คู่มือแนวทางการรักษาความปลอดภัย ของการให้บริการข้อมูลผ่านระบบ NGIS Portal

National Geo-Informatics Infrastructure System

จัดทำโดย

คณะทำงานด้านเทคนิคเพื่อจัดทำรายละเอียดการให้บริการภูมิสารสนเทศ
บนเครือข่ายออนไลน์ผ่านระบบสืบค้นและบริการภูมิสารสนเทศกลางของประเทศ (NGIS Portal)

คู่มือแนวทางการรักษาความปลอดภัย ของการให้บริการข้อมูลผ่านระบบ

NGIS Portal

จัดทำโดย

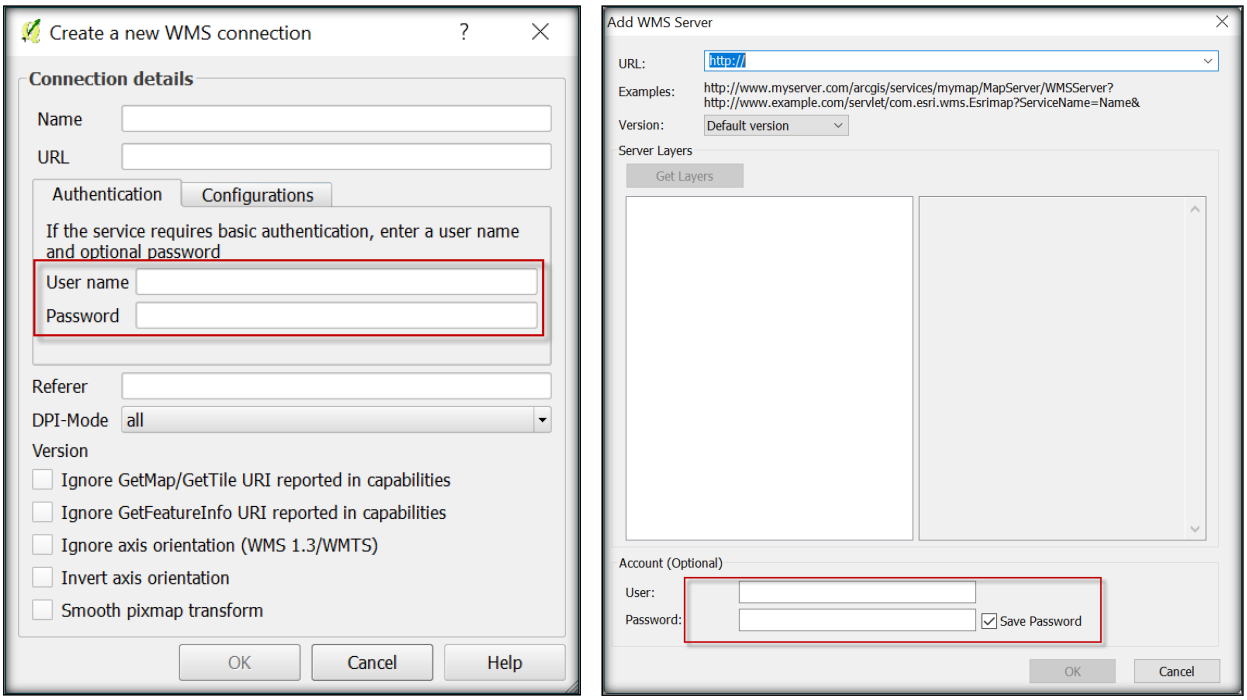
คณะทำงานด้านเทคนิคเพื่อจัดทำรายละเอียดการให้บริการภูมิสารสนเทศ
บนเครือข่ายออนไลน์ผ่านระบบสืบค้นและบริการภูมิสารสนเทศกลางของประเทศ (NGIS Portal)

คู่มือแนวทางการรักษาความปลอดภัยของการให้บริการข้อมูล ผ่านระบบ NGIS Portal

1. แนวทางการรักษาความปลอดภัยของการให้บริการข้อมูล สำหรับผู้ดูแลระบบของหน่วยงาน

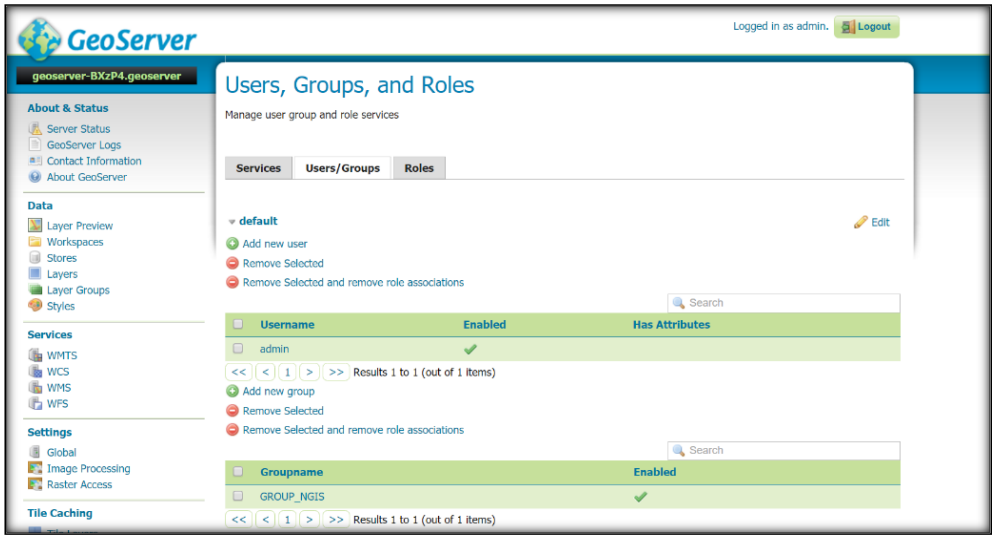
การให้บริการข้อมูลตามมาตรฐาน OGC Web Service สามารถใช้การควบคุมการเข้าถึงผ่านการระบุตัวตน (Authentication) และการจำกัดการเข้าถึงด้วย Domain name หรือ IP address ในการรักษาความปลอดภัยของข้อมูลได้ โดยแบ่งเป็น 3 ลักษณะ ดังนี้

1.1 การกำหนด Authentication แบบ Identification คือ การตรวจสอบผู้ที่ต้องการใช้งานข้อมูลด้วย Username และ Password โดยส่วนใหญ่โปรแกรมที่ให้บริการข้อมูล OGC Web Service หรือโปรแกรม Map Server สามารถกำหนดให้ผู้ใช้งานกรอก Username และ Password เพื่อระบุตัวตน หากถูกต้องแล้วผู้ใช้สามารถนำบริการข้อมูล OGC Web Service ไปใช้งานกับโปรแกรมต่างๆด้านภูมิสารสนเทศที่รองรับการแสดงข้อมูล OGC Web Service ดังภาพที่ 1



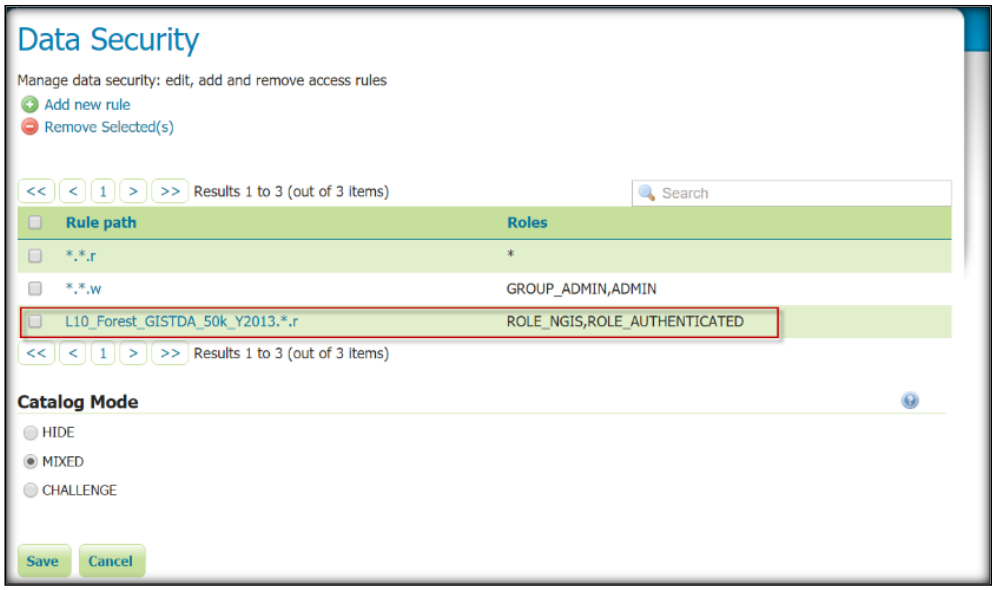
ภาพที่ 1 ตัวอย่างการใช้บริการข้อมูล OGC Web Service
โดยระบุ Username /Password (ซ้าย – QGIS/ ขวา – ArcGIS Desktop)

การกำหนด Username และ Password โดยส่วนใหญ่มีความเกี่ยวข้องกับการสร้างบทบาท (Role) หรือสร้างกลุ่ม (Group) ซึ่งผู้ดูแลระบบสามารถจัดกลุ่มผู้ใช้ตามความเหมาะสม จากนั้นผู้ดูแลระบบมีการกำหนด User, Group หรือ Role ให้สามารถใช้งานบริการชั้นข้อมูลแต่ละชั้นที่ให้บริการบนระบบได้ ดังภาพที่ 2 และ 3



ภาพที่ 2 ตัวอย่างหน้าต่างการจัดการ User, Group และ Role (GeoServer)

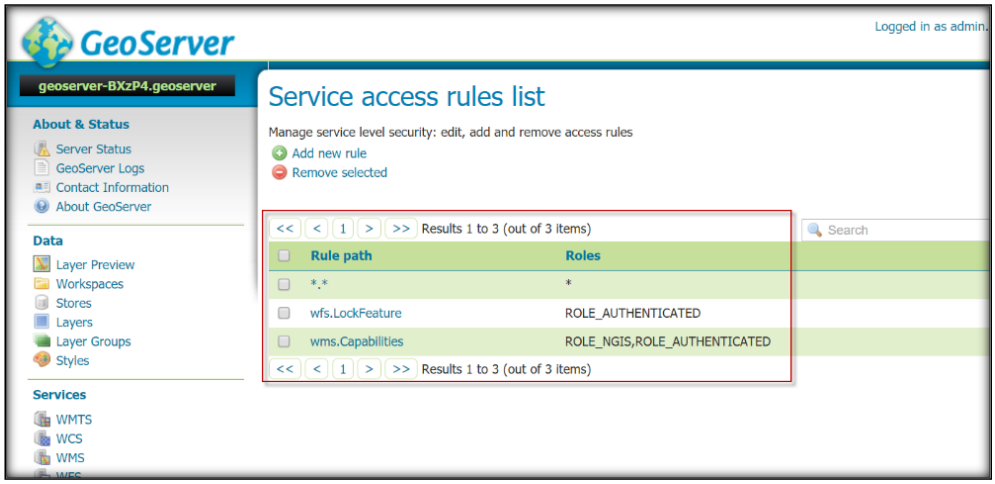
ผู้ดูแลระบบสามารถกำหนดสิทธิ์การใช้งานระดับชั้นข้อมูลให้แก่ผู้ใช้งานในระดับ (Role) ต่างๆ ได้ดังตัวอย่างในภาพที่ 3 ซึ่งมีการกำหนดให้ Role ที่ชื่อว่า ROLE_NGIS สามารถใช้งานชั้นข้อมูลชื่อ L10_Forest_GISTDA_50k_Y2013 แบบอ่านได้อย่างเดียว (r) ดังนั้น ผู้ใช้ที่อยู่ในกลุ่มดังกล่าวจะสามารถใช้งานชั้นข้อมูลที่ถูกกำหนดได้ และหากตั้งค่าให้เขียนได้ (w) ผู้ใช้จึงจะสามารถแก้ไขชั้นข้อมูลดังกล่าวได้



ภาพที่ 3 ตัวอย่างหน้าต่างการกำหนดสิทธิ์การใช้งานชั้นข้อมูลให้แก่ Role (GeoServer)

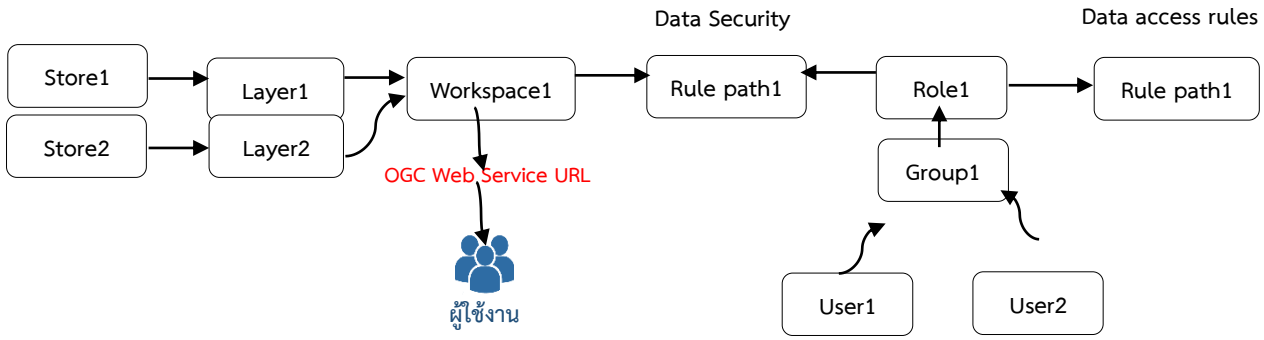
หมายเหตุ : Rule path ชื่อ *.*.r และ *.*.w คือการอนุญาตให้ Roles ทั้งหมด สามารถอ่านและเขียนข้อมูลได้ทุกชั้นที่อยู่ในระบบ จึงควรลบออกจากรายการเพื่อความปลอดภัยในการเข้าถึงรายการข้อมูล

ผู้ดูแลระบบสามารถกำหนดสิทธิ์การใช้งาน OGC Web Service ในแบบต่างๆ ให้แก่ Role ดังตัวอย่างในภาพที่ 4 ซึ่งมีการกำหนดให้ ROLE_NGIS สามารถใช้งานแบบ WFS ในโหมดการร้องขอ LockFeature และแบบ WMS โหมดการร้องขอ Capabilities ได้



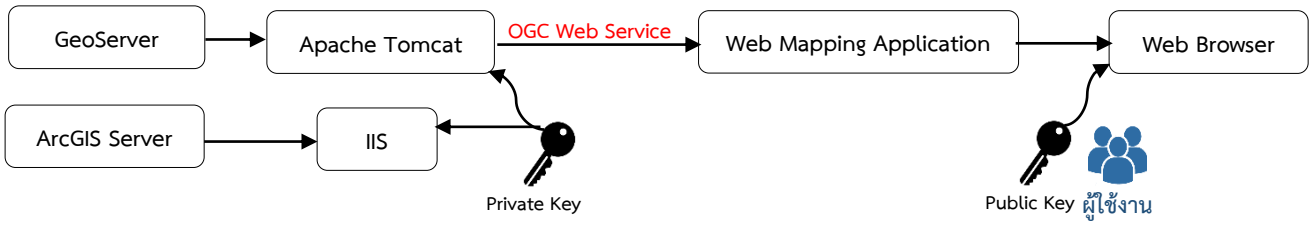
ภาพที่ 4 ตัวอย่างหน้าต่างการกำหนดสิทธิ์การใช้งาน OGC Web Service ให้แก่ Role (โปรแกรม GeoServer)

หมายเหตุ : ROLE_AUTHENTICATED เป็น Role ที่กำหนดเพื่อให้ผู้ใช้งานต้องระบุ Username และ Password ทุกครั้งก่อนใช้งานชั้นข้อมูล L10_Forest_GISTDA_50k_Y2013



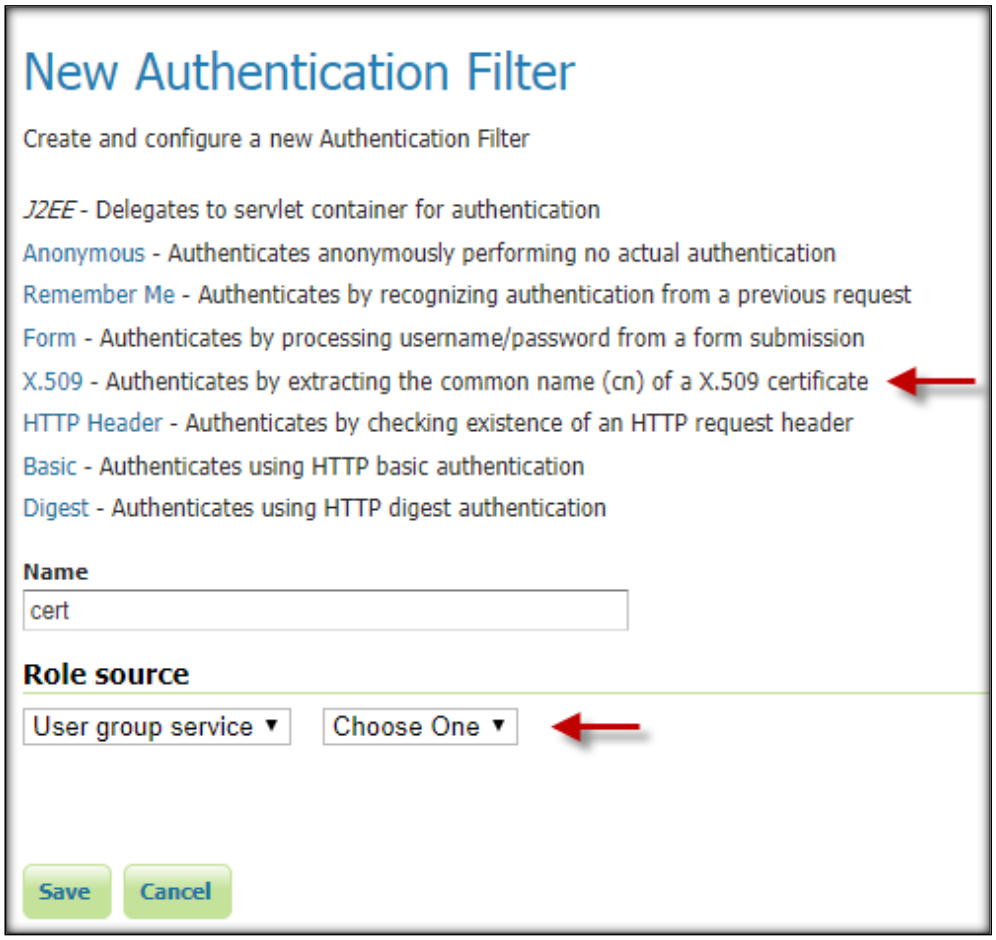
ภาพที่ 5 แผนภาพแสดงระบบความปลอดภัยของโปรแกรม GeoServer แบบ Identification
แหล่งที่มา : http://docs.geoserver.org/stable/en/user/security/index.html

1.2 การกำหนด Authentication แบบ Certificate คือ การตรวจสอบคุณสมบัติผู้ใช้ก่อนอนุญาตให้ใช้งานข้อมูล โดยส่วนใหญ่ผู้ดูแลระบบจะมอบกุญแจหรือ Public Key ให้กับผู้ใช้งาน ตามมาตรฐาน X.509 โดยโปรแกรม Map Server บางโปรแกรมสามารถสร้างการตรวจสอบดังกล่าวได้ในรูปแบบ two-way SSL



ภาพที่ 6 แผนภาพแสดงระบบความปลอดภัยแบบ Certificate

แหล่งที่มา : http://docs.geoserver.org/latest/en/user/security/tutorials/cert/



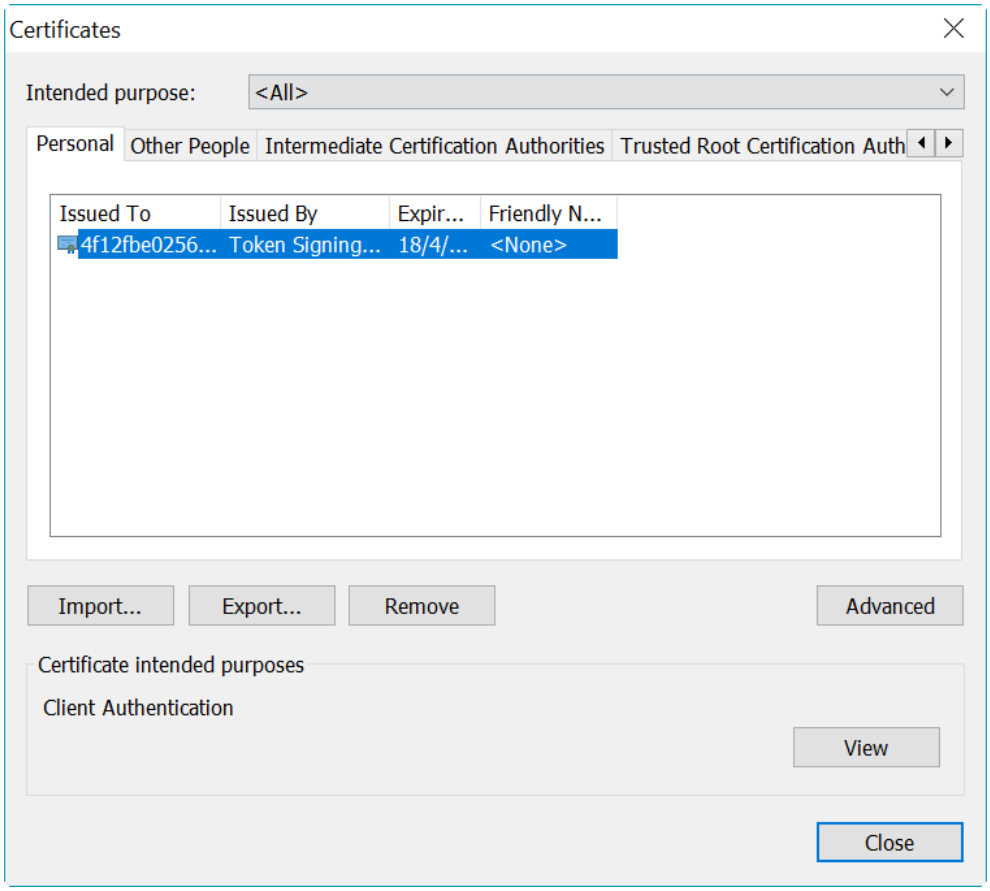
ภาพที่ 7 ตัวอย่างหน้าต่างการตั้งค่าการยืนตัวตนก่อนใช้ข้อมูลแบบ X.509 certificate (โปรแกรม GeoServer)

ผู้ดูแลระบบจะสร้าง Private Key และ Public Key โดยเก็บ Private Key ไว้ที่ Web Server ที่ทำงานรากฐานให้กับ Map Server

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true" scheme="https"
secure="true"
     clientAuth="true" sslProtocol="TLS"
     keystoreFile="${catalina.home}/conf/server.jks"
     keystoreType="JKS" keystorePass="password"
     truststoreFile="${catalina.home}/conf/server.jks"
     truststoreType="JKS" truststorePass="password" />
```

ภาพที่ 8 การตั้งค่าการกำหนด Private key (โปรแกรม Apache Tomcat)

การแจกจ่าย Public Key ให้แก่ผู้ใช้ โดยการใช้งานข้อมูลผ่านโปรแกรมแผนที่ออนไลน์ในรูปแบบต่างๆ ยกตัวอย่างการทำงานผ่านโปรแกรม Web Browser เช่น Chrome, Firefox, Microsoft Edge โดยผู้ใช้ต้องนำ Public Key ที่ได้รับ ไปลงทะเบียนกับ Web Browser ก่อนเข้าใช้งานระบบแผนที่ออนไลน์

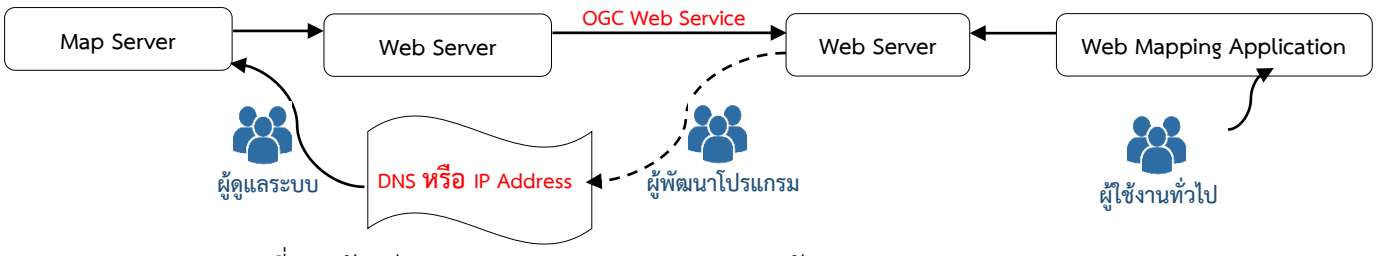


ภาพที่ 9 ตัวอย่างหน้าต่างการตั้งค่าการกำหนด Public key (โปรแกรม Google Chrome)

1.3 การกำหนด HTTP Referrer คือ การจำกัด Domain Name หรือ IP Address ในการเข้าถึง OGC Web Service ที่ผู้ดูแลระบบให้บริการแก่ผู้ใช้งานในระดับผู้พัฒนาโปรแกรม โดยส่วนใหญ่จะตั้งค่าที่โปรแกรม Web Server ที่ทำงานร่วมกับโปรแกรม Map Server ซึ่งผู้ใช้บริการต้องแจ้งผู้ดูแลระบบให้ทราบว่า นำบริการข้อมูลไปใช้ยังโปรแกรมแผนที่ออนไลน์ที่ทำงานบน Domain Name หรือ IP Address ใด จากนั้นผู้ดูแลระบบจะตั้งค่า Web Server ให้ Domain Name หรือ IP Address สามารถเรียกใช้ข้อมูลได้

```
<filter>
  <filter-name>Remote Address Filter</filter-name>
  <filter-class>org.apache.catalina.filters.RemoteAddrFilter</filter-class>
  <init-param>
    <param-name>allow</param-name>
    <param-value>127\.\d+\.\d+\.\d+|::1|0:0:0:0:0:0:0:1</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>Remote Address Filter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

ภาพที่ 10 การตั้งค่าการกำหนด HTTP Referrer (โปรแกรม Apache Tomcat)
แหล่งที่มา : https://tomcat.apache.org/tomcat-7.0-doc/config/filter.html



ภาพที่ 11 ตัวอย่างแผนภาพแสดงระบบความปลอดภัยแบบ HTTP Referrer
แหล่งที่มา : https://tomcat.apache.org/tomcat-7.0-doc/config/filter.html

2. มาตรการรักษาความปลอดภัยในการเข้าใช้งานระบบ NGIS Portal

ระบบ NGIS Portal มีแนวทางการรักษาความปลอดภัยของข้อมูลภายในระบบ 3 รูปแบบ ดังนี้

2.1 การควบคุมการเข้าถึงผ่านการระบุตัวตน (Authentication) ด้วยการกำหนดให้ใช้ Username และ Password ในการเข้าใช้งานระบบ ซึ่งการกำหนดสิทธิ์การเข้าใช้งานนั้น มีการจัดเก็บข้อมูลผู้ใช้งานโดยคำนึงถึงคือแหล่งที่มาของผู้ใช้งาน (User) และกลุ่มผู้ใช้งาน (Group) หรือที่เรียกว่า Identity store โดยระบบ NGIS Portal รองรับระบบจัดเก็บข้อมูลผู้ใช้งานในรูปแบบที่สามารถจัดเก็บข้อมูลผู้ใช้งาน (User) และกลุ่มผู้ใช้งาน (Group) ที่อยู่ภายนอกระบบฯ ได้ โดยผู้ใช้งานสามารถเข้าใช้งานระบบ NGIS Portal จากแหล่งข้อมูลผู้ใช้งานอื่น ๆ ได้โดยระบบจัดเก็บข้อมูลผู้ใช้งานในรูปแบบนี้ มีความสามารถในการทำงาน ดังต่อไปนี้

1. ผู้ดูแลระบบสามารถดึงผู้ใช้งาน (User) และกลุ่มผู้ใช้งาน (Group) จากภายนอกมาใช้งานกับระบบ NGIS Portal ได้โดยไม่จำเป็นต้องสร้าง User จากภายในระบบ (กรณีที่มี AD, LDAP หรือ SAML)
2. สามารถเข้าใช้งานแบบ Single sign-on ซึ่งเป็นระบบการยืนยันตัวบุคคล (Authentication) ที่รองรับการให้ผู้ใช้งานลงชื่อเข้าใช้งานระบบ (Login) เพียงครั้งเดียว แล้วสามารถเข้าใช้งานหลายระบบได้โดยไม่ต้องลงชื่อเข้าใช้งานซ้ำอีก
3. สามารถกำหนดสิทธิ์การเข้าใช้งาน เช่น ไม่อนุญาตให้ผู้ใช้งานที่ไม่ระบุตัวตน (Anonymous) เข้าใช้งานระบบได้
4. สามารถกำหนดนโยบายการหมดอายุของผู้ใช้งาน (User) และกลุ่มผู้ใช้งาน (Group) และกำหนดความซับซ้อนของ Password ได้
5. สามารถทำงานร่วมกับโปรโตคอล Integrated Windows Authentication (IWA) หรือ Public Key Infrastructure (PKI) ในการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลได้
6. รองรับการใช้งานแบบ Multiple identity stores หรือการทำงานร่วมกันระหว่างแหล่งจัดเก็บข้อมูลผู้ใช้งานหลายแห่ง กล่าวคือ การเข้าใช้งานระบบนั้น ผู้ใช้งาน (User) และกลุ่มผู้ใช้งาน (Group) สามารถถูกกำหนดได้จากภายในระบบเอง ร่วมกับผู้ใช้งาน (User) จากภายนอกได้พร้อม ๆ กัน

2.2 การแลกเปลี่ยนข้อมูลโดยใช้โปรโตคอล HTTPS

ระบบ NGIS Portal จะกำหนดค่าตั้งต้นในการให้บริการแลกเปลี่ยนข้อมูลด้วยโปรโตคอลหลักเป็น HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) หรือ HTTP over SSL ซึ่งเป็นโปรโตคอลสื่อสารที่ทำงานอยู่บนระบบโปรโตคอล TCP Port 443 ทำงานโดยการเพิ่มข้อมูลในการระบุตัวผู้ส่ง (Authentication) และการเข้ารหัสข้อมูล (Encryption) ภายใน HTTP กับ TCP มีการส่งข้อมูลเป็นแบบ Cipher text กล่าวคือ ข้อมูลที่ทำการส่งได้ถูกเข้ารหัสเอาไว้ โดยใช้กุญแจสองตัวในการเข้ารหัสและถอดรหัสข้อมูล (Asymmetric Algorithm) ซึ่งแม้ถูกดักจับได้ก็ไม่สามารถที่จะอ่านข้อมูลนั้นได้รู้เรื่อง ข้อมูลนั้นจะสามารถถูกอ่านโดยตัวเจ้าของข้อมูลกับเครื่อง Server เท่านั้น โดยการใช้งานโปรโตคอล HTTPS สามารถทำได้โดยการจดทะเบียน SSL Certificates รายละเอียดตามข้อที่ 4.

2.3 การเชื่อมโยงข้อมูลผ่านเครือข่าย GIN

เครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (Government Information Network : GIN) เป็นบริการเครือข่ายสารสนเทศกลางของภาครัฐที่เชื่อมโยงหน่วยงานภาครัฐเข้าด้วยกัน เพื่อสนับสนุนระบบบริการหน่วยงานภาครัฐให้ใช้งานได้อย่างมีประสิทธิภาพตลอดเวลาและต่อเนื่อง ใช้เทคโนโลยีสารสนเทศประสิทธิภาพสูงในการพัฒนาระบบบริหารจัดการและระบบบริการภาครัฐที่มั่นคงปลอดภัย รวดเร็ว และประหยัดงบประมาณ ซึ่งถูกออกแบบให้มีระบบป้องกันการโจมตีจากเครือข่ายภายนอก โดยสามารถทำหน้าที่เปรียบเสมือนเป็นหน้าด่านในการเฝ้าระวังผู้บุกรุกและจัดการกับไวรัสหรือข้อมูลแปลกปลอม เพื่อไม่ให้เกิดความเสียหายต่อเครือข่ายและอุปกรณ์เชื่อมต่อต่างๆ ของหน่วยงานภาครัฐ (VLAN, VPN, Firewall, IPS ฯลฯ) โดยสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) หรือ EGA เป็นผู้ดูแลดำเนินงานและเป็นระบบเครือข่ายที่รองรับการใช้งาน IPv6 เพื่อเชื่อมโยงเครือข่ายทั่วประเทศอย่างทั่วถึง ซึ่งผู้ที่สามารถใช้งานข้อมูลต่างๆ นั้นจะมีเพียงหน่วยงานภาครัฐเท่านั้น ทำให้มีความปลอดภัยในระดับหนึ่ง เพราะบุคคลภายนอกจะไม่สามารถเชื่อมต่อเครือข่ายนี้ได้

โครงสร้างพื้นฐานสำหรับจัดเก็บทรัพยากร (G-Cloud)

ผู้ดูแลระบบ NGIS Portal โดยสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (สทอภ.) ได้รับการจัดสรรโครงสร้างพื้นฐานบนอินเทอร์เน็ตแบบใช้ทรัพยากรร่วมกัน หรือ Government Cloud (G-Cloud) จากสำนักงานรัฐบาลอิเล็กทรอนิกส์ (สรอ.) ซึ่งเป็นโครงสร้างพื้นฐานสำหรับเก็บทรัพยากรไว้บนอินเทอร์เน็ต สามารถเรียกใช้งานผ่านเครือข่ายได้ตลอดเวลาจากระยะไกล ปรับขนาดได้ตามความต้องการของผู้ใช้ มีการจัดสรรทรัพยากร ลดภาระการบริหารจัดการ และมีความมั่นคงปลอดภัยสูง

โดยระบบ G-Cloud มีมาตรการการดูแลรักษา และการรักษาความปลอดภัยของข้อมูล ดังนี้

1. G-Cloud ให้บริการตามความต้องการจริง โดยจัดสรรทรัพยากรให้เหมาะกับความต้องการของผู้ใช้งาน ซึ่งรวมถึง จำนวนเครื่องแม่ข่ายเสมือน ระบบปฏิบัติการ หน่วยความจำ หน่วยประมวลผลกลาง
2. มีเจ้าหน้าที่ผู้เชี่ยวชาญบริการให้คำปรึกษาตลอด 24 ชั่วโมง ลดภาระในการบริหารจัดการ และดูแลรักษาระบบ ทำให้บุคลากรของหน่วยงานสามารถทุ่มเทเวลาในการให้บริการหน่วยงานภาครัฐได้อย่างเต็มที่
3. มีความปลอดภัยสูง เพราะเป็นระบบ Cloud Computing มาตรฐานสากล ใช้เฉพาะหน่วยงานภาครัฐเท่านั้น บริหารจัดการโดยหน่วยงานกลางของภาครัฐ และมีเสถียรภาพ (SLA) ไม่น้อยกว่า 99.5 %
4. ช่วยหน่วยงานลดความซ้ำซ้อนด้านการลงทุน เช่น อุปกรณ์ เครื่องแม่ข่าย อุปกรณ์เครือข่าย รวมถึง Data Center
5. สามารถเข้าถึงได้จากเครือข่าย GIN (เครือข่ายสื่อสารข้อมูลเชื่อมโยงภาครัฐ) และอินเทอร์เน็ต
6. รองรับระบบงานสนับสนุน Cloud ทุกระดับที่ สรอ. พัฒนาเพื่อให้บริการ รวมถึงบริการพื้นฐาน (Common Service) จากภาครัฐส่วนกลาง

3. ประเด็นสำคัญที่หน่วยงานควรพิจารณาในการให้บริการข้อมูลผ่านระบบ NGIS Portal

ในการให้บริการข้อมูลผ่านระบบ NGIS Portal นั้น ผู้ดูแลระบบของหน่วยงาน ควรพิจารณาถึงประเด็นสำคัญก่อนการให้บริการข้อมูล ดังต่อไปนี้

3.1 การควบคุมการเข้าถึง (Access control) : นอกจากการควบคุมการเข้าถึงด้วย Software ผ่านการระบุตัวตน (Authentication) ตามรายละเอียดในข้อ 1.1 แล้ว หน่วยงานควรมีการกำหนดสิทธิ์ในการเข้าใช้งาน (Authorization) โดยการอนุญาตให้เฉพาะผู้ที่เกี่ยวข้องและสามารถยืนยันตัวตนได้ ที่จะสามารถมีบัญชีผู้ใช้งานในการเข้าใช้งานระบบ NGIS Portal ตามอำนาจหน้าที่และเงื่อนไขที่หน่วยงานกำหนดเท่านั้น

3.2 การจำกัด Domain Name หรือ IP Address ในการเข้าถึงข้อมูล : ผู้ดูแลระบบควรสามารถตรวจสอบ Domain Name หรือ IP Address ของผู้ใช้งาน เพื่ออนุญาต หรือ จำกัดสิทธิ์ในการเข้าถึงข้อมูลในแต่ละกรณี

3.3 กลุ่มเป้าหมายที่ต้องการให้เข้าถึงข้อมูล : ในการให้บริการข้อมูลนั้น หน่วยงานควรพิจารณาถึงกลุ่มเป้าหมายที่ต้องการให้สามารถเข้าถึงข้อมูลได้ โดยระบบ NGIS Portal สามารถตั้งค่าขอบเขตการเผยแพร่ข้อมูลและสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานในแต่ละส่วนได้ ซึ่งหากเป็นชั้นข้อมูลที่สุ่มเสี่ยงต่อการเผยแพร่อาจตั้งค่าเป็นชั้นข้อมูลลับ และเผยแพร่เฉพาะในกลุ่มผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

4. ความสำคัญและแนวทางการจดทะเบียนระบบรักษาความปลอดภัยของการรับ-ส่งข้อมูลทางอินเทอร์เน็ต (Security Socket Layer :SSL)

4.1 SSL Certificates คืออะไร?

SSL Certificates คือใบรับรองความปลอดภัยทางอิเล็กทรอนิกส์บนมาตรฐาน SSL (Security Socket Layer) ที่อนุมัติให้แก่เว็บไซต์โดยองค์กรกลางผู้ออกใบรับรอง หรือเรียกโดยทั่วไปว่า CA (Certificate Authority) เป็นโปรโตคอลที่ใช้เป็นมาตรฐานในการเพิ่มความปลอดภัยสำหรับการรับส่งข้อมูลผ่านระบบอินเทอร์เน็ต ระหว่างเครื่อง Server กับ Web browser หรือ Application ที่ใช้งาน เพื่อให้ข้อมูลปลอดภัยจากการเข้าถึงโดยผู้ไม่ประสงค์ดี ซึ่งใบรับรองนี้จะช่วยสร้างความน่าเชื่อถือให้แก่เว็บไซต์ เนื่องจากข้อมูลทั้งหมดที่ผู้เยี่ยมชมเว็บไซต์กรอกบนหน้าเว็บ เช่น ข้อมูลส่วนตัว รหัสผ่าน หมายเลขบัตรเครดิต และข้อมูลความลับต่างๆ เป็นต้น จะถูกเข้ารหัสเพื่อปกป้องข้อมูล เพื่อลดปัญหาการเกิดอาชญากรรมทางอิเล็กทรอนิกส์ (E-crime) จึงทำให้ปัจจุบันมีการใช้งาน SSL Certificates อย่างแพร่หลาย โดยเฉพาะอย่างยิ่ง สำหรับเว็บไซต์ขององค์กรที่ต้องการสร้างความมั่นใจให้แก่ผู้ใช้งาน โดยวิธีการเรียกใช้งานเว็บไซต์ที่มี SSL Certificates จะเรียกผ่านโปรโตคอล HTTPS โดยจะมี URL ที่ขึ้นต้นด้วย https:// (ซึ่งเว็บไซต์ที่ไม่ได้จดทะเบียนจะมีเพียง http:// เท่านั้น) และเมื่อเข้าสู่เว็บไซต์ จะมีข้อความปรากฏให้ทราบว่าเป็นเว็บไซต์ที่มีการรับรองความปลอดภัย ดังภาพตัวอย่าง

ภาพที่ 12 แสดงการรับรองความปลอดภัยด้วย SSL Certificates ของระบบ NGIS Portal

4.2 ความสำคัญและประโยชน์ของการจดทะเบียน SSL Certificates

1) สร้างความน่าเชื่อถือให้กับเว็บไซต์ เนื่องจากข้อมูลที่มีการรับ – ส่งในเว็บไซต์จะถูกเข้ารหัสเพื่อปกป้องข้อมูล ซึ่งแม้ว่าข้อมูลจะถูกดักจับได้โดยผู้ไม่ประสงค์ดี ข้อมูลก็จะยังมีความปลอดภัย เนื่องจากผู้ไม่ประสงค์ดีที่ดักจับข้อมูลไปนั้น จะไม่สามารถถอดรหัสข้อมูลได้ เพราะข้อมูลจะอยู่ในรูปแบบที่อ่านไม่ออก จะต้องมีคีย์ถอดรหัสที่เหมาะสมและตรงกันเท่านั้น จึงจะสามารถถอดรหัสได้

2) ผู้ดูแลระบบจะสามารถทราบได้ทันที หากมีการเปลี่ยนแปลงหรือดักจับข้อมูลระหว่างการรับ - ส่งข้อมูลจากเว็บไซต์ต้นทาง ซึ่งจะช่วยในการติดตามการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต ทำให้ข้อมูลสำคัญที่ถูกส่งผ่านระบบเครือข่ายมีความปลอดภัยมากยิ่งขึ้น

3) สามารถใช้งานฟังก์ชัน Geolocation ที่มีให้บริการในเว็บไซต์ได้ เนื่องจากในปัจจุบัน ทุกเบราว์เซอร์มีการประกาศใช้งานมาตรฐาน SSL อย่างเป็นทางการ หากเว็บไซต์ใดไม่มี SSL Certificates จะไม่สามารถใช้งานฟังก์ชัน Geolocation ได้

4) Google ให้น้ำหนักความสำคัญในการค้นหาแก่เว็บไซต์ที่มีการปกป้องข้อมูลด้วย SSL Certificates เป็นหนึ่งในคะแนนการจัดอันดับเว็บไซต์ในผลลัพธ์การค้นหา และอาจจะพิจารณาเพิ่มน้ำหนักคะแนนมากขึ้นต่อไปในอนาคต

5) SSL Certificate มีการรับประกันความสูญเสีย โดยมูลค่า/รูปแบบของการรับประกัน จะขึ้นอยู่กับประเภทที่จดทะเบียน หากเกิดความเสียหายแก่ข้อมูลใดๆ ในเว็บไซต์ สามารถแจ้งเรียกร้องสิทธิ์จากความสูญเสียที่เกิดขึ้นจริงได้ ตามเงื่อนไขของผลิตภัณฑ์นั้นๆ (โดยส่วนใหญ่จะใช้กับเว็บไซต์ที่มีการดำเนินธุรกรรมทางการเงิน)

6) ปัจจุบันหลายหน่วยงานของโลก ทั้งในภาครัฐและภาคเอกชน เช่น องค์การบริหารการบินและอวกาศแห่งชาติ (NASA), องค์การสหประชาชาติ (UNESCO), องค์การค้าโลก (WTO), กองบัญชาการกองทัพไทย เป็นต้น มีการใช้งานมาตรฐาน SSL ในการรักษาความปลอดภัยของข้อมูลแพร่หลายมากยิ่งขึ้น การใช้งาน SSL Certificates จึงเปรียบเสมือนเป็นการปรับตัวเพื่อรองรับแนวโน้มการเปลี่ยนแปลงทางเทคโนโลยีของโลก

4.3 การใช้งานระบบ NGIS Portal ที่มีการจดทะเบียน SSL Certificates

ระบบ NGIS Portal มีการจดทะเบียน SSL Certificates ในการรับรองความปลอดภัยของระบบ โดยหากมีการนำข้อมูลภูมิสารสนเทศในรูปแบบ Web Service จากเว็บไซต์ต้นทางที่ไม่มีการจดทะเบียน SSL Certificates หรือไม่ได้ใช้งานโปรโตคอล HTTPS เข้าสู่ระบบ NGIS Portal จะปรากฏข้อความแจ้งเตือนว่าข้อมูลดังกล่าวไม่มีความปลอดภัย อย่างไรก็ตาม ผู้ใช้งานยังสามารถใช้งานข้อมูล Service ที่ไม่มีโปรโตคอล HTTPS ได้แต่จะไม่สามารถใช้งานฟังก์ชันที่เกี่ยวข้องกับ Geolocation เช่น การหาตำแหน่งปัจจุบัน ได้

4.4 แนวทางการจดทะเบียน SSL Certificates ให้กับเว็บไซต์ของหน่วยงาน

- **ติดต่อขอรับบริการจากองค์กรผู้ออกใบรับรอง (Private SSL)**

เป็นวิธีที่นิยมใช้งานอย่างแพร่หลายทั่วโลก เนื่องจากมีความน่าเชื่อถือสูงสุด โดยเมื่อเข้าสู่เว็บไซต์จะปรากฏข้อความให้ทราบว่าเว็บไซต์มีความปลอดภัย และมีสัญลักษณ์รูปกุญแจสีเขียวอยู่หน้า URL การติดตั้ง SSL รูปแบบนี้ จะต้องจดทะเบียนเพื่อซื้อ SSL Certificates จากองค์กรกลางผู้ออกใบรับรอง หรือเรียกโดยทั่วไปว่า CA (Certificate Authority) ซึ่งปัจจุบันมีหลายรายที่ให้บริการ เช่น Symantec, Entrust, Thawte, GoTrust, Digicert เป็นต้น ซึ่งการออกใบรับรอง SSL Certificate นั้น จะต้องมีการพิสูจน์ตัวตน (Authentication) และการยืนยันตัวตน (Verification) ก่อน เพื่อยืนยันความน่าเชื่อถือขององค์กรหรือหน่วยงานที่ประสงค์จะขอจดทะเบียน ทั้งนี้ ขั้นตอนวิธีการในการจดทะเบียน SSL Certificate มีดังต่อไปนี้

1) การเลือก Certificate Authority (CA) ที่ต้องการรับบริการ : โดยสามารถเลือก CA และประเภทของ SSL ที่เหมาะสมกับหน่วยงานและสอดคล้องกับวัตถุประสงค์ของเว็บไซต์ของหน่วยงานมากที่สุดได้ ทั้งนี้ ประเทศไทยมีเว็บไซต์กลางที่เป็นตัวแทนจำหน่ายของ CA หลายรายในโลก โดยเข้าไปที่เว็บไซต์ https://www.ssl.in.th จะมีรายละเอียดเปรียบเทียบการให้บริการ ทั้งในส่วนของประเภท ราคา อายุของใบรับรอง การรับประกัน รายละเอียดการติดต่อขอจดทะเบียน และอื่นๆ ของ CA แต่ละรายที่ให้บริการ
2) การพิสูจน์และยืนยันตัวตน (Authentication and Verification) : แต่ละ CA จะมีข้อกำหนดในการพิสูจน์และยืนยันตัวตนที่แตกต่างกันไป และขึ้นอยู่กับรูปแบบ/ขอบเขตการรับรองที่หน่วยงานเลือกจดทะเบียนด้วย แต่โดยทั่วไปแล้ว หากจดทะเบียนในนามองค์กร/หน่วยงานภาครัฐจะมีการตรวจสอบเพื่อพิสูจน์ตัวตนที่ค่อนข้างเข้มงวดกว่าองค์กรทั่วไป เพื่อความปลอดภัยของภาครัฐ โดยเอกสารหลักฐานที่จำเป็นต้องจัดเตรียมเพื่อประกอบการขอจดทะเบียน ได้แก่
   - เอกสารพรบ.จัดตั้งขององค์กร
   - เอกสารสำเนาบัตรประจำตัวผู้เสียภาษีขององค์กร
   - ลิงค์ของหน่วยงานที่ปรากฏในเว็บไซต์นามสงเคราะห์ส่วนราชการไทย : Thailand Government Directory ที่ http://gphone.prd.go.th/index.php

- เอกสารอื่นๆ ที่แสดงความน่าเชื่อถือขององค์กร เช่น เอกสารการลงทะเบียนกับ Dun and Bradstreet (Thailand) ที่เว็บไซต์ http://www.dnbthailand.com/index-th.html ซึ่งเป็นหน่วยงานผู้ให้บริการฐานข้อมูลที่น่าเชื่อถือของโลก

ทั้งนี้ หากยังไม่สามารถตรวจสอบองค์กรด้วยเอกสารหลักฐานเบื้องต้นดังกล่าวแล้ว CA จะส่งเรื่องให้ Global A&V ซึ่งเป็นองค์กรกลางในการตรวจสอบองค์กรทั่วโลก เพื่อทำการ Verify Call หรือติดต่อทางโทรศัพท์เพื่อยืนยันตัวตนโดยตรงกับผู้บริหาร/ผู้ที่ได้รับมอบหมายจากผู้บริหารขององค์กรนั้นๆ ต่อไป โดยในกรณีที่ไม่มีเอกสารยืนยันองค์กร จะต้องมีเอกสารการรับรององค์กร ที่ลงนามโดยอัยการ/ผู้พิพากษาที่มีใบอนุญาตตามกฎหมายไปแสดง

3) การติดตั้ง SSL Certificates ให้กับเว็บไซต์ : เมื่อได้รับ SSL Certificates เรียบร้อยแล้ว ผู้ดูแลเว็บไซต์จะต้องทำการติดตั้งให้กับเครื่องแม่ข่ายด้วยตนเอง โดยสามารถดูวิธีการติดตั้งได้ที่ https://ssl.in.th/tools/installation-ssl/

- **ใช้บริการ Web Hosting (Shared SSL)**

เป็นรูปแบบการติดตั้ง SSL เพื่อยกระดับการรักษาความปลอดภัยของข้อมูลโดยไม่ต้องมีค่าใช้จ่าย โดยการแชร์ SSL จาก Web Hosting ที่ให้บริการ ซึ่งเป็นทางเลือกสำหรับเว็บไซต์ที่ต้องการใช้ SSL แต่ไม่สะดวกที่จะซื้อ SSL Certificates เองโดยตรง ทั้งนี้ ข้อเสียคือ ในการเรียกใช้งานเว็บไซต์ จะต้องเรียกผ่านโดเมนของ Web Hosting ไม่สามารถเรียกผ่านชื่อโดเมนของเว็บไซต์ได้โดยตรง (ขึ้นอยู่กับ Web Hosting ที่เลือกใช้) และผู้ดูแลเว็บไซต์ต้องต่ออายุ SSL ด้วยตนเองในทุก 90 วัน

- **สร้าง Certificates File เพื่อติดตั้งเอง (Self Signed Certificates)**

เป็นรูปแบบการติดตั้ง SSL โดยไม่ได้ซื้อ SSL Certificates มาติดตั้ง แต่ผู้ดูแลเว็บไซต์จะทำการสร้าง Certificates File ขึ้นมาเอง แต่ SSL Certificate ที่ได้รับมา จะไม่ผ่านการรับรองที่เป็นมาตรฐานจากทาง CA ดังนั้น เมื่อนำไปใช้งานจริง เบราว์เซอร์ที่เข้าใช้งานเว็บไซต์ดังกล่าว จะขึ้นแจ้งเตือนว่า SSL certificate ไม่ปลอดภัย และมีรูปกุญแจสีแดงกับสัญลักษณ์กากบาท ปรากฏขึ้นที่หน้า URL ผู้ใช้งานต้องกด Continue เพื่อยอมรับความเสี่ยงจึงจะสามารถเข้าใช้งานได้ ส่วนใหญ่เว็บไซต์ที่ให้บริการผ่าน Intranet จะใช้ SSL รูปแบบนี้ ซึ่งแม้ว่าจะเป็นวิธีที่ง่าย แต่เป็นวิธีที่ไม่แนะนำ และได้รับความนิยมน้อย

ฝ่ายเลขานุการคณะกรรมการภูมิสารสนเทศแห่งชาติ กภช.

กระทรวงวิทยาศาสตร์และเทคโนโลยี (วท.)
เลขที่ 75/47 กระทรวงวิทยาศาสตร์และเทคโนโลยี
อาคารพระจอมเกล้า ถ.พระราม 6 เขตราชเทวี กรุงเทพฯ 10400
โทรศัพท์ : 02 333 3700 โทรสาร : 02 333 3833

สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา เลขที่ 120 หมู่ 3
อาคารรัฐประศาสนภักดี ชั้น 6 และชั้น 7
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ 02 141 4412 โทรสาร 02 143 9594
E-mail : thainsdi@gistda.or.th