การพิสูจน์ตัวตนแบบรวมศูนย์ เพื่อนำไปสู่การรวมศูนย์ระบบสารสนเทศ Federated Identity Management

วิชญ์ศุทธ์ เมาะพงษ
ที่ปรึกษาโครงการประจำกระทรวง ICT
สังกัดสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

ในปัจจุบันแต่ละองค์การมีการพัฒนา หรือจัดหาระบบสารสนเทศมาใช้งานเพื่อตอบสนองความต้องการในด้านต่างๆ ช่วยให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพ แต่เมื่อเริ่มเอาระบบสารสนเทศเข้ามาใช้อำนวยความสะดวกมากขึ้นจะเพื่อเป้าประสงค์ใดๆ ก็ตามแต่จำนวนของระบบสารสนเทศก็เพิ่มมากขึ้นเป็นเงาตามตัว ซึ่งแต่ละระบบก็เกิดขึ้นและมีการปรับเปลี่ยนรูปแบบ Version หรือพัฒนาขึ้นมาใหม่เพื่อทดแทนเทคโนโลยีเดิม เป็นวัฏจักรวงจรอายุของแต่ละระบบ ด้วยความแตกต่างของเทคโนโลยีที่ใช้ ระยะเวลาที่เปิดให้บริการ ซึ่งบางระบบในบางองค์การให้บริการมายาวนานนับ 10 ปีทั้งหลาย ทั้งปวงนั้น สร้างความยุ่งยากให้กับผู้ดูแลบริหารจัดการ การใช้งานระบบสารสนเทศและทรัพยากรที่เกี่ยวข้องขององค์การเป็นอย่างมากและส่งผลในแง่ของความยุ่งยากซับซ้อนไปถึงผู้ใช้งานอย่างหลีกเลี่ยงไม่ได้ในที่สุด ซึ่งอันที่จริงแล้วระบบสารสนเทศน่าจะเข้ามาช่วยลดภาระงาน ช่วยให้สามารถทำงานได้ง่ายขึ้นสะดวกรวดเร็วยิ่งขึ้น แต่เมื่อถึงจุดหนึ่งความสะดวกสบายกลับกลายเป็นความยุ่งยากขึ้นมาโดยไม่ทันตั้งตัว ดังนั้น จึงมีหลายองค์การที่พยายามจะลดความยุ่งยากซับซ้อนลง โดย**การทำระบบแบบรวมศูนย์** (Federation) ซึ่งนับเป็นเป้าหมายสูงสุดของการบริหารจัดการโครงสร้างพื้นฐานทางด้านสารสนเทศในปัจจุบัน

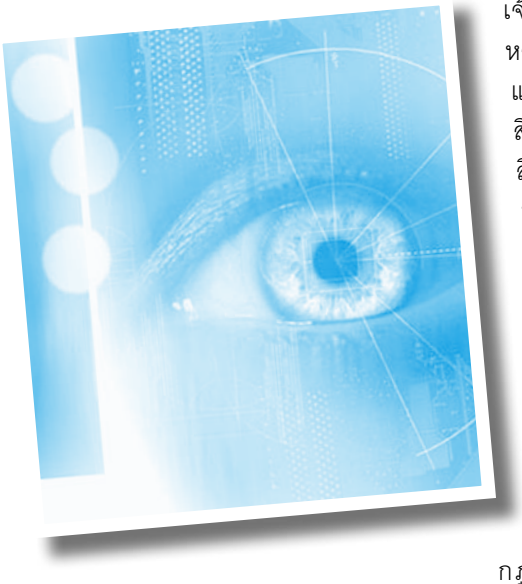
โดยปกติแล้วผู้ใช้งานแต่ละคนจะมีสิทธิ หรือหน้าที่รับผิดชอบในการเข้าใช้งาน

ระบบสารสนเทศขององค์การแตกต่างกัน แต่ที่แน่ๆ คือ ต้องใช้งานคนละหลายๆ ระบบ หากจะทำระบบเป็นแบบรวมศูนย์เพื่อลดความซ้ำซ้อนในการเข้าใช้ได้โดยใช้เทคโนโลยี Single Sign ON ยกตัวอย่าง เช่น เดิมใน Web Site ของ MSN, Yahoo หรือแม้แต่ Google จะมีบริการที่หลากหลายและหากต้องการใช้งาน ต้องทำการสมัครและ Login เข้าใช้เฉพาะบริการใดบริการหนึ่ง แต่ ณ ปัจจุบันเพียงแค่ Login ที่บริการหลักตัวใดก็ตาม ก็สามารถใช้งานได้ในเกือบทุกบริการที่เปิดให้ใช้งานอยู่ เป็นต้น

จะเห็นได้ว่าสิ่งที่เกิดขึ้นแล้วในปัจจุบันที่ยกตัวอย่างมานี้กำลังจะเปลี่ยนรูปแบบการให้บริการระบบสารสนเทศที่ยุ่งยากซับซ้อนให้ง่ายดายยิ่งขึ้นและมีความปลอดภัยในระดับที่ยอมรับได้ หากจะนำมาประยุกต์ใช้งานกับระบบสารสนเทศภายในองค์การ ซึ่งมีข้อมูลที่สำคัญๆ บรรจุอยู่ภายใน ประเด็นที่ควรคำนึงถึงเป็นอย่างมาก คือ การทำ Identity หรือการพิสูจน์เอกลักษณ์ความมีตัวตนผ่านทางเครือข่ายขององค์การ แต่การจะทำให้สำเร็จได้นั้นต้องการมากกว่าเทคโนโลยี

นับเป็นเวลาหลายปีที่องค์การต่างๆ เก็บสะสม Identity หรือข้อมูลเอกลักษณ์ของเจ้าหน้าที่ ลูกค้าและหุ้นส่วนทางธุรกิจเอาไว้เป็นจำนวนมาก ข้อมูลเหล่านี้นับเป็นข้อมูลสำคัญยิ่งของฐานข้อมูล Identity พื้นฐานขององค์การ แต่เมื่อวันหนึ่งที่ธุรกิจถูกผลักดันให้พัฒนาผลิตภัณฑ์ใหม่และเพิ่มกำลังการผลิตสินค้าต่างๆ รวมถึงระบบสารสนเทศใหม่ๆ จะพบอยู่เสมอว่าฐานข้อมูลเหล่านี้กลับเป็นตัวปัญหาให้ต้องปวดหัว เมื่อต้องให้บริการตามความต้องการของลูกค้า หรือ เจ้าหน้าที่แต่ละราย ซึ่งมันจะมีสิ่งแปลกใหม่อยู่เสมอ ระบบรวมศูนย์ใดๆ ก็เป็นไปไม่ได้สำหรับในกรณีนี้ แต่ในทางกลับกันองค์การจะต้องหันมาพิจารณาการดำเนินการแบบกระจาย หรือการดำเนินการที่ไม่รวมอยู่ที่ใดที่หนึ่ง

สำหรับการทำ “Federated Identity Management” นั้น คือ การรวมเอาระบบจัดการดูแล Identity ตั้งแต่สองระบบ หรือมากกว่ามาทำ Authentication ร่วมกันที่ส่วนกลางและดำเนินงานพิสูจน์อำนาจการเข้าถึงและดำเนินการบนระบบเครือข่าย หรือแลกเปลี่ยนลักษณะ (Attribute) ของ Identity สำหรับผู้ใช้งาน แล้วนำเสนอแนวทางโดยหนึ่งผู้ใช้งาน หรือหนึ่ง Identity สามารถใช้งานได้ทั่วทุกเครือข่าย หรือบริการต่างๆ แต่เบื้องหลังการดำเนินการดังกล่าวนั้น มีอะไรที่ซับซ้อนซ่อนอยู่ ซึ่งก็ไม่ได้เป็นเรื่องที่น่าประหลาดใจอะไร เพราะว่าส่วนที่ยากลำบากที่สุดนั้นไม่ใช่เรื่องเทคโนโลยี แต่กลับเป็นเรื่องของการจัดการความสัมพันธ์ระหว่างกระบวนการหรือธุรกิจเพื่อยืนยันความน่าเชื่อถือให้ได้



เพิ่มความซับซ้อนให้กับผู้ใช้งาน

การรวมศูนย์ หรือการทำ Federation นั้น บางทีก็ดูง่ายและดูแลควบคุมได้ไม่ลำบากนัก ยกตัวอย่างเช่น ถ้าเราเสนอบริการผ่านระบบออนไลน์อย่างหนึ่งที่ทำ Federation กับฐานข้อมูล Identity ของลูกข่ายที่ใหญ่ที่สุด สร้างผลประโยชน์ให้มากที่สุดและประกอบกับการที่เคยทำธุรกรรมกับลูกค้าในกลุ่มนั้นๆ มาบ้างแล้ว ทำให้การดำเนินการต่างๆ ง่ายยิ่งขึ้น แต่นั่นต้องไม่นับรวมการดำเนินการเกี่ยวเนื่องกับความเสี่ยงด้านการเงิน หรือข้อมูลส่วนบุคคลในรายละเอียดการส่งต่อความรับผิดชอบดูแลจัดการ Identity ให้กับลูกข่าย นั่นหมายถึง การที่ไม่ต้องมานั่งเปลี่ยน Password ให้ทุกครั้งเวลาที่ลูกค้าลืม Password และ Federation นี้ยังสร้างประโยชน์ให้กับลูกข่ายในองค์การเพิ่มความสะดวกสบายและกระจายการดูแลความปลอดภัยในส่วนที่ไม่จำเป็นลงไปให้ผู้ใช้งานดูแลเองตามชอบใจ การได้ประโยชน์ทั้งสองฝ่ายเช่นนี้ เป็นรูปแบบที่ทำให้การทำ Federation เกิดขึ้นได้ไม่ยากนัก

แต่อย่างไรก็ตามเมื่อผู้ใช้งานได้รับการ Authenticate โดยแผนก หรือฝ่ายหนึ่งในเครือข่ายแล้วจะต้องมีการทำรายการที่เกี่ยวเนื่องกับการเงิน สถานการณ์ก็จะซับซ้อนขึ้นในทันที โดยปัญหานั้นกลับไปสู่เรื่องข้อจำกัดของกฎระเบียบต่างๆ และความรับผิดชอบที่เกิดขึ้น ยกตัวอย่างเช่น ระบบ Federation สำหรับ web Portal ของเจ้าหน้าที่ก็อาจจะมีปัญหาขึ้นมาว่าใครเป็นเจ้าของฐานข้อมูล ซึ่งที่มีความหลากหลายแตกต่างตามหน้าที่ หรือวัตถุประสงค์ แล้วในกรณีที่เกิดปัญหาขึ้นมาใครจะมีสิทธิชี้ขาดในกรณีเกิดความขัดแย้งของสิทธิตามข้อมูล หรือการเข้าถึงข้อมูลเหล่านั้น ปัญหาในเรื่องความเป็นเจ้าของนั้นไม่ได้เป็นเรื่องของลูกค้าภายนอกเพียงอย่างเดียว ซึ่งไม่ว่าจะเป็นความแตกต่างหลากหลายระหว่างฐานข้อมูลบุคคลและการเงิน ก็นับได้ว่าเป็นปัญหาใหญ่ยิ่งกว่านั้นกฎระเบียบต่างๆ ก็กลายเป็นเรื่องใหญ่ได้ โดยเฉพาะในแง่มุมขององค์การข้ามชาติ เนื่องจากต่างประเทศต่างสถานที่ ก็มีการควบคุมด้านตัวบทกฎหมายในเรื่องความคุ้มครองสิทธิเสรีภาพส่วนบุคคลแตกต่างกันออกไป มีทั้งส่วนที่เหมือนและต่าง บางเรื่องก็มีความคลุมเครือ

ในการทำ Out Source งานบางอย่างจะช่วยให้องค์การไม่ต้องรับผิดชอบงานบริการที่ไม่จำเป็น เช่นเดียวกับการทำ Federation ก็ต้องการเฉลี่ยความรับผิดชอบหลายอย่างออกไปให้ผู้ใช้งาน แลกเปลี่ยนกับประสบการณ์การใช้งานที่ดีขึ้นและข้อมูลที่แม่นยำมากยิ่งขึ้นด้วย TPA news

อ่านต่อฉบับหน้า