การพิสูจน์ตัวตนแบบรวมศูนย์ เพื่อนำไปสู่การรวมศูนย์ระบบสารสนเทศ Federated Identity Management จบ

วิชญ์ศุทธ์ เมาะพงษ
ที่ปรึกษาโครงการประจำกระทรวง ICT
สังกัดสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

จุดบกพร่องของ Federation

สำหรับในเชิงบริหารจัดการ Federation น่าจะแบ่งออกได้เป็น 4 ส่วน ได้แก่ สาระทางด้านธุรกิจ ปัญหาและอุปสรรค ความเป็นส่วนตัวของผู้ใช้งาน หรือขององค์การและประเด็นด้านความปลอดภัย รายละเอียดเรื่องธุรกิจนั้นก็จะประกอบไปด้วย ใครทำอะไร ใครจ่ายอะไร และสัญญา แบ่งสรร ปันส่วน ผลประโยชน์ที่ได้อย่างเหมาะสม ซึ่งทั้งหมดก็มักจะเป็นสิ่งที่มีอยู่แล้ว หรือเป็นแนวทางอยู่ในระหว่างการดำเนินการในสัญญาธุรกิจที่มีอยู่เดิม ส่วนการคาดคะเนปัญหาและอุปสรรคดูจะเป็นเรื่องที่ยากกว่า ซึ่งมันมักจะเกี่ยวเนื่องกับความต้องการในการใช้งาน Federation ร่วมกันระหว่างหลายๆ ฝ่ายในที่สุด

โดยทั้งหลายฝ่ายนั้นจะต้องทำความเข้าใจกันก่อนว่า มันเป็นเรื่องของความเสี่ยงที่จะต้องมานั่งคุยกัน ไม่มีสูตรสำเร็จในการคำนวณหรือประเมินความเสี่ยงขึ้นกับธรรมชาติของระบบสารสนเทศและขนาดของความเสี่ยงที่ต้องเผชิญ เพราะระบบสารสนเทศด้านข้อมูลการท่องเที่ยวก็คงจะมีความเสี่ยงน้อยกว่าการจัดการสิทธิดำเนินการด้านการเงินอย่างแน่นอน การตรวจสอบโดยทีมผู้เชี่ยวชาญเป็นประจำก็จะช่วยลดความเสี่ยงลงไปได้บ้าง ไม่ว่าจะเป็นการตรวจสอบจากภายในเองหรือจากการ Out Source ไปเป็นงานภายนอกก็ยังคงสามารถโน้มน้าวให้องค์การคู่ค้าเชื่อมั่นว่าความเสี่ยงที่จะเกิดขึ้นมีอัตราส่วนลดลงได้ แต่อย่าลืมว่าหากคุณรู้อยู่แล้วว่าลูกค้าใช้มาตรฐาน หรือปฏิบัติตามอะไร (เช่น ISO) คุณก็จะต้องโดนชี้นำจากทางลูกค้าให้เข้าสู่มาตรฐานเดียวกันในที่สุด หากคุณต้องรับการตรวจสอบการปฏิบัติตามมาตรฐานของลูกค้าก็จงเตรียมพร้อมรับการตรวจสอบในแบบเดียวกันสำหรับในองค์การของเราเอาไว้ด้วยเช่นกัน

เรื่องความเป็นส่วนตัวในการใช้งานนั้น บางทีในงานสารสนเทศอาจจะไม่ให้ความสำคัญมากนัก แต่สำหรับกรณีของ Federation จะไม่สามารถละเลยเรื่องดังกล่าวไปได้ Federation หลายตัวจะรวมเอา Authentication ง่ายๆ เอาไว้ภายใน ดังนั้น กลุ่มที่ต้องร่วมกันระบุเอกลักษณ์ของแต่ละผู้ใช้งานอาจจะต้องให้ข้อมูลส่วนบุคคลไปยังหุ้นส่วนทางธุรกิจในกลุ่ม Federation ไม่ว่าจะเป็นข้อมูลประกันสังคม วันเกิด หรือแม้แต่เลขบัตรเครดิตในบางที่แล้วแต่ละชนิดของระบบสารสนเทศ ซึ่งในหลายกรณีการใช้งานข้อมูลดังกล่าวนี้ต้องปฏิบัติตามกฎหมาย อย่างในยุโรป หรืออเมริกาโดยเฉพาะที่เกี่ยวกับการเงิน หรือสุขภาพ หรือในบางกรณีอาจจะต้องทำสัญญากับลูกค้าว่าจะดูแลข้อมูลส่วนตัวของลูกค้าแต่ละรายในทางใดทางหนึ่ง

การทำ Federation นั้น หุ้นส่วนทางธุรกิจของเราจะต้องรับรู้ถึงข้อตกลง หรือข้อจำกัดเหล่านี้ด้วยการรู้จักจัดการกับข้อมูลที่มีอยู่เป็นกุญแจสำคัญอันหนึ่งในการทำ Federation ให้ประสบความสำเร็จ มิฉะนั้นแล้วการทำ Federation จะกลายเป็นการขยายข้อมูลที่ผิดพลาดให้ขยายวงกว้างออกไปตามกลุ่มการใช้งาน หรือมีการขโมยข้อมูลเอกลักษณ์ของแต่ละคนไปได้ จะต้องมีระบบตรวจสอบและบ่งชี้ปัญหาเพื่อปรับปรุงแก้ไข รวมถึงการตรวจสอบ ความถูกต้องของข้อมูลที่ได้มาด้วย หากว่าข้อมูลดังกล่าวหมดอายุและไม่มีการ Update แล้ว ก็จะต้องจัดการลบออกจากฐานข้อมูล

ความสำคัญของนโยบาย

เป้าหมายของ Federation นั้นคือการสร้างการกระจายอำนาจและข้อมูลระบุตัวบุคคลเข้าไปในทุกๆ กระบวนการที่สนับสนุนการทำ

ธุรกิจให้ได้มากที่สุด Internet เป็นตัวอย่างที่ดีของระบบดังกล่าว Protocol ที่ใช้และนโยบายในการดำเนินกิจกรรมต่างๆ ทำให้ Internet ดำรงอยู่ได้เป็นอย่างดีเสมอมา เหมือนๆ กับว่าการจะทำ Federation ให้ประสบความสำเร็จนั้น ก็จะต้องให้ความสำคัญกับ Protocol และนโยบายที่สอดคล้อง เลือกเอาตามมาตรฐานหลายอันที่มีว่าสิ่งใดที่เราเห็นด้วยและพร้อมที่จะใช้งานกับสิ่งใดที่ไม่สนใจ บันทึกสิ่งที่เลือกเอาไว้ในนโยบายพิเศษที่เรียกว่า IF (Interoperability Framework) หรือกรอบแนวทางในการปฏิบัติงานร่วม (ของระบบสารสนเทศ) ซึ่งไม่ได้เป็นอะไรที่มากไปกว่ารายการของสิ่งที่องค์การเราเห็นควรที่จะทำนั่นเอง ควรจัดกลุ่มให้เป็นมาตรฐานส่วนที่จำเป็นและส่วนที่จะสนับสนุน ทุกครั้งเมื่อมีการทำ Federation เพราะว่าเราจะต้องติดต่อทำงานร่วมกับหุ้นส่วนทางธุรกิจซึ่งเขาก็จะมี IF ของตนเองเช่นเดียวกันและก็มักจะไม่เหมือนกับที่เราเลือกเอาไว้ 100%

นอกเหนือจากมาตรฐานทางเทคนิคในการดำเนินการแล้ว ยังรวมถึงส่วนสำคัญอื่นๆ อาทิ ธุรกิจ หรือองค์การจะดูแลป้องกันและใช้งานข้อมูลต่างๆ อย่างไร แล้วในนโยบายก็จะต้องระบุด้วยว่าธุรกิจตรวจสอบความน่าเชื่อถือของหุ้นส่วนทางธุรกิจต่างๆ อย่างไร เช่นเดียวกันหัวข้อใดบ้างที่จำเป็นในการพิจารณาในแต่ละโครงการที่แตกต่างกัน ข้อมูลถูกปกป้องมากน้อยแค่ไหน แต่ละหน่วยธุรกิจจะทำงานร่วมกันอย่างไร

องค์การขนาดใหญ่ระดับโลกหลายแห่งได้ใช้แนวทางของ Federated Identity มาจัดการกับความซับซ้อนของการให้บริการระบบสารสนเทศทั้งภายในและภายนอกองค์การ อาทิเช่น Hewlett-Packard หรือ HP ซึ่งได้แสดงให้เห็นว่าการใช้งานระบบ Federated Identity นั้นเทียบเท่ากับการพัฒนาระบบสารสนเทศแบบรวมศูนย์ขึ้นมาใหม่ แต่สามารถประหยัดค่าใช้จ่ายโดยใช้เพียงหนึ่งในสามของค่าใช้จ่ายที่ควรจะเป็นและในแต่ละโครงการที่เกี่ยวข้องทางหัวหน้าโครงการเองต้องพิจารณาเรื่องผลตอบแทนการลงทุนกันอย่างเข้มข้น จึงไม่ได้เป็นการยากเลยที่จะได้รับความเห็นชอบจากทุกฝ่ายแทบจะในทันทีที่แสดงให้เห็นถึงผลประโยชน์ที่จะได้รับ แต่สำหรับรายที่ยังไม่สนใจนโยบายจาก CIO ก็คงต้องใช้เป็นมาตรการบังคับที่จะช่วยผลักดันได้อีกทางหนึ่งและ HP ยังแสดงความเห็นเกี่ยวกับที่ปรึกษา หรือนักวิเคราะห์จากภายนอกองค์การว่า การรับความช่วยเหลือในการตรวจสอบจากภายนอกเป็นการการันตีระบบได้เป็นอย่างดีว่า สามารถทำงานได้จริงจากสายตาคนภายนอกที่ไม่มีส่วนได้ส่วนเสียกับระบบสารสนเทศที่บริหารงานโดยหน่วยธุรกิจต่างๆ กันหลายแห่ง จะเริ่มต้นอย่างไรดี

หลายๆ องค์การที่ประสบความสำเร็จในการทำ Federation นั้นมีสิ่งหนึ่งที่เป็นจุดร่วมที่เหมือนกัน นั่นคือ การสร้าง COE (Center of excellence) ในออฟฟิศของ CIO หรือตั้งคณะกรรมการขึ้นมาดูแลในการดำเนินงานดังกล่าวหรือทั้งสองอย่าง COE นั้น ช่วยกระจายข้อมูลให้ทางเลือกในการดำเนินงานและให้การศึกษาแก่ทีมงานว่า Federation ควรจะถูกใช้งานอย่างไรภายในองค์การและคณะกรรมการก็จะช่วยผลักดันหน่วยธุรกิจเข้าสู่กระบวนการที่เหมาะสม เหมือนอย่างที่ HP ตั้งคณะกรรมการขึ้นมากำกับดูแล ซึ่งทางคณะกรรมการได้ใช้กรณีศึกษาเพื่อสื่อสารกับคนทั่วทั้งองค์การ กับคำถามอาทิ ผู้ใช้งานจะเชื่อมต่อเข้าหากันได้อย่างไร ความเป็นตัวตนของแต่ละคนมีความสำคัญอย่างไร เราจะตระเตรียมการสำหรับการรับการตรวจสอบอย่างไรดี คำถามต่างๆ เหล่านี้ให้ผลดีต่อการสื่อสารเกี่ยวกับสถาปัตยกรรมขององค์การสื่อความให้รู้ถึงสิ่งสำคัญในเชิงนโยบายต่อธุรกิจขององค์การเอง

โครงการ SSO (Single Sign On) ภายในองค์การเป็นจุดเริ่มต้นที่ดี เพราะเราสามารถเลือกมาตรฐานต่างๆ ได้โดยไม่มีความกดดันจากภายนอกองค์การเข้ามาเกี่ยวข้อง ระบบสารสนเทศมากมายที่นำมาใช้งานในระบบ SSO นั้นมักจะเป็นการทำงานที่พึ่งพา Web Application อาจเริ่มต้นอย่างง่ายๆ โดยการ Login เข้า ระบบสารสนเทศพื้นฐานภายในองค์การก่อน ระบบสารสนเทศที่มีการทำงานผ่านเว็บนั้น นับอยู่ใกล้มือที่สุด ซึ่งเราสามารถจะเอื้อมถึงได้ในการทำ Federation เพราะมีผลิตภัณฑ์จัดการการ Login มากมายให้เลือกใช้งานไม่ว่าจะจาก Oracle RSA Novel หรืออื่นๆ

โครงการ Federation ภายในองค์กรนั้นมีข้อดีหลักอีกประการนั่นก็คือ เป็นการผลักดันให้เราทำความสะอาดจัดและระเบียบโครงสร้างภายในองค์การ มันเป็นขั้นตอนแรกที่จะต้องทำและจะสามารถขยายผลได้จากขั้นต้นดังกล่าว หากมองย้อนหลังกลับไปองค์การของเรามีการจัดการเอกลักษณ์หรือ Login ต่างๆ มากมายทั้ง UserID หรือ Password แม้แต่บางครั้งในระบบสารสนเทศเดียวกันยังมีมากกว่าหนึ่งชุดด้วยซ้ำไป โดยในการทำ SSO เราได้เริ่มทำการยุบรวม Directory หรือแฟ้มข้อมูลในระบบต่างๆ ที่เก็บอยู่อย่างกระจัดกระจายเข้าด้วยกัน รวมถึงแนวทาง หรือวิธีการทางที่เราใช้ทำ Authentication ด้วย ซึ่งก่อนหน้านี้เรารู้สึกว่าเราไม่สามารถทำอะไรไปได้มากกว่านี้อีกแล้ว เนื่องจากความซับซ้อนต่าง ๆ ที่มีอยู่มากมาย แต่เมื่อเราได้เริ่มทำ เราก็จะรู้ว่ามันสามารถทำได้และเมื่อเราได้สำรวจการทำ Federation ภายในองค์การจนสามารถควบคุมได้แล้วก็ถึงเวลาที่จะขยายผลออกไปสู่นอกองค์การไปสู่องค์การที่เป็นพันธมิตรและเคยแก้ปัญหา Federation ที่ซับซ้อนมาเหมือนกัน ซึ่งเป็นทางที่ดีที่จะเรียนรู้โดยการทำงานร่วมกัน เพราะเราจะมีสัญญาข้อตกลงหลายประการเป็นแนวทางระหว่างกันอยู่แล้วและเป็นที่น่าสนใจว่าสิ่งที่ท้าทายอันหนึ่งของการทำ Federation ก็คือการประสานงานให้เกิดการคุยกันของสององค์การนั่นเอง มันเป็นการยากที่จะให้องค์การมาแก้ไขปรับปรุงอะไรที่เคยทำเอาไว้อยู่แล้วแต่เดิมซึ่งอาจไม่เห็นประโยชน์ทางธุรกิจใดๆ เลย แต่เมื่อเริ่มดำเนินการได้รายหนึ่งแล้ว รายอื่นๆ ที่ตามมาก็จะง่ายขึ้น TPA news