็น Login/ Password หรือในอนาคตอาจเป็น One Time Password หรือใบรับรองอิเล็กทรอนิกส์ก็ได้ (http://openid.egov.go.th)
  - กรณีเจ้าหน้าที่รัฐที่ใช้บริการระบบ MailGoThai (http://govid.egov.go.th)

EGA
e-Government Agency

องค์ประกอบหลักที่เกี่ยวข้อง (ต่อ)

- **ระบบสารสนเทศภาครัฐ ครอบคลุมถึงระบบต่าง ๆ ดังนี้**
  - ระบบบริการอิเล็กทรอนิกส์ภาครัฐ (e-Service) หมายถึงระบบของหน่วยงานภาครัฐซึ่งให้บริการอิเล็กทรอนิกส์สำหรับประชาชน ผู้ประกอบการ หรือชาวต่างชาติ โดยบริการดังกล่าวอาจจะเป็นในลักษณะของการให้ข้อมูล (Information) มีการปฏิสัมพันธ์กับประชาชน (Interaction) รองรับการดำเนินธุรกรรมภาครัฐ (Interchange Transaction) หรืออยู่ในระดับของการบูรณาการ (Integration) ก็ได้
  - ระบบงานภายในของภาครัฐ (Back Office) หมายถึง ระบบของหน่วยงานภาครัฐซึ่งใช้ในการบริหารจัดการ สนับสนุนงานตามภารกิจของหน่วยงาน อาทิเช่น ระบบบัญชี ระบบบริหารงานบุคคล ระบบงบประมาณ ระบบยุทธศาสตร์ แผนงาน โครงการ เป็นต้น

สถาปัตยกรรมในภาพรวม

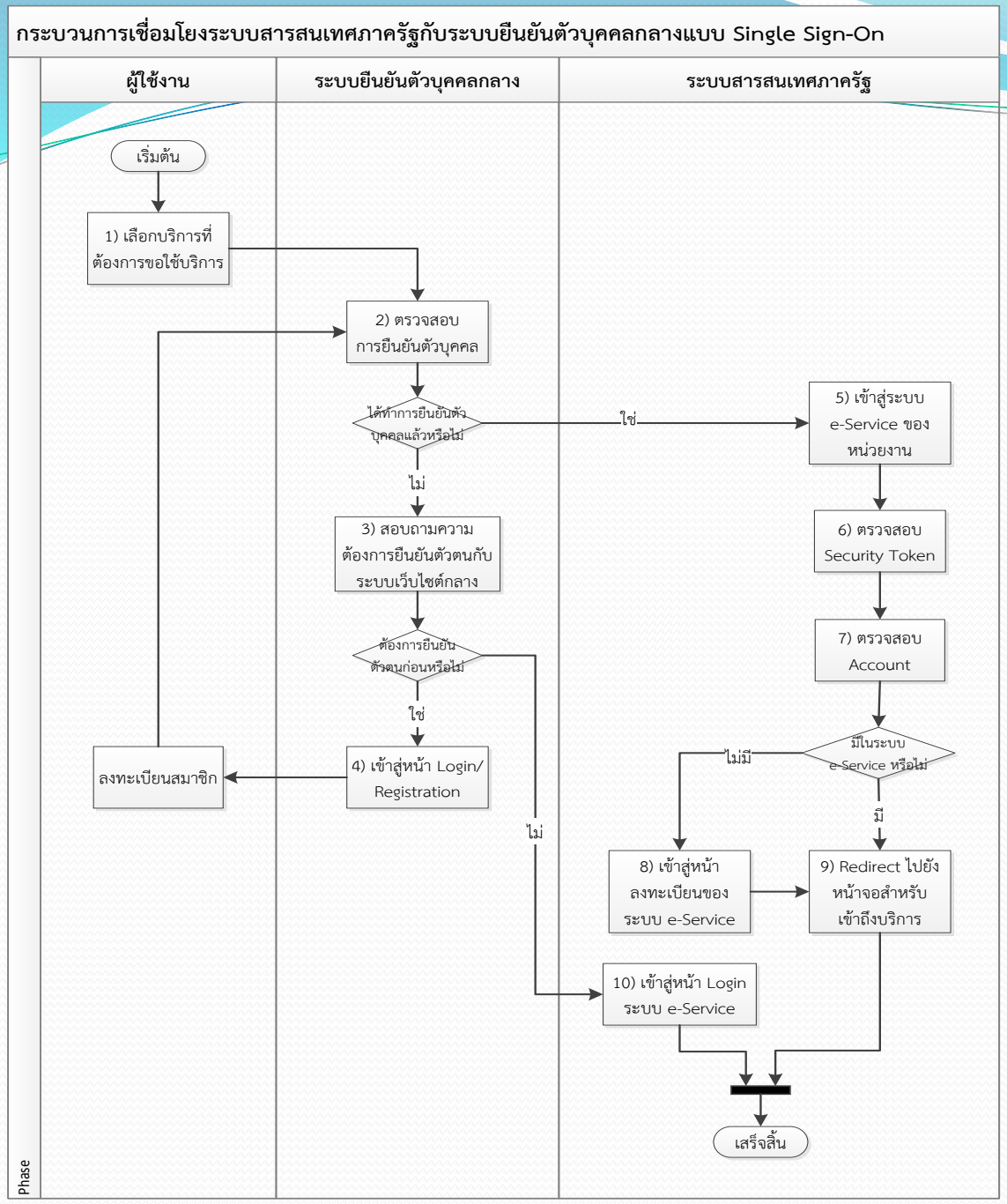


ประเภทของผู้ใช้ที่รองรับ

- **ระบบยืนยันตัวบุคคลกลางรองรับผู้ใช้งาน 5 ประเภท ดังนี้**

	ประเภทผู้ใช้ที่รองรับ	วิธีการสมัครเพื่อขอใช้งาน
1	ประชาชน/ บุคคลธรรมดา	สมัครด้วยตนเองแบบออนไลน์
2	นิติบุคคล	สมัครด้วยตนเองแบบออนไลน์
3	ชาวต่างชาติ	สมัครด้วยตนเองแบบออนไลน์
4	ข้าราชการ/ เจ้าหน้าที่รัฐที่ไม่มีบัญชีผู้ใช้งานอยู่กับระบบ MailGoThai	สมัครด้วยตนเองแบบออนไลน์
5	ข้าราชการ/ เจ้าหน้าที่รัฐที่มีบัญชีผู้ใช้งานอยู่กับระบบ MailGoThai	1) หน่วยงานต้นสังกัดสมัครขอใช้บริการ MailGoThai กับ สรอ. 2) เจ้าหน้าที่ขอบัญชีผู้ใช้งานกับผู้ดูแลระบบของหน่วยงาน

EGA
e-Government Agency



ขั้นตอนการทำงานของการเชื่อมโยงระบบสารสนเทศภาครัฐแบบ Single Sign-On

EGA
e-Government Agency

แนวทางการเข้าถึงระบบบริการอิเล็กทรอนิกส์แบบรวมศูนย์ (Single Sign-On)

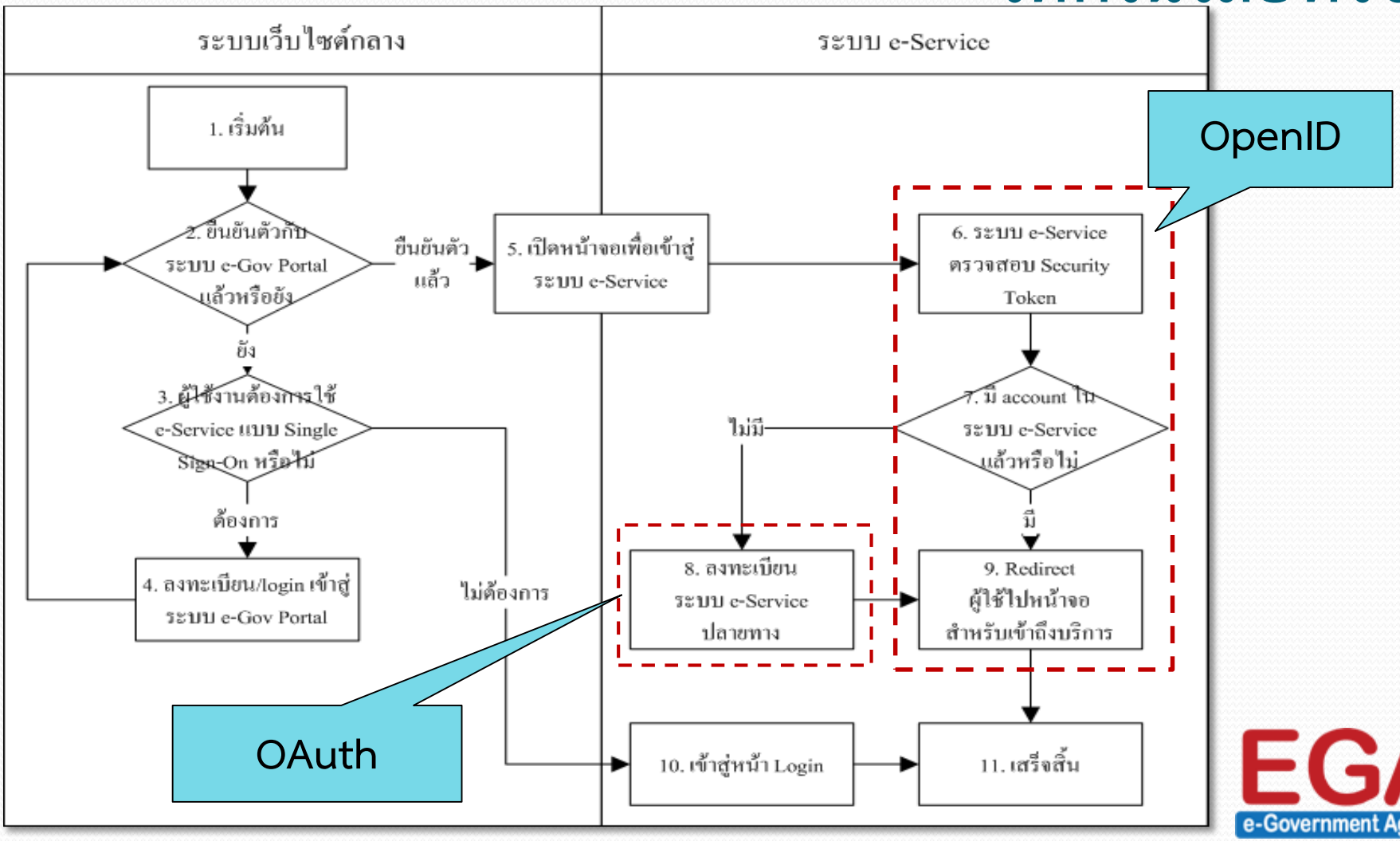
เทคโนโลยีที่ใช้

EGA
e-Government Agency

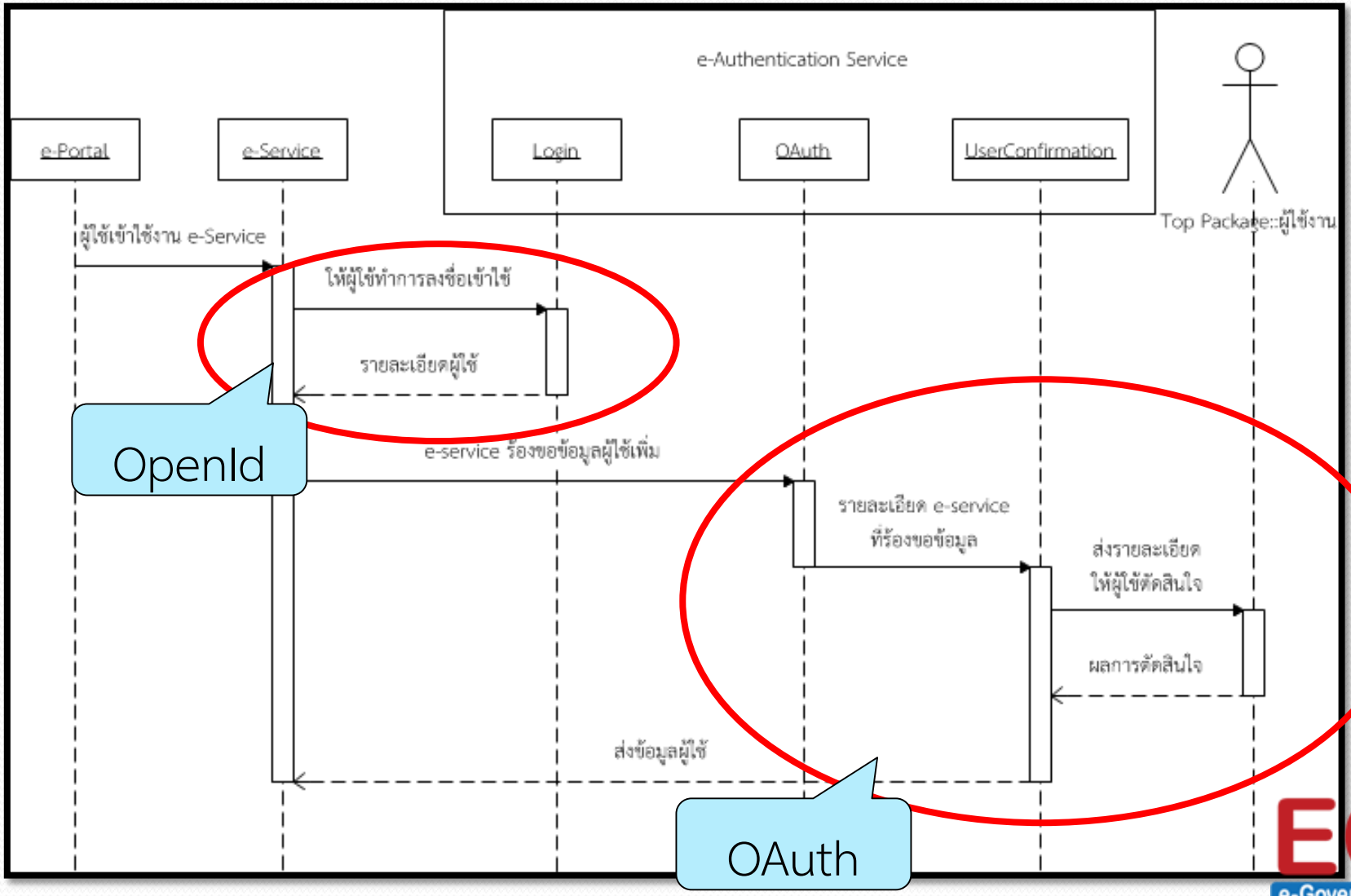
เทคโนโลยีที่ใช้

- OpenId : ใช้ในการยืนยันตัวบุคคล
  - สรอ. ได้พัฒนาระบบยืนยันตัวบุคคลกลาง (OpenId Provider) ขึ้นมาเพื่อให้ระบบสารสนเทศภาครัฐ (e-service) สามารถตรวจสอบ และอนุญาตให้ผู้ใช้ที่ยืนยันตัวตนแล้วสามารถเข้าใช้ระบบสารสนเทศภาครัฐ (e-service) ได้
  - ในการใช้งานระบบยืนยันตัวบุคคลกลาง ระบบสารสนเทศภาครัฐ (e-service) ต้องทำการพัฒนาชุดคำสั่งหรือระบบ (OpenId Relying Party) ในการส่งและรับข้อมูลจากระบบยืนยันตัวบุคคลกลาง
- OAuth : ใช้ในการร้องขอข้อมูลส่วนตัวของผู้ใช้บริการ
  - ระบบสารสนเทศภาครัฐ (e-service) ต้องทำการพัฒนาชุดคำสั่งหรือระบบ (OAuth Consumer) เพื่อใช้ในการร้องขอข้อมูลผู้ใช้จากระบบข้อมูลผู้ใช้ (OAuth Provider) ที่อยู่ภายใต้ระบบยืนยันตัวบุคคลกลาง โดยระบบจะส่งข้อมูลกลับมาในรูปแบบของ xml

เทคโนโลยีที่ใช้



ขั้นตอนการทำงานที่เกิดขึ้น



เว็บต่างประเทศที่ใช้ OpenID และ OAuth

- OpenID (http://openid.net/get-an-openid/)
  - Google
  - Yahoo
- OAuth
  - Facebook (http://developers.facebook.com/docs/reference/dialogs/oauth/)
  - Twitter (https://dev.twitter.com/docs/auth/oauth)

แนวทางการเข้าถึงระบบบริการอิเล็กทรอนิกส์แบบรวมศูนย์ (Single Sign-On)

OpenID

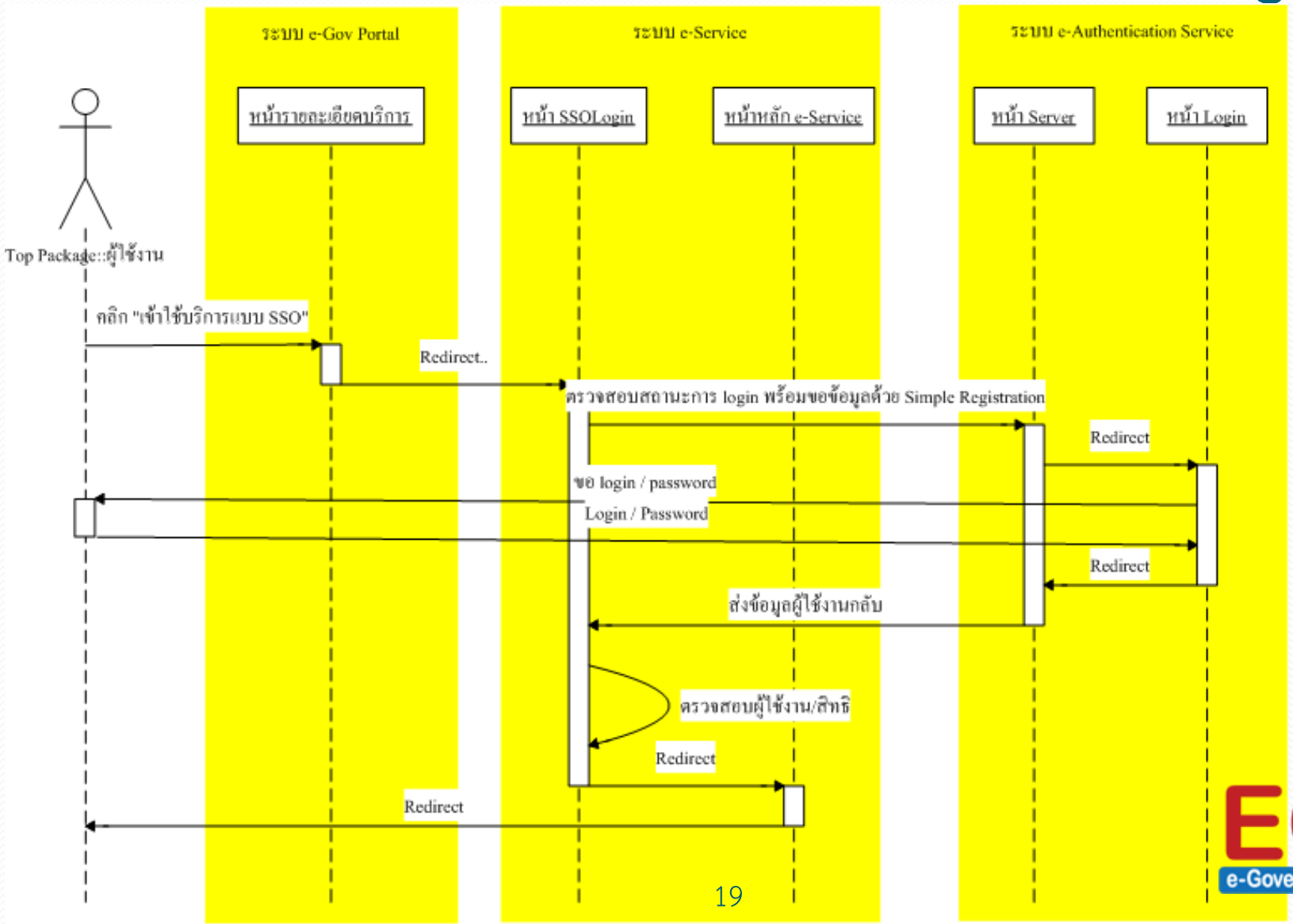
EGA
e-Government Agency

องค์ประกอบหลักที่เกี่ยวข้อง

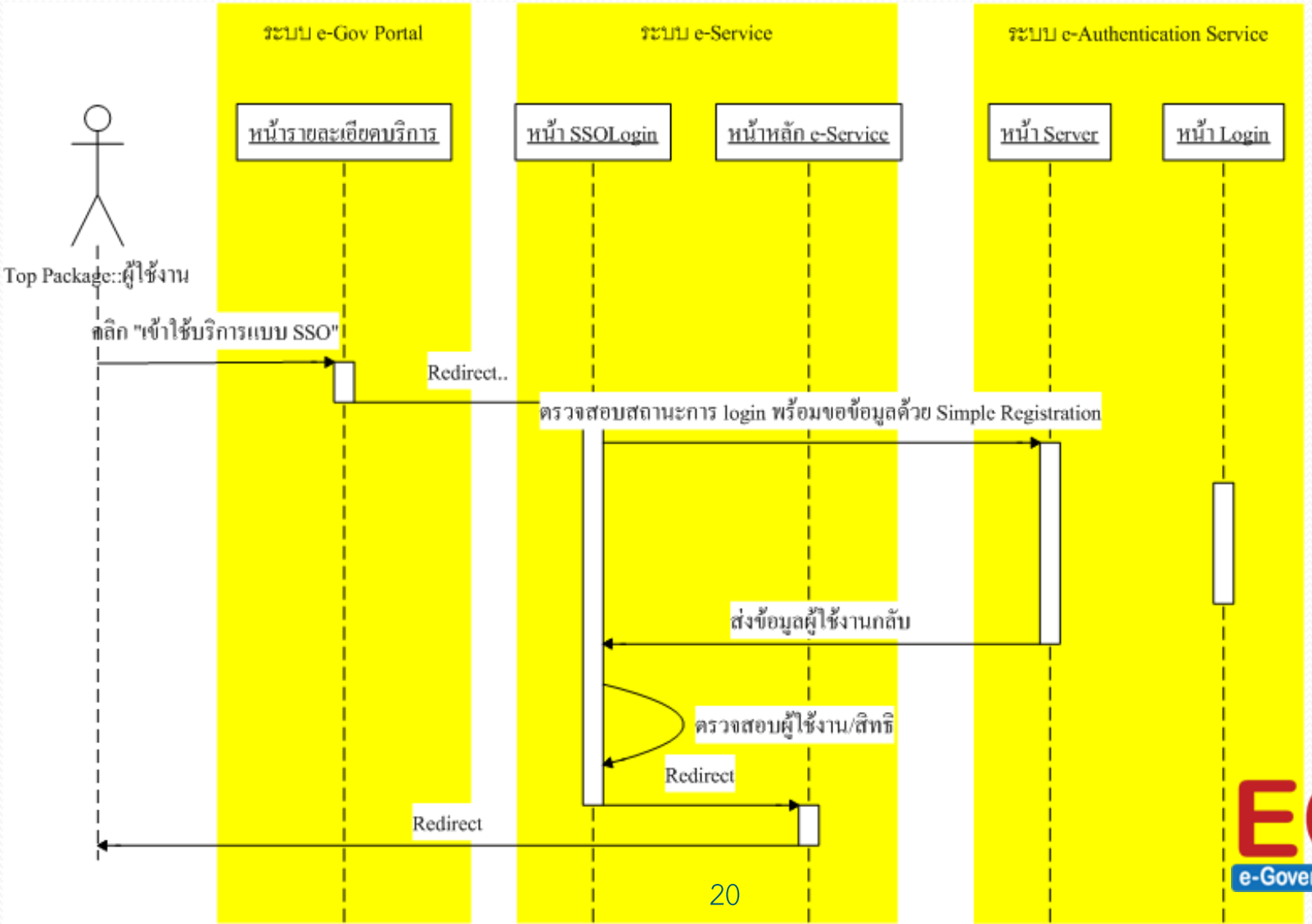
- ฝั่งระบบสารสนเทศภาครัฐ “OpenID Relying Party”
  - หน้าเว็บเพจ SSOLogin
  - ไลบรารี่สำหรับรองรับการใช้งาน OpenID 2.0 ตามภาษาที่ใช้พัฒนาระบบ (PHP, Java, ASP.NET)
- ฝั่งระบบยืนยันตัวบุคคลกลาง “OpenID Provider”
  - หน้าเว็บ openid.egov.go.th (govid.egov.go.th สำหรับเจ้าหน้าที่รัฐที่ใช้บริการ MailGoThai)

EGA
e-Government Agency

ขั้นตอนการทำงาน (กรณียังไม่ได้ login)



ขั้นตอนการทำงาน (กรณี login แล้ว)



OpenID Request

- เป็นการ Request ขอใช้งาน OpenID กับ OpenID Provider
- HTTP GET Request
- OpenID end point ของสรอ. อยู่ที่ https://openid.egov.go.th (https:govid.egov.go.th กรณีเจ้าหน้าที่รัฐ ที่ใช้บริการ MailGoThai)
- ใน Request จะต้องแนบ OpenID parameter ไปด้วย
  - Basic Parameter
  - Attribute Exchange Extension Parameter
- Character Encoding ต้องใช้ Utf8
- HTTP Encode

EGA
e-Government Agency

ตัวอย่าง Request

http://openid.egov.go.th/server.aspx?openid.claimed_id=http://specs.openid.net/auth/2.0/identifier_select&openid.identity=http://specs.openid.net/auth/2.0/identifier_select&openid.assoc_handle=nixR!IAAAAB56GYx_ecAUdoR3qhyvqAi9MZxO-Ahl00nqoeUcrtnQQQAAAAGNVREK0g4S_Zb8IgSlb96sYGjE4AYbsk GBPXGmwQ3yrBvH2CmwGL6bIW_6m2Ibh0cN5Zt5rl0hhM4hvHj6HDlZ&openid.return_to=http://localhost:4856/loginProgrammatic.aspx?dnoa.userSuppliedIdentifier=http%3A%2F%2Flocalhost%3A1807%2FEGA.EGA_CAS.Security.eAuthen%2F&openid.realm=http://localhost:4856/&openid.mode=checkid_setup&openid.ns=http://specs.openid.net/auth/2.0&openid.ns.alias3=http://openid.net/srv/ax/1.0&openid.alias3.required=alias1,alias2,alias3,alias4&openid.alias3.mode=fetch_request&openid.alias3.type.alias1=http://axschema.org/contact/email&openid.alias3.count.alias1=1&openid.alias3.type.alias2=http://axschema.org/namePerson&openid.alias3.count.alias2=1&openid.alias3.type.alias3=http://axschema.org/namePerson/friendly&openid.alias3.count.alias3=1

EGA
e-Government Agency

Basic OpenID parameter

Parameter	Description
openid.mode	(ต้องระบุ) เป็นการบอกให้ OpenId Provider รู้ว่า OpenId Provider นี้สามารถติดต่อกับผู้ใช้ได้หรือไม่ โดยมีค่าดังนี้ • “checked_immediate” (ไม่ให้ติดต่อกับผู้ใช้) • “checked_setup”(ให้ติดต่อกับผู้ใช้ได้ แนะนำ)
openid.ns	(ต้องระบุ) เป็นการบอก verison ของ OpenId Request โดยระบบยืนยันตัวบุคคลกลางใช้งานรองรับ OpenId 2.0 ระบบบริการภาครัฐจึงควรใช้ Relying Party ไลบรารี่ที่รองรับ OpenId 2.0 แล้วใส่ค่าเป็น “http://specs.openid.net/auth/2.0”

Basic OpenID parameter

Parameter	Description
openid.return_to	(ต้องระบุ) เป็น URL ที่ระบบยืนยันตัวบุคคลกลางจะส่งผู้ใช้กลับมาหลังจากผู้ใช้งานทำการลงชื่อเข้าใช้แล้ว
openid.assoc_handle	(ไม่จำเป็นต้องระบุ) ค่าที่ใช้ในการ sign response
openid.claimed_id	(ไม่จำเป็นต้องระบุ) ค่านี้ต้องถูกตั้งเป็น “http://specs.openid.net/auth/2.0/identifier_select”
openid.identity	(ไม่จำเป็นต้องระบุ) ค่านี้ต้องถูกตั้งเป็น “http://specs.openid.net/auth/2.0/identifier_select”
openid.realm	(ไม่จำเป็นต้องระบุ)

Attribute Exchange Extension

Parameter	Description
openid.ns.<extension_alias>	(ต้องระบุ) เป็นการบอกระบบยืนยันตัวบุคคลกลางให้ส่งค่าคืนมาในรูปแบบของ Attribute Exchange (ระบบยืนยันตัวบุคคลกลาง สนับสนุนการส่งค่าคืนในรูปแบบ Attribute Exchange เท่านั้น) ค่านี้ต้องถูกตั้งเป็น “http://openid.net/srv/ax/1.0”
openid.<extension_alias>.mode	(ต้องระบุ) เป็นค่าบังคับเพื่อใช้งาน Attribute Exchange ค่านี้ต้องถูกตั้งเป็น “fetch_request”

EGA
e-Government Agency

Attribute Exchange Extension

Parameter	Description
openid.<extension_alias>.required	(ต้องระบุ) เป็นการบอกระบบยืนยันตัวบุคคลกลางว่าระบบบริการภาครัฐต้องการ attribute อะไรคืนไปบ้าง โดยทุก attribute ต้องระบุค่าจริงเพื่อให้ใช้งานได้ครอบคลุม
openid.<extension_alias>.type.<attribute_alias>	(ต้องระบุ) เป็นการบอกระบบยืนยันตัวบุคคลกลางว่าระบบบริการภาครัฐมีการส่งชื่อ attribute อะไรบ้างโดยชื่อ attribute_alias ต้องถูกกำหนดใน openid.<extension_alias>.required ถ้าระบบบริการภาครัฐต้องการ attribute นั้น

Attribute alias

ชื่อ Attribute	ค่าที่ส่งคืน
http://axschema.org/contact/email	e-mail ของผู้ใช้
http://axschema.org/namePerson	ชื่อ-นามสกุล ของผู้ใช้
http://axschema.org/namePerson/friendly	User name ในระบบ e-portal ของผู้ใช้
http://axschema.org/contact/phone/cell	หมายเลขโทรศัทพ์เคลื่อนที่
http://www.egov.go.th/2012/identifier/citizenid	เลขประจำตัวประชาชน
http://www.egov.go.th/2012/identifier/passportid	เลขที่หนังสือเดินทาง (กรณีชาวต่างชาติ)
http://www.egov.go.th/2012/identifier/juristicid	เลขนิติบุคคล

Attribute alias

ชื่อ Attribute	ค่าที่ส่งคืน
http://www.egov.go.th/2012/identifier/usertype	ประเภทของผู้ใช้ ในระบบ e-portal ค่า Citizen : บุคคลธรรมดา ค่า JuristicPerson : นิติบุคคล ค่า Foreigner : ชาวต่างชาติ ค่า GovernmentAgent : เจ้าหน้าที่ของรัฐ
http://www.egov.go.th/2012/identifier/identity	รหัสยืนยัน โดยรูปแบบขึ้นอยู่กับประเภทของผู้ใช้ดังนี้ บุคคลธรรมดา : เลขประจำตัวประชาชน นิติบุคคล : เลขนิติบุคคล ชาวต่างชาติ : เลขที่หนังสือเดินทาง เจ้าหน้าที่ของรัฐ : เลขประจำตัวประชาชน

Attribute alias

ชื่อ Attribute	ค่าที่ส่งคืน
http://www.egov.go.th/2012/identifier/identityverifiedlevel	ระดับการยืนยันของรหัสยืนยัน
http://www.egov.go.th/2012/identifier/citizenidverifiedlevel	ระดับการยืนยันของเลขประจำตัวประชาชน
http://www.egov.go.th/2012/identifier/juristicidverifiedlevel	ระดับการยืนยันของเลขนิติบุคคล
http://www.egov.go.th/2012/identifier/passportidverifiedlevel	ระดับการยืนยันของเลขที่หนังสือเดินทาง
http://www.egov.go.th/2012/identifier/organizationid	รหัสหน่วยงาน

ระดับของการยืนยันบุคคล

ในปัจจุบัน ระบบเว็บไซด์กลางได้แบ่งระดับของการยืนยันบุคคล โดยได้ประยุกต์เนื้อหาจากเอกสาร “Registration and Authentication: e-Government Strategy Framework Policy and Guidelines” เวอร์ชั่น 3.0 จัดทำโดยรัฐบาลอังกฤษ กันยายน 2545 ซึ่งเป็น 4 ระดับดังนี้

- ระดับ 0 (Unverified)
- ระดับ 1
- ระดับ 2
- ระดับ 3

ระดับ 0 (Unverified)

- เหมาะสมกับธุรกรรมอิเล็กทรอนิกส์ภาครัฐที่*ไม่ก่อให้เกิดความเสียหาย* ถ้าเกิดข้อผิดพลาดในการยืนยันบุคคล
- ไม่ก่อให้เกิดความไม่สะดวกต่อผู้ที่เกี่ยวข้อง
- ข้อมูลส่วนตัวหรือข้อมูลที่สามารถนำไปใช้ประโยชนเชิงพาณิชย์ได้ ไม่เกิดการรั่วไหลไปยังบุคคลภายนอก
- ไม่ก่อให้เกิดความเสียหายด้านร่างกายหรือทรัพย์สิน
- ไม่ก่อให้เกิดความเสื่อมเสียต่อบุคคลใด
- ไม่ก่อให้เกิดอุปสรรคหรือความล่าช้าต่อการตรวจพบอาชญากรรม

ระดับ 1

- เหมาะสมกับธุรกรรมอิเล็กทรอนิกส์ภาครัฐที่*อาจก่อให้เกิดความเสียหายเล็กน้อย* ถ้าเกิดข้อผิดพลาดในการยืนยันบุคคล
- อาจก่อให้เกิดความไม่สะดวกต่อผู้ที่เกี่ยวข้องเล็กน้อย
- ข้อมูลส่วนตัวหรือข้อมูลที่สามารถนำไปใช้ประโยชนเชิงพาณิชย์ได้ ไม่เกิดการรั่วไหลไปยังบุคคลภายนอก
- ไม่ก่อให้เกิดความเสียหายด้านร่างกายต่อผู้ที่เกี่ยวข้อง
- อาจก่อให้เกิดความเสียหายด้านทรัพย์สินต่อผู้ที่เกี่ยวข้องเล็กน้อย
- อาจก่อให้เกิดความเสื่อมเสียต่อผู้ที่เกี่ยวข้องเล็กน้อย
- ไม่ก่อให้เกิดอุปสรรคหรือความล่าช้าต่อการตรวจพบอาชญากรรม

ระดับ 2

- เหมาะสมกับธุรกรรมอิเล็กทรอนิกส์ภาครัฐที่*อาจก่อให้เกิดความเสียหายพอสมควร* ถ้าเกิดข้อผิดพลาดในการยืนยันบุคคล
- อาจก่อให้เกิดความไม่สะดวกต่อผู้ที่เกี่ยวข้องพอสมควร
- ข้อมูลส่วนตัวหรือข้อมูลที่สามารถนำไปใช้ประโยชนเชิงพาณิชย์ได้ อาจเกิดการรั่วไหลไปยังบุคคลภายนอก
- ไม่ก่อให้เกิดความเสียหายด้านร่างกายต่อผู้ที่เกี่ยวข้อง
- อาจก่อให้เกิดความเสียหายด้านทรัพย์สินต่อผู้ที่เกี่ยวข้องพอสมควร
- อาจก่อให้เกิดความเสื่อมเสียต่อผู้ที่เกี่ยวข้องพอสมควร
- อาจก่อให้เกิดอุปสรรคหรือความล่าช้าต่อการตรวจพบอาชญากรรม

ระดับ 3

- เหมาะสมกับธุรกรรมอิเล็กทรอนิกส์ภาครัฐที่*อาจก่อให้เกิดความเสียหายอย่างมาก* ถ้าเกิดข้อผิดพลาดในการยืนยันบุคคล
- อาจก่อให้เกิดความไม่สะดวกต่อผู้ที่เกี่ยวข้องอย่างมาก
- ข้อมูลส่วนตัวหรือข้อมูลที่สามารถนำไปใช้ประโยชนเชิงพาณิชย์ได้อาจเกิดการรั่วไหลไปยังบุคคลภายนอก
- อาจก่อให้เกิดความเสียหายด้านร่างกายต่อผู้ที่เกี่ยวข้อง
- อาจก่อให้เกิดความเสียหายด้านทรัพย์สินต่อผู้ที่เกี่ยวข้องอย่างมาก
- อาจก่อให้เกิดความเสื่อมเสียต่อผู้ที่เกี่ยวข้องอย่างมาก
- อาจก่อให้เกิดอุปสรรคหรือความล่าช้าต่อการตรวจพบอาชญากรรม

ตัวอย่าง Response

http://localhost:4856/loginProgrammatic.aspx?dnoa.userSuppliedIdentifier=http://localhost:1807/EGA.EGA_CAS.Security.eAuthen/&openid.claimed_id=http://localhost:1807/EGA.EGA_CAS.Security.eAuthen/user.aspx/Administrator&openid.identity=http://localhost:1807/EGA.EGA_CAS.Security.eAuthen/user.aspx/Administrator&openid.sig=P6+IZf5yVHeOTnngzycP7vw8BRLJiBHF4ZSOm1Mauxg=&openid.signed=claimed_id,identity,assoc_handle,op_endpoint,return_to,response_nonce,ns.alias3,alias3.mode,alias3.type.alias1,alias3.value.alias1,alias3.type.alias2,alias3.value.alias2,alias3.type.alias3,alias3.value.alias3,alias3.type.alias4,alias3.value.alias4&openid.assoc_handle=nixR!IAAAAB56GYx_ecAUdoR3qhyvqAi9MZxO-Ahl00nqoeUcrtnQQQAAAAGNVREK0g4S_Zb8IgSlb96sYGjE4AYbskGBPXGmwQ3yrBvH2CmwGL6bIW_6m2Ibh0cN5Zt5rl0hhM4hvHj6HDlZ&openid.op_endpoint=http://localhost:1807/EGA.EGA_CAS.Security.eAuthen/server.aspx&openid.return_to=http://localhost:4856/loginProgrammatic.aspx?dnoa.userSuppliedIdentifier=http%3A%2F%2Flocalhost%3A1807%2FEGA.EGA_CAS.Security.eAuthen%2F&openid.response_nonce=2012-05-15T10:45:54ZrrKt7tDX

EGA
e-Government Agency

ตัวอย่าง Response (ต่อ)

&openid.mode=id_res&openid.ns=http://specs.openid.net/auth/2.0&openid.ns.alias3=http://openid.net/srv/ax/1.0&openid.alias3.mode=fetch_response&openid.alias3.type.alias1=http://axschema.org/contact/email&openid.alias3.value.alias1=test@gits.net.th&openid.alias3.type.alias2=http://axschema.org/namePerson&openid.alias3.value.alias2=Administrator eGov-Portal&openid.alias3.type.alias3=http://axschema.org/namePerson/friendly&openid.alias3.value.alias3=administrator&openid.alias3.type.alias4=http://www.egov.go.th/2012/identifier/citizenid&openid.alias3.value.alias4=

การตรวจสอบความถูกต้อง

- เพื่อป้องกันการทำ replay attack ระบบ e-service ต้องทำการตรวจสอบข้อมูลที่ได้มากับระบบเว็บไซด์กลางทุกครั้ง โดยการแก้ parameter “openid.mode” ให้เป็น “check_authentication” พร้อมทั้งแนบข้อมูลที่ไดรับมาทั้งหมดส่งให้ระบบเว็บไซด์กลางแบบ Http post request
- ระบบ e-service จะได้รับค่า “Is_valid” เป็น “true” ถ้าข้อมูลทั้งหมดถูกส่งมาจาก ระบบเว็บไซด์กลางจริง

การนำข้อมูลที่ได้ไปใช้งาน

- สรอ.แนะนำให้ระบบสารสนเทศของหน่วยงานใช้ข้อมูลต่อไปนี้เทียบเคียงเพื่อยืนยันตัวบุคคล

  - อีเมล์

  - เลขประจำตัวประชาชน

- กรณีข้อมูลอีเมล์ เลขบัตรประชาชน ไม่มีอยู่ที่เว็บไซต์ท่า (ระบบยืนยันตัวบุคคล)

  - ระบบยืนยันตัวบุคคลกลาง จะแสดงหน้าให้ผู้ใช้ทำการเพิ่มข้อมูลก่อนส่งผู้ใช้ไปยังระบบสารสนเทศของหน่วยงาน

การนำข้อมูลที่ได้ไปใช้งาน

- กรณีที่ระบบสารสนเทศของหน่วยงานไม่ได้เก็บข้อมูลอีเมล์ เลขบัตรประชาชน หรือเทียบค่าแล้วไม่พบผู้ใช้ ทางสรอ. แนะนำให้ใช้แนวทางดังนี้
  - สร้างหน้าขึ้นมาเพื่อให้ผู้ใช้ทำการ login ด้วยบัญชีของ e-service ก่อน เพื่อทำการระบุตัวตน หรือสร้างผู้ใช้ใหม่ในกรณีที่ไม่มีบัญชีอยู่ที่ e-service
  - ถ้าระบบไม่ได้เก็บค่าเหล่านี้ลงในฐานข้อมูล ทางสรอ. แนะนำให้สร้าง ตารางเพิ่มเพื่อเก็บค่านี้

ไลบรารี่ที่สรอ.แนะนำให้ใช้

- ASP.NET -> DotNetOpenAuth
- PHP -> LightOpenID
  -> PHP OpenID Library
- Java -> JOpenID
  -> OpenID4Java

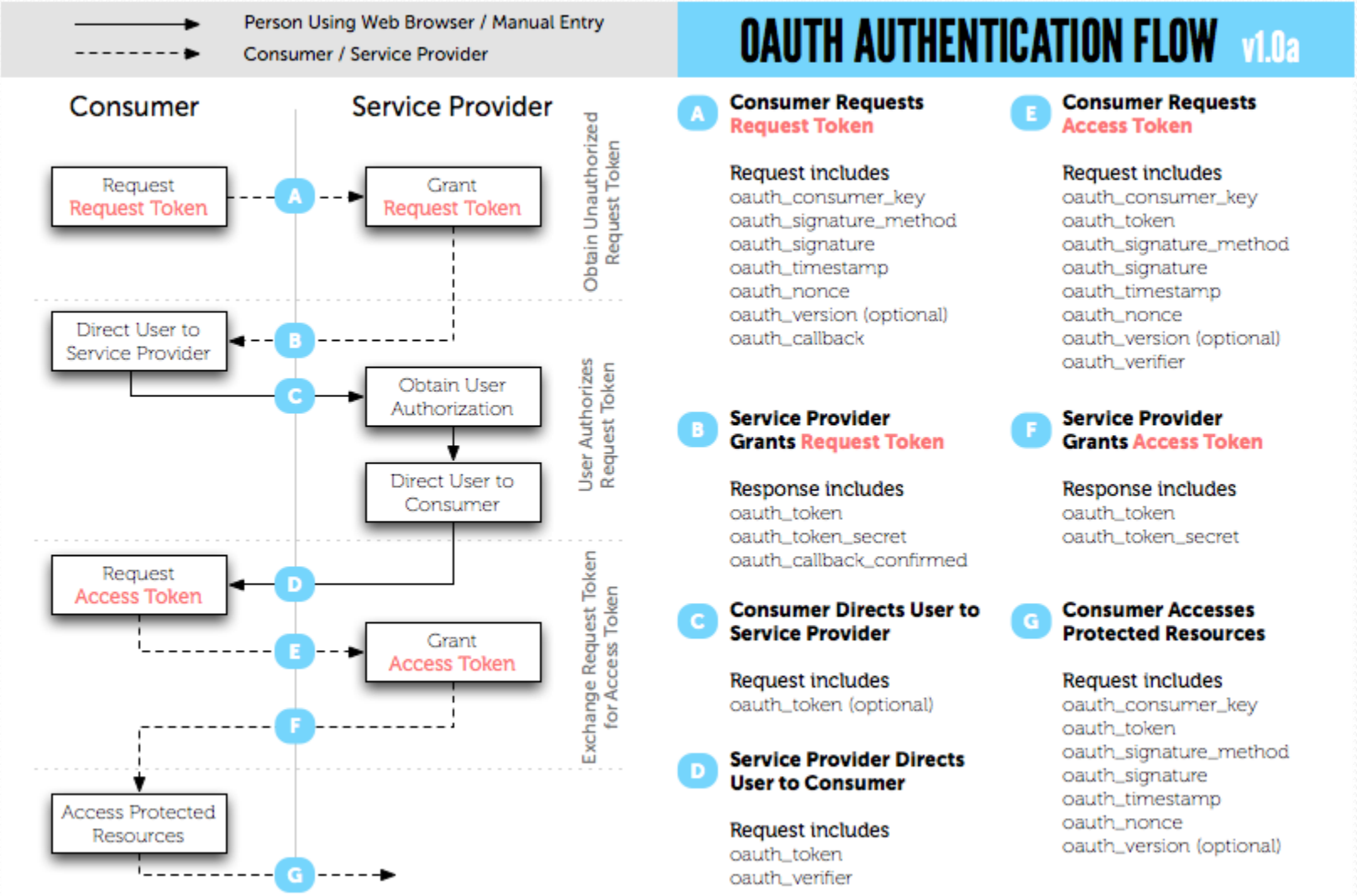
แนวทางการเข้าถึงระบบบริการอิเล็กทรอนิกส์แบบรวมศูนย์ (Single Sign-On)

OAuth

องค์ประกอบหลักที่เกี่ยวข้อง

- ฝั่งระบบ e-Service “Oauth Consumer”
  - หน้าจอ SSORegister
  - ไลบรารี่สำหรับรองรับการใช้งาน OAuth v1.0a ตามแต่ภาษาที่ใช้ (PHP, Java, ASP.NET)
  - OAuth Consumer “key” และ “secret” ที่ทางสรอ.ส่งให้
- ฝั่งระบบยืนยันตัวบุคคลกลาง “Service Provider”
  - หน้าเว็บเพจ OAuth.ashx (https://openid.egov.go.th/OAuth.ashx)
  - หน้าเว็บเพจ XmlUserInfo.aspx (https://openid.egov.go.th/XmlUserInfo.aspx)

ขั้นตอนการทำงานของ Oauth (http://oauth.net/core/1.0/)



Request ในขั้นตอน A.

- HTTP POST -> http://testopenid.ega.or.th/OAuth.ashx
- oauth_callback=http://localhost:61420/code/SSORegister.aspx&
  oauth_consumer_key=sampleconsumer&
  oauth_nonce=MqoTuozw&
  oauth_signature_method=HMAC-SHA1&
  oauth_signature=1q259ZnTlWXaI97HDG736KFKqRI=&
  oauth_version=1.0&oa
  scope=

A. การขอ “Request Token”จากระบบยืนยันตัวบุคคลกลาง

Parameter	Description
oauth_consumer_key	“key” ที่ทางสรอ.ส่งให้
oauth_signature_method	วิธีการ Sign Request (ควรใช้ค่าเป็น HMAC-SHA1)
oauth_signature	ค่าที่ในการ Sign Request ตาม oauth_signature_method (โดยทั่วไป parameter นี้จะถูกตั้งค่าให้อัตโนมัติในขั้นตอนสร้าง Request ของแต่ละไลบรารี่)
oauth_timestamp	เวลาที่ทำการ Request
oauth_nonce	เป็นชุดของเลขที่ถูกสุ่มขึ้นมาให้ไม่ซ้ำกันในแต่ละ Request ของแต่ละระบบบริการภาครัฐ เพื่อเอาไว้ตรวจสอบว่า Request นี้เป็น Request ที่ไม่เคยถูกใช้มาก่อน และป้องกันการโจมตีผ่าน HTTP
oauth_version	เวอร์ชั่นของ OAuth
oauth_callback	URL ที่จะให้ส่ง “Request Token” กลับไป

Response ในขั้นตอน B.

- HTTP POST -> http://localhost:61420/code/SSORegister.aspx
- oauth_token=w6yxDlpNB8QK2Y6xpyKszTZpVps=&
  oauth_token_secret=oHN1HvCFzaX/vI17faCyiFiVzRk=&
  oauth_callback_confirmed=true

B. ระบบยืนยันตัวบุคคลกลางส่ง “Request Token” กลับไปให้

Parameter	Description
oauth_token	“Request Token” จากระบบข้อมูลผู้ใช้
oauth_token_secret	เป็นค่าที่ระบบข้อมูลผู้ใช้ส่งมาพร้อมกับ “Request Token” เพื่อใช้ในการตรวจสอบ “Request Token” โดยค่านี้จะไม่ซ้ำกันในแต่ละ “Request Token”
oauth_callback_confirmed	เป็น True ถ้าได้รับการยืนยันจากระบบเว็บไซต์กลาง

Request ในขั้นตอน C.

- HTTP GET -> http://testopenid.ega.or.th/OAuth.ashx
- oauth_token=w6yxDlpNB8QK2Y6xpyKszTZpVps=

C. ให้ผู้ใช้ทำการยืนยันตัวตน

- ระบบสารสนเทศภาครัฐส่งผู้ใช้ไปยังระบบยืนยันตัวบุคคลกลาง เพื่อทำการยืนยันตัวตน (ในกรณีที่ผู้ใช้ยังไม่ได้ทำการลงชื่อเข้าใช้กับระบบยืนยันตัวบุคคลกลาง) และให้ผู้ใช้ตัดสินใจว่าจะอนุญาติให้ระบบสารสนเทศภาครัฐสามารถเข้าถึงข้อมูลของผู้ใช้ได้หรือไม่ parameter ที่ใช้ในขั้นตอนนี้มีแค่ oauth_token ซึ่งได้มาจากขั้นตอน B (Request Token)

Response ในขั้นตอน D.

- HTTP GET -> http://localhost:61420/code/SSORegister.aspx
- oauth_verifier=piRunFM=&

  oauth_token=w6yxDlpNB8QK2Y6xpyKszTZpVps=

EGA
e-Government Agency

D. ระบบยืนยันตัวบุคคลกลางส่งผู้ใช้กลับไปยังระบบสารสนเทศภาครัฐ

Parameter	Description
oauth_token	“Request Token” จากขั้นตอน B (ในขั้นตอนนี้ “Request Token” ได้รับการอนุญาตให้ใช้งานได้จากระบบข้อมูลผู้ใช้แล้ว)
oauth_verifier	เป็นค่าที่ระบบข้อมูลผู้ใช้ส่งมาพร้อมกับ “Request Token” โดยค่านี้จะมีความเชื่อมโยงกับระบบบริการภาครัฐ ค่านี้ถูกใช้ในขั้นตอน E เพื่อยืนยันว่าระบบบริการภาครัฐที่จะขอ “Access Token” นั้นเป็นระบบบริการภาครัฐเดียวกับที่ขอ “Request Token”

Request ในขั้นตอน E.

- HTTP POST -> http://testopenid.ega.or.th/OAuth.ashx
- oauth_verifier=piRunFM%3D&
  oauth_token=w6yxDlpNB8QK2Y6xpyKszTZpVps%3D&
  oauth_consumer_key=sampleconsumer&
  oauth_nonce=Y2FPEOhg&
  oauth_signature_method=HMAC-SHA1&
  oauth_signature=DLKewGmNI1%2BrmpUUHgsviQQ9Z6I%3D&
  oauth_version=1.0&oau

EGA
e-Government Agency

E. แลก “Request Token” เป็น “Access Token”

Parameter	Description
oauth_consumer_key	“key” ที่ทางสรอ.ส่งให้
oauth_token	“Request Token” ในขั้นตอน D
oauth_signature_method	วิธีการเข้ารหัส Request (ต้องใส่ค่าเป็น HMAC-SHA1)
oauth_signature	ค่าที่ได้จากขั้นตอนการเข้ารหัส ตาม oauth_signature_method ค่าในขั้นตอนนี้จะไม่เหมือนค่าในขั้นตอน A (โดยทั่วไป parameter นี้จะถูกตั้งค่าให้อัตโนมัติในขั้นตอนสร้าง Request ของแต่ละไลบรารี่)
oauth_timestamp	เวลาที่ทำการ Request
oauth_nonce	เป็นชุดของตัวเลขที่ถูกสุ่มขึ้นมาให้ไม่ซ้ำกันในแต่ละ Request ของแต่ละระบบบริการภาครัฐ เพื่อเอาไว้ตรวจสอบว่า Request นี้เป็น Request ที่ไม่เคยถูกใช้มาก่อน และป้องกันการโจมตีผ่าน HTTP
oauth_version	เวอร์ชั่นของ OAuth
oauth_verifier	ค่าที่ได้จากระบบข้อมูลผู้ใช้ในขั้นตอน D

Response ในขั้นตอน F.

- HTTP POST -> http://localhost:61420/code/SSORegister.aspx
- oauth_token=FpLQoLmK997T+i9lsaA33+bWIEY=&
  oauth_token_secret=kzvbxfPP+pCscwOcvYWpk3waRNw=

F. ระบบเว็บไซต์กลางส่ง “Access Token” กลับไปให้

Parameter	Description
oauth_token	“Access Token” ที่ได้รับจากระบบยืนยันตัวบุคคลกลาง
oauth_token_secret	เป็นค่าที่ระบบข้อมูลผู้ใช้ส่งมาพร้อมกับ “Access Token” เพื่อใช้ในการตรวจสอบ “Access Token” โดยค่านี้จะไม่ซ้ำกันในแต่ละ “Access Token”

G. นำ “Access Token” ไปแลกข้อมูลผู้ใช้

- ระบบสารสนเทศภาครัฐนำ “Access Token” ที่ได้ไปเข้าถึงข้อมูลของผู้ใช้ โดยทางสรอ.ได้ปรับวิธีการเข้าถึงข้อมูลเพื่อให้ได้ข้อมูลกลับมาในรูปแบบของ xml โดยผู้พัฒนาสามารถเข้าถึง xml ผ่าน URL : “http://openid.egov.go.th/XmlUserInfo.aspx?AccessToken={Access Token ที่ระบบสารสนเทศภาครัฐได้รับ}” โดย “Access Token” มีอายุการใช้งาน 10 นาที
- กรณีที่ผู้พัฒนา Request Token ในขั้นตอน A ไปที่ https://govid.egov.go.th ผู้พัฒนาสามารถเข้าถึง xml ผ่าน URL : “http://govid.egov.go.th/XmlUserInfo.aspx?AccessToken={Access Token ที่ระบบสารสนเทศภาครัฐได้รับ}”

EGA
e-Government Agency

ไลบรารี่ที่สรอ.เคยใช้

- ASP.NET -> DotNetOpenAuth
- PHP -> basic php library

ตัวอย่าง XML ของประชาชน

```
<? Xml version=“1.0” encoding="UTF-8"?>
<Member type="Citizen">
    <UserID>a4d8b6a0-37db-4f44-b598fb0e6550a31f</UserID>
    <UserName>TestVender3</UserName>
    <Title VerifiedLevel="Unverified"/>
    <FullName VerifiedLevel="Unverified">Vender3 Test</FullName>
    <FirstName VerifiedLevel="Unverified">Vender3</FirstName>
    <LastName VerifiedLevel="Unverified">Test</LastName>
    <DateOfBirth VerifiedLevel="Unverified"/>
    <Gender VerifiedLevel="Unverified"/>
    <Identification>
        <Code VerifiedLevel="Unverified"/>
        <IssueBy VerifiedLevel="Unverified"/>
        <IssueDate VerifiedLevel="Unverified"/>
        <ExpireDate VerifiedLevel="Unverified"/>
    </Identification>
```

ตัวอย่าง XML ของประชาชน (ต่อ)

```
<Nationality VerifiedLevel="Unverified"/>
  <Occupation VerifiedLevel="Unverified"/>
  <Address>
      <HouseNumber VerifiedLevel="Unverified"/>
      <VillageName VerifiedLevel="Unverified"/>
      <Moo VerifiedLevel="Unverified"/>
      <Soi VerifiedLevel="Unverified"/>
      <Road VerifiedLevel="Unverified"/>
      <SubDistrict VerifiedLevel="Unverified"/>
      <District VerifiedLevel="Unverified"/>
      <Province VerifiedLevel="Unverified"/>
      <PostCode VerifiedLevel="Unverified"/>
      <GeoCode VerifiedLevel="Unverified"/>
  </Address>
```

ตัวอย่าง XML ของประชาชน (ต่อ)

```
    <ContactInfo>
        <Telephone VerifiedLevel="Unverified"/>
        <Mobilephone VerifiedLevel="Unverified"/>
         <EMail VerifiedLevel="Unverified">vender3@test.com</EMail>
        <AlternativeEMail VerifiedLevel="Unverified"/>
    </ContactInfo>
</Member>
```

ตัวอย่าง XML ของเจ้าหน้าที่รัฐ

```
<? Xml version=“1.0” encoding="UTF-8"?>
<Member type="GovernmentAgent">
    <UserID>b8c871c0-e951-102f-8d63-83b2f2cc5bab</UserID>
    <UserName>Test.User</UserName>
    <Title VerifiedLevel="Unverified"/>
    <FullName VerifiedLevel="Unverified">Test User</FullName>
    <FirstName VerifiedLevel="Unverified">Test</FirstName>
    <LastName VerifiedLevel="Unverified">User</LastName>
    <DateOfBirth VerifiedLevel="Unverified"/>
    <Gender VerifiedLevel="Unverified"/>
    <Identification>
        <Code VerifiedLevel="Unverified"/>
        <IssueBy VerifiedLevel="Unverified"/>
        <IssueDate VerifiedLevel="Unverified"/>
        <ExpireDate VerifiedLevel="Unverified"/>
    </Identification>
```

ตัวอย่าง XML ของเจ้าหน้าที่รัฐ (ต่อ)

```
<Nationality VerifiedLevel="Unverified"/>
  <Occupation VerifiedLevel="Unverified"/>
  <Organization>
    <Name VerifiedLevel="VerifiedLevel2" Code="10009000">สำนักงานรัฐบาล
          อิเล็กทรอนิกส์ (องค์การมหาชน)</Name>
    <Ministry VerifiedLevel="VerifiedLevel2" Code="10">กระทรวงเทคโนโลยี
          สารสนเทศและการสื่อสาร</Ministry>
    <Department VerifiedLevel="VerifiedLevel2" Code="009">สำนักงานรัฐบาล
          อิเล็กทรอนิกส์ (องค์การมหาชน)</Department>
    <Division VerifiedLevel="VerifiedLevel2" Code="000"/>
  </Organization>
```

ตัวอย่าง XML ของเจ้าหน้าที่รัฐ (ต่อ)

```
<Address>
        <HouseNumber VerifiedLevel="Unverified"/>
        <VillageName VerifiedLevel="Unverified"/>
        <Moo VerifiedLevel="Unverified"/>
        <Soi VerifiedLevel="Unverified"/>
        <Road VerifiedLevel="Unverified"/>
        <SubDistrict VerifiedLevel="Unverified"/>
        <District VerifiedLevel="Unverified"/>
        <Province VerifiedLevel="Unverified"/>
        <PostCode VerifiedLevel="Unverified"/>
        <GeoCode VerifiedLevel="Unverified"/>
    </Address>
```

ตัวอย่าง XML ของเจ้าหน้าที่รัฐ (ต่อ)

```
    <ContactInfo>
        <Telephone VerifiedLevel="Unverified"/>
        <Mobilephone VerifiedLevel="Unverified"/>
         <EMail VerifiedLevel="Unverified">Test.User@ega.or.th</EMail>
        <AlternativeEMail VerifiedLevel="Unverified"/>
    </ContactInfo>
</Member>
```


EGA
e-Government Agency

ตัวอย่าง XML ของนิติบุคคล

```
<?xml version="1.0" encoding="UTF-8"?>
<Member type="JuristicPerson">
    <UserID>09ddc1eb-360b-41e5-8e3f-12206065cda9</UserID>
    <UserName>testjuristic</UserName>
    <Name VerifiedLevel="Unverified">อีจีเอ จำกัด (มหาชน)</Name>
    <Abbreviation VerifiedLevel="Unverified"></Abbreviation>
    <ContactPerson VerifiedLevel="Unverified"></ContactPerson>
    <ContactPhoneNumber
    VerifiedLevel="Unverified">026126000</ContactPhoneNumber>
    <Identification>
        <Code VerifiedLevel="Unverified">0105553077469</Code>
    </Identification>
```


EGA
e-Government Agency

ตัวอย่าง XML ของนิติบุคคล(ต่อ)

```
<Address>
    <HouseNumber VerifiedLevel="Unverified">108</HouseNumber>
    <VillageName VerifiedLevel="Unverified">BKKทาวเวอร์19</VillageName>
    <Moo VerifiedLevel="Unverified"></Moo>
    <Soi VerifiedLevel="Unverified">รางน้ำ</Soi>
    <Road VerifiedLevel="Unverified">รางน้ำ</Road>
    <SubDistrict VerifiedLevel="Unverified">ทุ่งพญาไท</SubDistrict>
    <District VerifiedLevel="Unverified">เขตราชเทวี</District>
    <Province VerifiedLevel="Unverified">กรุงเทพมหานคร</Province>
    <PostCode VerifiedLevel="Unverified">10400</PostCode>
    <GeoCode VerifiedLevel="Unverified">10370100</GeoCode>
</Address>
```

ตัวอย่าง XML ของนิติบุคคล(ต่อ)

```
    <ContactInfo>
        <Telephone VerifiedLevel="Unverified">026126000</Telephone>
        <Mobilephone VerifiedLevel="Unverified"></Mobilephone>
        <EMail VerifiedLevel="Unverified">juristic@ega.or.th</EMail>
        <AlternativeEMail VerifiedLevel="Unverified"></AlternativeEMail>
    </ContactInfo>
</Member>
```

การใช้งาน xml

- ทำการแกะข้อมูลออกมาจาก xml
- นำข้อมูลที่ได้ไปใส่ฟอร์มสมัครสมาชิก
- ถ้าระบบ e-service ต้องให้ผู้ใช้ใส่ Username และ Password ทางเว็บไซด์กลางสามารถให้ข้อมูล Username ได้ แต่ผู้ใช้ต้องกรอก Password เอง

ข้อแนะนำในการติดตั้ง

- ทำการสำรองข้อมูลก่อนการติดตั้ง
- ทำเอกสารจดบันทึกว่าได้เพิ่มหรือแก้ไขอะไรไปบ้าง
- ทำการทดสอบระบบโดยต้องทำการทดสอบอย่างน้อยดังนี้
  - เข้าใช้งานในกรณีมีผู้ใช้อยู่ที่ e-service และทำการ mapping ผู้ใช้แล้ว
  - เข้าใช้งานในกรณีมีผู้ใช้อยู่ที่ e-service แต่ยังไม่ได้ทำการ mapping
  - เข้าใช้งานในกรณีไม่มีผู้ใช้อยู่ที่ e-service

สรุปสิ่งที่นักพัฒนาต้องดำเนินการ

- สร้างหน้าเพจ SSOLogin และ/หรือ SSORegister และ Software Library ต่างๆ
  - สามารถดาวน์โหลดตัวอย่าง source code จากเว็บไซต์ของระบบยืนยันตัวบุคคลกลาง http://openid.egov.go.th/publish/DevMain.aspx
- กรณีเพจ SSOLogin ให้นำเอาข้อมูลที่ได้รับจากระบบยืนยันตัวบุคคลกลางไปตรวจสอบสิทธิในการเข้าถึงข้อมูล และบริการของระบบสารสนเทศของหน่วยงาน
- กรณีเพจ SSORegister ให้ทำการแกะข้อมูลโพรไฟล์ (เป็นรูปแบบของ XML) ที่ได้รับจากระบบยืนยันตัวบุคคลกลาง เพื่อนำไปใส่ในฟอร์ม Register
- แจ้ง domain หรือ ip address ของระบบระบบสารสนเทศของหน่วยงานกับเจ้าหน้าที่ สรอ. เพื่อเปิดให้ใช้งานระบบยืนยันตัวบุคคลกลาง

คำถาม?

ขอบคุณครับ