การรับรองความปลอดภัยและศูนย์การปฏิบัติตามกฎเกณฑ์

ธันวาคม 2564

สารบัญ

บทนำการรับประกันความปลอดภัยของ Apple

ด้วยความยึดมั่นในความปลอดภัย Apple ได้เข้าไปมีส่วนร่วมกับองค์กรอื่นอยู่เสมอเพื่อรับรองและพิสูจน์ยืนยันความปลอดภัยของฮาร์ดแวร์ ซอฟต์แวร์ และบริการของ Apple องค์กรที่ได้รับการยอมรับในระดับสากลเหล่านี้ให้การรับรองที่สอดคล้องกับการเปิดตัวระบบปฏิบัติการครั้งใหญ่แต่ละครั้งกับ Apple ด้วยเหตุนี้ องค์กรเหล่านี้จึงมอบมาตรการที่ให้ความเชื่อมั่นที่ตอบสนองความต้องการด้านความปลอดภัยของระบบ ซึ่งก็คือการรับประกันความปลอดภัย Apple มุ่งมั่นที่จะเข้าไปมีส่วนร่วมในการพัฒนามาตรฐานความปลอดภัยที่เหมาะสมในขอบเขตด้านเทคนิคที่ไม่ได้รับการยอมรับภายใต้การจัดการการยอมรับร่วมกัน (MRA) หรือขอบเขตที่ขาดมาตรฐานการรับรองความปลอดภัยที่ก้าวหน้า ภารกิจของเราคือการผลักดันให้มีการนำการรับรองความปลอดภัยซึ่งเป็นที่ยอมรับทั่วโลกไปใช้กับฮาร์ดแวร์ ระบบปฏิบัติการ แอป และบริการของ Apple อย่างครอบคลุม

โดยส่วนใหญ่แล้ว การรับรองจำเป็นจะต้องเป็นไปตามข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และบรรทัดฐานด้านอุตสาหกรรม บริการอย่าง Apple School Manager และ Apple Business Manager อยู่ภายใต้การรับรอง ISO/IEC 27001 และ ISO/IEC 27018 ของ Apple ลูกค้าทั้งหมด รวมถึงหน่วยงานภาครัฐ องค์กรต่างๆ หรือองค์กรทางการศึกษาที่ปรับใช้อุปกรณ์ของ Apple สามารถใช้การรับรองฮาร์ดแวร์ ระบบปฏิบัติการ ซอฟต์แวร์ และบริการเพื่อสนับสนุนการปฏิบัติตามกฎเกณฑ์ได้

การรับรองฮาร์ดแวร์

เนื่องจากซอฟต์แวร์ที่ปลอดภัยต้องใช้รากฐานความปลอดภัยที่สร้างขึ้นในฮาร์ดแวร์ อุปกรณ์ของ Apple ทั้งหมดจึงมีความสามารถด้านการรักษาความปลอดภัยที่ได้รับการออกแบบลงในซิลิคอน ไม่ว่าจะเป็นอุปกรณ์ที่ใช้ iOS, iPadOS, macOS, tvOS หรือ watchOS ก็ตาม ซึ่งรวมถึงความสามารถของ CPU แบบกำหนดเองที่ให้พลังงานแก่คุณสมบัติด้านความปลอดภัยของระบบ และซิลิคอนที่มุ่งไปที่ฟังก์ชั่นด้านความปลอดภัย ส่วนประกอบที่สำคัญที่สุดคือหน่วยประมวลผลร่วม Secure Enclave ซึ่งมีอยู่บนอุปกรณ์ iOS, iPadOS, watchOS และ tvOS รุ่นใหม่ทุกรุ่น บนคอมพิวเตอร์ Mac ทุกรุ่นที่ใช้ Apple Silicon และคอมพิวเตอร์ Mac ทุกรุ่นที่ใช้ Intel ที่มีชิป Apple T2 Security ซึ่ง Secure Enclave จะใช้รากฐานสำหรับการเข้ารหัสข้อมูลในเครื่อง การบูตอย่างปลอดภัยใน macOS และไบโอเมตริก

ความมุ่งมั่นของ Apple ในการรับประกันความปลอดภัยเริ่มต้นจากการรับรองส่วนประกอบความปลอดภัยพื้นฐานในซิลิคอนจากรากของความเชื่อถือฮาร์ดแวร์ ไปจนถึงการบังคับใช้การบูตอย่างปลอดภัย การจัดเก็บกุญแจอย่าง ปลอดภัยที่สามารถทำได้โดย Secure Enclave ไปจนถึงการตรวจสอบสิทธิ์ที่ปลอดภัยด้วย Touch ID และ Face ID คุณสมบัติความปลอดภัยของอุปกรณ์ของ Apple สามารถเป็นจริงขึ้นมาได้จากการผสมผสานระหว่างการออกแบบซิลิคอน ฮาร์ดแวร์ ซอฟต์แวร์ และบริการที่มีให้เฉพาะจาก Apple เท่านั้น การรับรองของส่วนประกอบเหล่านี้เป็นส่วนที่สำคัญสำหรับการตรวจสอบยืนยันการรับประกันที่ Apple มีให้

สำหรับข้อมูลเกี่ยวกับการรับรองแบบสาธารณะที่เกี่ยวกับส่วนประกอบฮาร์ดแวร์และเฟิร์มแวร์ที่เกี่ยวข้อง ให้ดูที่:

- การรับรองความปลอดภัยสำหรับชิป Apple T2 Security
- การรับรองความปลอดภัยสำหรับหน่วยประมวลผล Secure Enclave

การรับรองซอฟต์แวร์และแอป

Apple มีการรับรองและการพิสูจน์ยืนยันที่เป็นอิสระสำหรับระบบปฏิบัติการและแอปของบริษัทเองซึ่งสอดคล้องกับมาตรฐานการประมวลผลข้อมูลสหรัฐอเมริกากลาง (FIPS) 140-2/-3 สำหรับโมดูลการเข้ารหัสและเกณฑ์ทั่วไปสำหรับระบบปฏิบัติการ แอป และบริการของอุปกรณ์ ระบบปฏิบัติการครอบคลุมถึง iOS, iPadOS, macOS, sepOS, เฟิร์มแวร์ T2, tvOS และ watchOS สำหรับแอปต่างๆ ในเบื้องต้นการรับรองอิสระจะประกอบไปด้วยเบราว์เซอร์ Safari และแอปรายชื่อ ส่วนแอปอื่นๆ จะมีการรับรองเพิ่มขึ้นอีกในอนาคต

สำหรับข้อมูลเกี่ยวกับการรับรองแบบสาธารณะที่เกี่ยวกับ**ระบบปฏิบัติการ**ของ Apple ให้ดูที่:

- การรับรองความปลอดภัยสำหรับ iOS
- การรับรองความปลอดภัยสำหรับ iPadOS
- การรับรองความปลอดภัยสำหรับ macOS
- การรับรองความปลอดภัยสำหรับ tvOS
- การรับรองความปลอดภัยสำหรับ watchOS

สำหรับข้อมูลเกี่ยวกับการรับรองแบบสาธารณะที่เกี่ยวกับ**แอป**ของ Apple ให้ดูที่:

- การรับรองความปลอดภัยสำหรับแอปของ Apple

การรับรองการให้บริการ

Apple มีการรับรองความปลอดภัยเพื่อให้การสนับสนุนลูกค้าของเราตั้งแต่องค์กรไปจนถึงการศึกษา การรับรองเหล่านี้ทำให้ลูกค้าของ Apple สามารถจัดการกับหน้าที่ตามกฎหมายและตามสัญญาของตนได้เมื่อใช้บริการของ Apple ด้วยฮาร์ดแวร์และซอฟต์แวร์ของ Apple การรับรองเหล่านี้ให้การพิสูจน์ยืนยันอย่างอิสระแก่ลูกค้าของเราเกี่ยวกับวิธีปฏิบัติด้านความปลอดภัยของข้อมูลของ Apple, สภาพแวดล้อม และความเป็นส่วนตัวสำหรับสำหรับระบบของ Apple

สำหรับข้อมูลเกี่ยวกับการรับรองแบบสาธารณะที่เกี่ยวกับ**บริการอินเทอร์เน็ต**ของ Apple ให้ดูที่:

- การรับรองความปลอดภัยสำหรับบริการอินเทอร์เน็ตของ Apple

สำหรับคำถามเกี่ยวกับการรับรองความปลอดภัยและความเป็นส่วนตัวของ Apple ให้ติดต่อ security-certifications@apple.com

การรับรองความปลอดภัยด้านฮาร์ดแวร์

ภาพรวมการรับรองความปลอดภัยด้านฮาร์ดแวร์ของ Apple

Apple มีการรับรองการตรวจสอบความถูกต้องด้านความสอดคล้องกับมาตรฐานการประมวลผลข้อมูลสหรัฐอเมริกากลาง (FIPS) 140-2/-3 สำหรับ sepOS และเฟิร์มแวร์ T2 รวมถึงการรับรองอื่นๆ ด้วย Apple เริ่มต้นจาก**โครงสร้างการรับรอง**ที่สามารถปรับใช้ได้ในวงกว้างกับแพลตฟอร์มที่หลากหลายตามความเหมาะสม หนึ่งในโครงสร้างดังกล่าวคือการตรวจสอบความถูกต้องของคลัง corecrypto ที่ใช้ในการปรับใช้โมดูลการเข้ารหัสของซอฟต์แวร์และฮาร์ดแวร์ภายในระบบปฏิบัติการที่พัฒนาโดย Apple โครงสร้างที่สองคือการรับรอง Secure Enclave ซึ่งฝังอยู่ในอุปกรณ์ Apple หลายๆ รุ่น โครงสร้างที่สามคือการรับรอง Secure Element (SE) ที่พบได้ในอุปกรณ์ Apple ทุกเครื่องที่มี Touch ID และอุปกรณ์ที่มี Face ID โครงสร้างการรับรองฮาร์ดแวร์เหล่านี้สร้างรากฐานสำหรับการรับรองความปลอดภัยของแพลตฟอร์มที่กว้างขึ้น

การตรวจสอบความถูกต้องอัลกอริทึมการเข้ารหัส

การตรวจสอบความถูกต้องของการปรับใช้ความถูกต้องของอัลกอริทึมการเข้ารหัสจำนวนมากและฟังก์ชั่นความปลอดภัยที่เกี่ยวข้องเป็นข้อกำหนดเบื้องต้นสำหรับการตรวจสอบความถูกต้อง FIPS 140-3 อีกทั้งสนับสนุนของการรับรองอื่นๆ การตรวจสอบความถูกต้องจะได้รับการจัดการโดยโปรแกรมการตรวจสอบความถูกต้องอัลกอริทึมการเข้ารหัส (CAVP) ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) การรับรองของการตรวจสอบความถูกต้องสำหรับการปรับใช้กับ Apple สามารถดูได้โดยใช้ตัวช่วยอำนวยความสะดวกการค้นหาของ CAVP โปรดดูที่เว็บไซต์โปรแกรมการตรวจสอบความถูกต้องอัลกอริทึมการเข้ารหัส (CAVP) สำหรับข้อมูลเพิ่มเติม

การตรวจสอบความถูกต้องของโมดูลการเข้ารหัส: FIPS 140-2/3 (ISO/IEC 19790)

โมดูลการเข้ารหัสของ Apple ได้รับการตรวจสอบความถูกต้องซ้ำๆ โดยโปรแกรมการตรวจสอบความถูกต้องโมดูลการเข้ารหัส (CMVP) ว่าเป็นไปตามมาตรฐานการประมวลผลข้อมูลสำหรับโมดูลการเข้ารหัสสหรัฐอเมริกากลาง (FIPS 140-2) หลังจากการเปิดตัวครั้งใหญ่แต่ละครั้งของระบบปฏิบัติการตั้งแต่ปี 2555 หลังจากการเปิดตัวครั้งใหญ่ในแต่ละครั้ง Apple จะส่งโมดูลทั้งหมดไปยัง CMVP เพื่อตรวจสอบความถูกต้องเกี่ยวกับความสอดคล้องกับมาตรฐาน นอกจากโมดูลเหล่านี้จะถูกใช้งานโดยระบบปฏิบัติการและแอปของ Apple แล้ว โมดูลเหล่านี้ยังมอบความสามารถด้านการเข้ารหัสให้กับบริการที่ให้บริการโดย Apple และมีให้ใช้งานสำหรับแอปของบริษัทอื่นอีกด้วย

Apple ได้รับ**ความปลอดภัยระดับ** 1 ในแต่ละปีสำหรับโมดูลแบบซอฟต์แวร์ "Corecrypto Module สำหรับ Intel" และ "Corecrypto Kernel Module สำหรับ Intel" สำหรับ macOS สำหรับ Apple Silicon โมดูล "Corecrypto Module สำหรับ ARM" และ "Corecrypto Kernel Module สำหรับ ARM" สามารถใช้ได้กับ iOS, iPadOS, tvOS, watchOS และเฟิร์มแวร์บนชิป Apple T2 Security ที่ฝังอยู่ในคอมพิวเตอร์ Mac

ในปี 2562 Apple ได้รับ**ความปลอดภัยระดับ** 2 FIPS 140-2 สำเร็จเป็นครั้งแรกสำหรับโมดูลการเข้ารหัสฮาร์ดแวร์แบบฝังในที่ระบุเป็น "Apple Corecrypto Module: การจัดเก็บกุญแจอย่างปลอดภัย" ซึ่งทำให้รัฐบาลของสหรัฐอเมริกาอนุญาตให้ใช้กุญแจที่สร้างขึ้นและจัดการใน Secure Enclave Apple เดินหน้าการตรวจสอบความถูกต้องสำหรับโมดูลการเข้ารหัสฮาร์ดแวร์ในระดับความปลอดภัยที่สูงขึ้นอยู่เสมอในการเปิดตัวระบบปฏิบัติการครั้งใหญ่แต่ละครั้ง

FIPS 140-3 ได้รับการอนุญาตโดยกระทรวงพาณิชย์ของสหรัฐอเมริกาในปี 2562 การเปลี่ยนแปลงที่โดดเด่นที่สุดของมาตรฐานในเวอร์ชั่นนี้คือข้อกำหนดมาตรฐาน ISO/IEC โดยเฉพาะอย่างยิ่ง ISO/IEC 19790:2015 และมาตรฐานการทดสอบที่เกี่ยวข้อง ISO/IEC 24759:2017 CMVP ได้เริ่มต้นโปรแกรมการเปลี่ยนผ่านและระบุว่า ตั้งแต่ปี 2563 เป็นต้นไป โมดูลการเข้ารหัสจะเริ่มรับการตรวจสอบความถูกต้องโดยใช้ FIPS 140-3 เป็นพื้นฐาน โมดูลการเข้ารหัสของ Apple มุ่งหมายที่จะปฏิบัติตามและเปลี่ยนไปใช้มาตรฐาน FIPS 140-3 ในทันทีที่สามารถปฏิบัติได้

สำหรับโมดูลการเข้ารหัสที่อยู่ระหว่างกระบวนการทดสอบและการตรวจสอบความถูกต้อง CMVP จะเก็บรักษารายการที่แยกกันสองรายการซึ่งอาจมีข้อมูลเกี่ยวกับการตรวจสอบความถูกต้องที่เสนอ สำหรับโมดูลการเข้ารหัสที่อยู่ระหว่างการทดสอบในห้องปฏิบัติการที่มีการรับรอง รายการการปรับใช้อยู่ระหว่างการทดสอบ อาจระบุโมดูลในรายการ หลังจากที่ห้องปฏิบัติการได้ดำเนินการทดสอบเสร็จสมบูรณ์แล้วและแนะนำให้เข้ารับการตรวจสอบความถูกต้องจาก CMVP โมดูลการเข้ารหัสของ Apple จะแสดงขึ้นในรายการโมดูลในกระบวนการ ตอนนี้การทดสอบในห้องปฏิบัติการเสร็จสมบูรณ์แล้วและรอการตรวจสอบความถูกต้องของการทดสอบโดย CMVP เนื่องจากระยะเวลาของกระบวนการประเมินสามารถผันแปรได้ ให้ดูรายการกระบวนการทั้งสองรายการที่ด้านบนเพื่อระบุสถานะปัจจุบันของโมดูลการเข้ารหัสของ Apple ระหว่างวันที่ที่มีการเปิดตัวระบบปฏิบัติการครั้งใหญ่และการออกการรับรองการตรวจสอบความถูกต้องโดย CMVP

การรับรองผลิตภัณฑ์: (เกณฑ์ทั่วไป ISO/IEC 15408)

เกณฑ์ทั่วไป (ISO/IEC 15408) เป็นมาตรฐานที่หลายองค์กรใช้เป็นพื้นฐานในการดำเนินการประเมินความปลอดภัยของผลิตภัณฑ์ IT

สำหรับการรับรองที่อาจรู้จักกันในชื่อการจัดการรับรองเกณฑ์ทั่วไป (CCRA) ระดับสากล ให้ดูที่พอร์ทัลเกณฑ์ทั่วไป มาตรฐานเกณฑ์ทั่วไปยังอาจมีการใช้ภายนอก CCRA โดยแบบแผนการตรวจสอบความถูกต้องระดับชาติและระดับส่วนตัวอีกด้วย ในยุโรป การยอมรับร่วมกันอยู่ภายใต้ข้อตกลง SOG-IS เช่นเดียวกันกับ CCRA

เป้าหมายก็เพื่อให้ชุดมาตรฐานความปลอดภัยที่ผ่านการรับรองในระดับสากลสามารถประเมินความสามารถด้านการรักษาความปลอดภัยของผลิตภัณฑ์เทคโนโลยีสารสนเทศได้อย่างชัดเจนและน่าเชื่อถือ ซึ่งเป็นเป้าหมายที่ชุมชนเกณฑ์ทั่วไประบุไว้ เมื่อจัดให้มีการประเมินแบบอิสระเกี่ยวกับความสามารถของผลิตภัณฑ์ในการปฏิบัติตามมาตรฐานด้านความปลอดภัย การรับรองเกณฑ์ทั่วไปจึงทำให้ลูกค้ามีความมั่นใจมากขึ้นเกี่ยวกับความปลอดภัยของผลิตภัณฑ์เทคโนโลยีสารสนเทศและตัดสินใจได้อย่างรอบคอบมากขึ้น

ประเทศสมาชิกได้ตกลงที่จะยอมรับการรับรองผลิตภัณฑ์เทคโนโลยีสารสนเทศด้วยความเชื่อมั่นในระดับเดียวกันผ่าน CCRA การประเมินที่จำเป็นก่อนการรับรองจะครอบคลุมและรวมถึง:

- โปรไฟล์การปกป้อง (PP)
- เป้าหมายความปลอดภัย (ST)
- ข้อกำหนดฟังก์ชั่นความปลอดภัย (SFR)
- ข้อกำหนดการรับประกันความปลอดภัย (SAR)
- ระดับการรับประกันการประเมิน (EAL)

โปรไฟล์การปกป้อง (PP) เป็นเอกสารที่ระบุข้อกำหนดด้านความปลอดภัยสำหรับคลาสของประเภทอุปกรณ์ (เช่น อุปกรณ์เคลื่อนที่) ซึ่งใช้สำหรับแสดงการเปรียบเทียบระหว่างการประเมินของผลิตภัณฑ์ IT ภายในคลาสเดียวกัน การเป็นสมาชิกของ CCRA รวมถึงการเพิ่มขึ้นของ PP ที่ได้รับการรับรองมีการเพิ่มขึ้นทุกปีอย่างต่อเนื่อง การทำความตกลงนี้อนุญาตให้นักพัฒนาผลิตภัณฑ์ใช้การรับรองเดียวภายใต้แบบแผนการอนุญาตการรับรองแบบใดแบบหนึ่งและกำหนดให้ได้รับการยอมรับจากผู้ลงนามทุกๆ คนที่ใช้การรับรอง

เป้าหมายความปลอดภัย (ST) กำหนดว่า**อะไรบ้าง**ที่จะได้รับการประเมินเมื่อผลิตภัณฑ์ IT ได้รับการรับรอง ST หมายถึง**ข้อกำหนดฟังก์ชั่นความปลอดภัย (SFR)** ที่เฉพาะเจาะจงยิ่งขึ้น ซึ่งใช้สำหรับการประเมิน ST อย่างละเอียดยิ่งขึ้น

เกณฑ์ทั่วไป (CC) ยังรวมถึง**ข้อกำหนดการรับประกันความปลอดภัย**อีกด้วย ตัววัดหนึ่งที่มักถูกระบุอยู่เป็นประจำก็คือ**ระดับการรับประกันการประเมิน (EAL)** โดย EAL จะรวมกลุ่มชุดของ SAR ที่เกิดขึ้นบ่อยครั้งเข้าด้วยกันและอาจถูกระบุอยู่ใน PP และ ST เพื่อรองรับการเปรียบเทียบ

PP ก่อนหน้านี้จำนวนมากถูกเก็บถาวรและแทนที่ด้วย PP แบบมุ่งเป้าซึ่งได้รับการพัฒนาและมุ่งเน้นโซลูชั่นและสภาพแวดล้อมที่เฉพาะเจาะจง ในความพยายามจากหลายฝ่ายที่จะให้มีการยอมรับร่วมกันระหว่างสมาชิก CCRA ทั้งหมดต่อไป ชุมชนเทคนิคสากล (iTC) ได้ถูกจัดตั้งขึ้นเพื่อพัฒนาและรักษาไว้ซึ่งโปรไฟล์การปกป้องเชิงร่วมมือ (cPP) ซึ่งมีการพัฒนาตั้งแต่เริ่มต้นโดยมีแผนของผู้ลงนาม CCRA ร่วมด้วย PP แบบมุ่งเป้าสำหรับกลุ่มผู้ใช้และการจัดการการยอมรับร่วมกันที่นอกเหนือจาก CCRA จะได้รับการพัฒนาต่อไปโดยผู้ที่ได้รับประโยชน์ร่วมกันที่เหมาะสม

Apple เริ่มใช้การรับรองภายใต้ CCRA ที่ได้รับการอัปเดตกับ cPP ที่เลือกตั้งแต่ต้นปี 2558 ตั้งแต่นั้นมา Apple ก็ได้รับการรับรองเกณฑ์ทั่วไปสำหรับการเปิดตัว iOS ครั้งใหญ่ในแต่ละครั้งและได้ขยายความครอบคลุมให้รวมถึงการรับประกันความปลอดภัยที่ได้จาก PP ใหม่

Apple มีบทบาทเชิงรุกในชุมชนเทคนิคที่มุ่งเน้นการประเมินเทคโนโลยีความปลอดภัยของอุปกรณ์เคลื่อนที่ ซึ่งรวมถึง iTC ที่รับผิดชอบในการพัฒนาและอัปเดต cPP Apple ยังคงประเมินและใช้การรับรองกับ PP และ cPP ที่มีอยู่ในปัจจุบันอย่างต่อเนื่อง

การรองรับแพลตฟอร์ม Apple สำหรับตลาดอเมริกาเหนือปกติแล้วจะดำเนินการโดยความร่วมมือในการรับประกันข้อมูลแห่งชาติ (NIAP) ที่เก็บบันทึกรายการโปรเจ็กต์ที่อยู่ระหว่างการประเมินแต่ยังไม่ได้รับรอง

นอกเหนือจากใบรับรองแพลตฟอร์มทั่วไปแล้ว ยังมีการออกใบรับรองอื่นๆ เพื่อแสดงข้อกำหนดด้านความปลอดภัยที่เฉพาะเจาะจงสำหรับตลาดบางแห่งอีกด้วย

การรับรองความปลอดภัยสำหรับหน่วยประมวลผล Secure Enclave

ความเป็นมาของการรับรอง Secure Enclave

โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัย SEP ของ Apple เป็นโมดูลการเข้ารหัสของฮาร์ดแวร์ที่ฝังอยู่ใน SOC ของ Apple ในผลิตภัณฑ์ต่อไปนี้: ซีรีส์ A สำหรับ iPhone และ iPad, ซีรีส์ M สำหรับคอมพิวเตอร์ Mac ที่ใช้ Apple Silicon, ซีรีส์ S สำหรับ Apple Watch ของ Apple และชิปความปลอดภัยซีรีส์ T ที่พบในคอมพิวเตอร์ Mac ที่ใช้ Intel ซึ่งเริ่มตั้งแต่ iMac Pro ที่เปิดตัวในปี 2560

ในปี 2561 Apple ได้เชื่อมข้อมูลกับการตรวจสอบความถูกต้องของโมดูลการเข้ารหัสซอฟต์แวร์เข้ากับระบบปฏิบัติการที่เปิดตัวในปี 2560: iOS 11, macOS 10.13, tvOS 11 และ watchOS 4 โมดูลการเข้ารหัสฮาร์ดแวร์ SEP ที่ระบุเป็นโมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัย SEP v1.0 ของ Apple ได้รับการตรวจสอบความถูกต้องด้วยข้อกำหนดความปลอดภัยระดับ 1 FIPS 140-2 ในตอนแรก

ในปี 2562 Apple ได้ตรวจสอบความถูกต้องของโมดูลฮาร์ดแวร์ด้วยข้อกำหนดความปลอดภัยระดับ 2 FIPS 140-2 และอัปเดตข้อมูลจำเพาะเวอร์ชั่นของโมดูลเป็น v9.0 เพื่อเชื่อมข้อมูลกับเวอร์ชั่นที่สอดคล้องกันของการตรวจสอบความถูกต้องของโมดูล corecrypto User และ corecrypto Kernel ในปี 2562 ยังรวมถึง iOS 12, macOS 10.14, tvOS 12 และ watchOS 5 ด้วย

ในปี 2563 และ 2564 Apple ใช้การตรวจสอบความถูกต้องสำหรับความสอดคล้องกับ FIPS 140-3 และกับการรับประกันเพิ่มเติมสำหรับความปลอดภัยระดับ 3 ของข้อกำหนดด้านความปลอดภัยทางกายภาพสำหรับ Apple Silicon: ชิป A13, A14, S6 และ M1

นอกจากนี้แล้ว Apple ยังได้เข้าไปมีส่วนร่วมเชิงรุกในการตรวจสอบความถูกต้องโมดูล corecrypto User และ corecrypto Kernel ในการเปิดตัวระบบปฏิบัติการครั้งใหญ่ในแต่ละครั้งอีกด้วย การตรวจสอบความถูกต้องของความสอดคล้องสามารถดำเนินการได้เฉพาะกับเวอร์ชั่นสุดท้ายที่เปิดตัวเท่านั้น

สถานะการตรวจสอบความถูกต้องโมดูลการเข้ารหัส

โปรแกรมการตรวจสอบความถูกต้องโมดูลการเข้ารหัส (CMVP) ยังคงใช้สถานะการตรวจสอบความถูกต้องของโมดูลการเข้ารหัสภายใต้รายการที่แยกออกจากกันสามรายการซึ่งขึ้นอยู่กับสถานะปัจจุบันของแต่ละรายการ:

- ในการที่จะได้รับการระบุอยู่ในรายการการปรับใช้อยู่ระหว่างการทดสอบของ CMVP ห้องปฏิบัติการจะต้องทำสัญญากับ Apple ในการดำเนินการทดสอบ
- หลังจากที่การทดสอบเสร็จสมบูรณ์โดยห้องปฏิบัติการ และเมื่อห้องปฏิบัติการได้แนะนำการตรวจสอบความถูกต้องโดย CMVP และได้ชำระค่าธรรมเนียม CMVP แล้ว จากนั้นโมดูลจะถูกเพิ่มไปยังรายการโมดูลในกระบวนการ รายการ MIP จะติดตามความคืบหน้าของความพยายามในการตรวจสอบความถูกต้องของ CMVP ซึ่งแบ่งเป็นสี่ระยะ:
  - **รอการตรวจสอบ:** รอการกำหนดทรัพยากรของ CMVP
  - **อยู่ในระหว่างการตรวจสอบ:** ทรัพยากรของ CMVP อยู่ในระหว่างดำเนินการกิจกรรมการตรวจสอบความถูกต้อง
  - **ดำเนินการร่วมกัน:** ห้องปฏิบัติการและ CMVP กำลังแก้ไขปัญหาที่พบ
  - **สรุป:** กิจกรรมและระเบียบแบบแผนที่เกี่ยวข้องกับการออกการรับรอง
- หลังจากการตรวจสอบความถูกต้องโดย CMVP โมดูลจะได้รับการรับรองความสอดคล้องและถูกเพิ่มไปยังรายการโมดูลการเข้ารหัสที่ได้รับการตรวจสอบความถูกต้องแล้ว ซึ่งประกอบด้วย:
  - โมดูลที่ได้รับการตรวจสอบความถูกต้องแล้วจะถูกทำเครื่องหมายว่าใช้งานอยู่
  - หลังจาก 5 ปี โมดูลจะถูกทำเครื่องหมายเป็นประวัติ
  - ถ้าการรับรองโมดูลถูกเพิกถอนด้วยเหตุผลบางประการ โมดูลจะถูกทำเครื่องหมายว่าถูกเพิกถอน

ในปี 2563 CMVP ได้นำมาตรฐานสากล ISO/IEC 19790 มาใช้เป็นพื้นฐานสำหรับ FIPS 140-3

การรับรอง FIPS 140-3

สถานะปัจจุบัน

ตารางด้านล่างจะแสดงโมดูลการเข้ารหัสปี 2563 และปี 2564 ที่อยู่ในระหว่างการทดสอบด้านความสอดคล้องกับ FIPS 140-3 ในห้องปฏิบัติการในตอนนี้

การจัดเก็บกุญแจอย่างปลอดภัย (SKS) ที่เกี่ยวข้องกับการเปิดตัวระบบปฏิบัติการของทั้งปี 2563 และ 2564 ได้รับการทดสอบโดยเสร็จสมบูรณ์ในห้องปฏิบัติการแล้วและได้รับคำแนะนำจากห้องปฏิบัติการในการตรวจสอบความถูกต้องกับ CMVP รายการจะได้รับการระบุอยู่บนรายการโมดูลในกระบวนการและเมื่อได้รับการตรวจสอบความถูกต้องแล้วจะย้ายไปที่รายการโมดูลการเข้ารหัสที่ได้รับการตรวจสอบความถูกต้องแล้ว

พื้นที่ผู้ใช้ของ iOS 15 (2564), พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยกำลังอยู่ระหว่างการทดสอบในห้องปฏิบัติการ รายการจะได้รับการระบุอยู่บนรายการการปรับใช้อยู่ระหว่างการทดสอบ

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple corecrypto Module v12 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับการเปิดตัวในปี 2564 ของ iOS, iPadOS, macOS, tvOS และ watchOS **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (A9-A14, T2, M1, S3-S6) **ระดับความปลอดภัยโดยรวม:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับการเปิดตัวในปี 2564 ของ iOS, iPadOS, macOS, tvOS และ watchOS **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (A13, A14, S6, M1) **ระดับความปลอดภัยโดยรวม:** 2 **ระดับความปลอดภัยทางกายภาพ:** 3
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับการเปิดตัวในปี 2563 ของ iOS, iPadOS, macOS, tvOS และ watchOS **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (A9-A14, T2, M1, S3-S6) **ระดับความปลอดภัยโดยรวม:** 2

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับการเปิดตัวในปี 2563 ของ iOS, iPadOS, macOS, tvOS และ watchOS **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (A13, A14, S6, M1) **ระดับความปลอดภัยโดยรวม:** 2 **ระดับความปลอดภัยทางกายภาพ:** 3

การรับรอง FIPS 140-2

ตารางด้านล่างจะแสดงโมดูลการเข้ารหัสที่ได้รับการทดสอบด้านความสอดคล้องกับ FIPS 140-2 ในห้องปฏิบัติการ

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 5 กุมภาพันธ์ 2564	**การรับรอง:** 3811 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v10.0 **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 10.15 Catalina **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 10 กันยายน 2562	**การรับรอง:** 3523 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v9.0 **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 10.14 Mojave **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 10 กันยายน 2562	**การรับรอง:** 3223 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v1.0 **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 10.13 High Sierra **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2

การรับรองเกณฑ์ทั่วไป (CC)

Apple ได้เข้าไปมีส่วนร่วมเชิงรุกในการประเมินเกณฑ์ทั่วไปที่ซึ่งโปรไฟล์การปกป้องที่เหมาะสมจะครอบคลุมฟังก์ชั่นการทำงานด้านความปลอดภัยของเทคโนโลยี Apple

สถานะการรับรองเกณฑ์ทั่วไป (CC)

แบบแผนของสหรัฐอเมริกาที่ดำเนินการโดย NIAP จะเก็บรักษารายการของผลิตภัณฑ์ในการประเมิน ซึ่งรายการนี้จะประกอบไปด้วยผลิตภัณฑ์ที่อยู่ระหว่างการประเมินกับห้องปฏิบัติการการทดสอบเกณฑ์ทั่วไป (CCTL) ที่ได้รับการรับรองจาก NIAP ในสหรัฐอเมริกาและผลิตภัณฑ์ที่ผ่านการประชุมเริ่มงานการประเมิน (หรือเทียบเท่า) ซึ่งผู้บริหารของ CCEVS ได้ยอมรับผลิตภัณฑ์เข้าสู่การประเมินอย่างเป็นทางการแล้ว

หลังผลิตภัณฑ์ได้รับการรับรองแล้ว NIAP ใส่การรับรองที่สามารถใช้งานได้ในตอนนี้ไว้บนรายการข้อร้องเรียนผลิตภัณฑ์ขององค์กร การรับรองเหล่านี้จะถูกตรวจสอบด้านความสอดคล้องกับนโยบายการรับประกันการซ่อมในปัจจุบันหลังจาก 2 ปี หลังจากวันรับประกันการซ่อมหมดอายุแล้ว NIAP จะย้ายการแสดงการรับรองไปยังรายการผลิตภัณฑ์ที่ถูกเก็บถาวรขององค์กร

พอร์ทัลเกณฑ์ทั่วไปจะแสดงการรับรองที่สามารถยอมรับร่วมกันได้ภายใต้การจัดการรับรองเกณฑ์ทั่วไป (CCRA) พอร์ทัล CC อาจเก็บผลิตภัณฑ์ไว้บนรายการผลิตภัณฑ์ที่ได้รับการรับรองเป็นเวลา 5 ปี โดยการบันทึกจะถูกเก็บไว้โดยพอร์ทัล CC สำหรับการรับรองที่ถูกเก็บถาวร

ตารางด้านล่างจะแสดงการรับรองที่อยู่ในระหว่างการประเมินในห้องปฏิบัติการในตอนนี้ หรือการรับรองที่ได้รับการรับรองแล้วว่าสอดคล้องกับเกณฑ์ทั่วไป

ระบบปฏิบัติการ / วันที่ออกการรับรอง	ID แบบแผน / เอกสาร	ชื่อเรื่อง / โปรไฟล์การปกป้อง
ระบบปฏิบัติการ: sepOS **วันที่ออกการรับรอง:** —	**ID แบบแผน:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** Apple Secure Enclave [2020] **โปรไฟล์การปกป้อง:** CPP_DSC_V1.0 **ฮาร์ดแวร์:** Secure Enclave สำหรับ (A9-A14, M1, T2, S3-S6) **ซอฟต์แวร์:** sepOS ที่เผยแพร่พร้อมกับ iOS 14, iPadOS 14, macOS 11 Big Sur, tvOS 14, watchOS 7

การรับรองเพิ่มเติม

ตารางที่ด้านล่างจะแสดงการรับรองสำหรับ Secure Enclave ที่ไม่ได้ใช้ทั้งเกณฑ์ทั่วไปหรือ FIPS 140-3

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** 07/12/2562 ถึง 26/12/2565	**การรับรอง:** CFNR201902910002 (สาธารณรัฐ ประชาชนจีน: การรับรองเทคโนโลยีสำหรับบริการทางการเงินบนอุปกรณ์เคลื่อนที่) เวอร์ชั่นภาษาจีน เวอร์ชั่นภาษาอังกฤษ	**ชื่อเรื่อง:** สภาพแวดล้อมการดำเนินการที่เชื่อถือแล้วของเทอร์มินัลอุปกรณ์เคลื่อนที่ **ระบบปฏิบัติการ:** iOS 13.5.1 **ข้อมูลจำเพาะ:** JR/T 0156-2017

การรับรองความปลอดภัยสำหรับชิป Apple T2 Security

ความเป็นมาของการตรวจสอบความถูกต้องโมดูลการเข้ารหัส

Apple ได้เข้าไปมีส่วนร่วมเชิงรุกในการตรวจสอบความถูกต้องโมดูลซอฟต์แวร์และฮาร์ดแวร์แบบฝังในของ Apple ในการเปิดตัวระบบปฏิบัติการครั้งใหญ่ในแต่ละครั้ง การตรวจสอบความถูกต้องของความสอดคล้องสามารถดำเนินการได้เฉพาะกับการเปิดตัวโมดูลเวอร์ชั่นสุดท้ายเท่านั้น

ในปี 2563 CMVP ได้นำมาตรฐานสากล ISO/IEC 19790 มาใช้เป็นพื้นฐานสำหรับมาตรฐานการประมวลผลข้อมูลสหรัฐอเมริกากลาง (FIPS) 140-3

นอกจาก Intel CPU แล้ว คอมพิวเตอร์ Mac ส่วนใหญ่ตั้งแต่ปี 2560 ยังมีชิป Apple T2 Security แบบแยกต่างหากที่เป็นระบบบนชิป (SoC) ที่ใช้ Apple Silicon อีกด้วย คอมพิวเตอร์ Mac ที่มีชิป T2 เหล่านี้ใช้โมดูลการเข้ารหัสห้าแบบที่มีอยู่ทั้งหมดสำหรับบริการต่างๆ ในอุปกรณ์

- โมดูลผู้ใช้ Corecrypto สำหรับ Intel (ใช้โดย macOS บนคอมพิวเตอร์ Mac ที่ใช้ Intel)
- โมดูลเคอร์เนล Corecrypto สำหรับ Intel (ใช้โดย macOS บนคอมพิวเตอร์ Mac ที่ใช้ Intel)
- โมดูลผู้ใช้ Corecrypto สำหรับ ARM (ใช้โดยชิป T2)
- โมดูลเคอร์เนล Corecrypto สำหรับ ARM (ใช้โดยชิป T2)
- โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัย (ใช้โดยหน่วยประมวลผลร่วม Secure Enclave ที่ฝังอยู่ในชิป T2)

หมายเหตุ: โมดูลแบบ Apple Silicon ที่ทำงานบนชิป T2 เป็นโมดูลเดียวกันกับที่ทำงานบน Apple Silicon อื่นๆ เช่น ซีรีส์ A, ซีรีส์ S และซีรีส์ M ของ Apple

สถานะการตรวจสอบความถูกต้องโมดูลการเข้ารหัส

โปรแกรมการตรวจสอบความถูกต้องโมดูลการเข้ารหัส (CMVP) ยังคงใช้สถานะการตรวจสอบความถูกต้องของโมดูลการเข้ารหัสภายใต้รายการที่แยกออกจากกันสามรายการซึ่งขึ้นอยู่กับสถานะปัจจุบันของแต่ละรายการ:

- ในการที่จะได้รับการระบุอยู่ในรายการการปรับใช้อยู่ระหว่างการทดสอบของ CMVP ห้องปฏิบัติการจะต้องทำสัญญากับ Apple ในการดำเนินการทดสอบ
- หลังจากที่การทดสอบเสร็จสมบูรณ์โดยห้องปฏิบัติการ และเมื่อห้องปฏิบัติการได้แนะนำการตรวจสอบความถูกต้องโดย CMVP และได้ชำระค่าธรรมเนียม CMVP แล้ว จากนั้นโมดูลจะถูกเพิ่มไปยังรายการโมดูลในกระบวนการ (MIP) รายการ MIP จะติดตามความคืบหน้าของความพยายามในการตรวจสอบความถูกต้องของ CMVP ซึ่งแบ่งเป็นสี่ระยะ:
  - **รอการตรวจสอบ:** รอการกำหนดทรัพยากรของ CMVP
  - **อยู่ในระหว่างการตรวจสอบ:** ทรัพยากรของ CMVP อยู่ในระหว่างดำเนินการกิจกรรมการตรวจสอบความถูกต้อง
  - **ดำเนินการร่วมกัน:** ห้องปฏิบัติการและ CMVP กำลังแก้ไขปัญหาที่พบ
  - **สรุป:** กิจกรรมและระเบียบแบบแผนที่เกี่ยวข้องกับการออกการรับรอง
- หลังจากการตรวจสอบความถูกต้องโดย CMVP โมดูลจะได้รับการรับรองความสอดคล้องและถูกเพิ่มไปยังรายการโมดูลการเข้ารหัสที่ได้รับการตรวจสอบความถูกต้องแล้ว ซึ่งประกอบด้วย:
  - โมดูลที่ได้รับการตรวจสอบความถูกต้องแล้วจะถูกทำเครื่องหมายว่าใช้งานอยู่
  - หลังจาก 5 ปี โมดูลจะถูกทำเครื่องหมายเป็นประวัติ
  - ถ้าการรับรองโมดูลถูกเพิกถอนด้วยเหตุผลบางประการ โมดูลจะถูกทำเครื่องหมายว่าถูกเพิกถอน

การรับรอง FIPS 140-3

สถานะปัจจุบัน

โมดูลปี 2563 สำหรับพื้นที่ผู้ใช้ พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยได้รับการทดสอบโดยเสร็จสมบูรณ์ในห้องปฏิบัติการแล้วและได้รับคำแนะนำจากห้องปฏิบัติการในการตรวจสอบความถูกต้องกับ CMVP รายการจะได้รับการระบุอยู่บนรายการโมดูลในกระบวนการ

โมดูลปี 2564 สำหรับพื้นที่ผู้ใช้ พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยกำลังอยู่ระหว่างการทดสอบในห้องปฏิบัติการ รายการจะได้รับการระบุอยู่บนรายการการปรับใช้อยู่ระหว่างการทดสอบ

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12.0 **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 12 Monterey **สภาพแวดล้อม:** Apple Silicon, ผู้ใช้, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12.0 **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 12 Monterey **สภาพแวดล้อม:** Apple Silicon, เคอร์เนล, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12.0 **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 12 Monterey **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (T2) **ระดับความปลอดภัย:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 11 Big Sur **สภาพแวดล้อม:** Apple Silicon, ผู้ใช้, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 11 Big Sur **สภาพแวดล้อม:** Apple Silicon, เคอร์เนล, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 11 Big Sur บน Intel **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2

การรับรอง FIPS 140-2

ตารางด้านล่างจะแสดงโมดูลการเข้ารหัสที่ได้รับการทดสอบด้านความสอดคล้องกับ FIPS 140-2 ในห้องปฏิบัติการ

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 23 มีนาคม 2564	**การรับรอง:** 3856 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v10.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 10.15 Catalina **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 23 มีนาคม 2564	**การรับรอง:** 3855 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v10.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 10.15 Catalina **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 5 กุมภาพันธ์ 2564	**การรับรอง:** 3811 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัย Corecrypto ของ Apple v10.0 **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 10.15 Catalina **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 23 เมษายน 2562	**การรับรอง:** 3438 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v9.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 10.14 Mojave **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 11 เมษายน 2562	**การรับรอง:** 3433 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v9.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 10.14 Mojave **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 10 กันยายน 2562	**การรับรอง:** 3523 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v9.0 **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 10.14 Mojave **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 9/3/2561, 22/5/2561, 6/7/2561	**การรับรอง:** 3148 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v8.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 10.13 High Sierra **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 9/3/2561, 17/5/2561, 3/7/2561	**การรับรอง:** 3147 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v8.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 10.13 High Sierra **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 10 กรกฎาคม 2561	**การรับรอง:** 3223 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v1.0 **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 10.13 High Sierra **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2559 **วันที่ตรวจสอบความถูกต้อง:** 1 กุมภาพันธ์ 2560	**การรับรอง:** 2828 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** iOS Corecrypto Kernel Module v7.0 ของ Apple **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 10.12 Sierra **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2559 **วันที่ตรวจสอบความถูกต้อง:** 1 กุมภาพันธ์ 2560	**การรับรอง:** 2827 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** iOS Corecrypto Kernel Module v7.0 ของ Apple **ระบบปฏิบัติการ:** sepOS สำหรับ macOS 10.12 Sierra **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1

การรับรองความปลอดภัยระบบปฏิบัติการ

ภาพรวมการรับรองความปลอดภัยระบบปฏิบัติการของ Apple

Apple มีการรับรองการตรวจสอบความถูกต้องด้านความสอดคล้องกับมาตรฐานการประมวลผลข้อมูลสหรัฐอเมริกากลาง (FIPS) 140-2/-3 สำหรับ sepOS และเฟิร์มแวร์ T2 รวมถึงการรับรองอื่นๆ ด้วย Apple เริ่มต้นจาก**โครงสร้างการรับรอง**ที่สามารถปรับใช้ได้ในวงกว้างกับแพลตฟอร์มที่หลากหลายตามความเหมาะสม หนึ่งในโครงสร้างดังกล่าวคือการตรวจสอบความถูกต้องของ corecrypto ที่ใช้ในการปรับใช้โมดูลการเข้ารหัสของซอฟต์แวร์และฮาร์ดแวร์ภายในระบบปฏิบัติการที่พัฒนาโดย Apple โครงสร้างที่สองคือการรับรอง Secure Enclave ซึ่งฝังอยู่ในอุปกรณ์ Apple หลายๆ รุ่น โครงสร้างที่สามคือการรับรอง Secure Element (SE) ที่พบได้ในอุปกรณ์ Apple ทุกเครื่องที่มี Touch ID และอุปกรณ์ที่มี Face ID โครงสร้างการรับรองฮาร์ดแวร์เหล่านี้สร้างรากฐานสำหรับการรับรองความปลอดภัยของแพลตฟอร์มที่กว้างขึ้น

การตรวจสอบความถูกต้องอัลกอริทึมการเข้ารหัส

การตรวจสอบความถูกต้องของการปรับใช้ความถูกต้องของอัลกอริทึมการเข้ารหัสจำนวนมากและฟังก์ชั่นความปลอดภัยที่เกี่ยวข้องเป็นข้อกำหนดเบื้องต้นสำหรับการตรวจสอบความถูกต้อง FIPS 140-3 อีกทั้งสนับสนุนของการรับรองอื่นๆ การตรวจสอบความถูกต้องจะได้รับการจัดการโดยโปรแกรมการตรวจสอบความถูกต้องอัลกอริทึมการเข้ารหัส (CAVP) ของ NIST การรับรองของการตรวจสอบความถูกต้องสำหรับการปรับใช้กับ Apple สามารถดูได้โดยใช้ตัวช่วยอำนวยความสะดวกการค้นหาของ CAVP

การตรวจสอบความถูกต้องของโมดูลการเข้ารหัส: FIPS 140-2/3 (ISO/IEC 19790)

โมดูลการเข้ารหัสในระบบปฏิบัติการของ Apple ได้รับการตรวจสอบความถูกต้องซ้ำๆ โดยโปรแกรมการตรวจสอบความถูกต้องโมดูลการเข้ารหัส (CMVP) ว่าเป็นไปตามมาตรฐานการประมวลผลข้อมูลสหรัฐอเมริกากลาง (FIPS) 140-2 หลังจากการเปิดตัวครั้งใหญ่ของระบบปฏิบัติการตั้งแต่ปี 2555 หลังจากการเปิดตัวครั้งใหญ่ในแต่ละครั้ง Apple จะส่งโมดูลทั้งหมดไปยัง CMVP เพื่อตรวจสอบความถูกต้องทางการเข้ารหัสอย่างสมบูรณ์ โมดูลที่ตรวจสอบความถูกต้องแล้วเหล่านี้จะมอบการดำเนินการเข้ารหัสสำหรับบริการที่ Apple จัดหาให้และจะสามารถใช้ได้กับแอปของบริษัทอื่น

Apple ได้รับ**ความปลอดภัยระดับ** 1 ในแต่ละปีสำหรับโมดูลแบบซอฟต์แวร์ "Corecrypto Module สำหรับ Intel" และ "Corecrypto Kernel Module สำหรับ Intel" สำหรับ macOS สำหรับ Apple Silicon โมดูล "Corecrypto Module สำหรับ ARM" และ "Corecrypto Kernel Module สำหรับ ARM" สามารถใช้ได้กับ iOS, iPadOS, tvOS, watchOS และเฟิร์มแวร์บนชิป Apple T2 Security ที่ฝังอยู่ในคอมพิวเตอร์ Mac

ในปี 2562 Apple ได้รับ**ความปลอดภัยระดับ** 2 FIPS 140-2 สำเร็จเป็นครั้งแรกสำหรับโมดูลการเข้ารหัสฮาร์ดแวร์แบบฝังในที่ระบุเป็น "Apple Corecrypto Module: การจัดเก็บกุญแจอย่างปลอดภัย" ซึ่งทำให้รัฐบาลของสหรัฐอเมริกาอนุญาตให้ใช้กุญแจที่สร้างขึ้นและจัดการใน Secure Enclave Apple เดินหน้าการตรวจสอบความถูกต้องสำหรับโมดูลการเข้ารหัสฮาร์ดแวร์ในระดับความปลอดภัยที่สูงขึ้นอยู่เสมอในการเปิดตัวระบบปฏิบัติการครั้งใหญ่แต่ละครั้ง

FIPS 140-3 ได้รับการอนุญาตโดยกระทรวงพาณิชย์ของสหรัฐอเมริกาในปี 2562 การเปลี่ยนแปลงที่โดดเด่นที่สุดของมาตรฐานในเวอร์ชั่นนี้คือข้อกำหนดมาตรฐาน ISO/IEC โดยเฉพาะอย่างยิ่ง ISO/IEC 19790:2015 และมาตรฐานการทดสอบที่เกี่ยวข้อง ISO/IEC 24759:2017 CMVP ได้เริ่มต้นโปรแกรมการเปลี่ยนผ่านและระบุว่า ตั้งแต่ปี 2563 เป็นต้นไป โมดูลการเข้ารหัสจะเริ่มรับการตรวจสอบความถูกต้องโดยใช้ FIPS 140-3 เป็นพื้นฐาน โมดูลการเข้ารหัสของ Apple มุ่งหมายที่จะปฏิบัติตามและเปลี่ยนไปใช้มาตรฐาน FIPS 140-3 ในทันทีที่สามารถปฏิบัติได้

สำหรับโมดูลการเข้ารหัสที่อยู่ระหว่างกระบวนการทดสอบและการตรวจสอบความถูกต้อง CMVP จะเก็บรักษารายการที่แยกกันสองรายการซึ่งอาจมีข้อมูลเกี่ยวกับการตรวจสอบความถูกต้องที่เสนอ สำหรับโมดูลการเข้ารหัสที่อยู่ระหว่างการทดสอบในห้องปฏิบัติการที่มีการรับรอง รายการการปรับใช้อยู่ระหว่างการทดสอบ อาจระบุโมดูลในรายการ หลังจากที่ห้องปฏิบัติการได้ดำเนินการทดสอบเสร็จสมบูรณ์แล้วและแนะนำให้เข้ารับการตรวจสอบความถูกต้องจาก CMVP โมดูลการเข้ารหัสของ Apple จะแสดงขึ้นในรายการโมดูลในกระบวนการ ตอนนี้การทดสอบในห้องปฏิบัติการเสร็จสมบูรณ์แล้วและรอการตรวจสอบความถูกต้องของการทดสอบโดย CMVP เนื่องจากระยะเวลาของกระบวนการประเมินสามารถผันแปรได้ ให้ดูรายการกระบวนการทั้งสองรายการที่ด้านบนเพื่อระบุสถานะปัจจุบันของโมดูลการเข้ารหัสของ Apple ระหว่างวันที่ที่มีการเปิดตัวระบบปฏิบัติการครั้งใหญ่และการออกการรับรองการตรวจสอบความถูกต้องโดย CMVP

การรับรองผลิตภัณฑ์: (เกณฑ์ทั่วไป ISO/IEC 15408)

เกณฑ์ทั่วไป (ISO/IEC 15408) เป็นมาตรฐานที่หลายองค์กรใช้เป็นพื้นฐานในการดำเนินการประเมินความปลอดภัยของผลิตภัณฑ์ IT

สำหรับการรับรองที่อาจรู้จักกันในชื่อการจัดการรับรองเกณฑ์ทั่วไป (CCRA) ระดับสากล ให้ดูที่พอร์ทัลเกณฑ์ทั่วไป มาตรฐานเกณฑ์ทั่วไปยังอาจมีการใช้ภายนอก CCRA โดยแบบแผนการตรวจสอบความถูกต้องระดับชาติและระดับส่วนตัวอีกด้วย ในยุโรป การยอมรับร่วมกันอยู่ภายใต้ข้อตกลง SOG-IS เช่นเดียวกันกับ CCRA

เป้าหมายก็เพื่อให้ชุดมาตรฐานความปลอดภัยที่ผ่านการรับรองในระดับสากลสามารถประเมินความสามารถด้านการรักษาความปลอดภัยของผลิตภัณฑ์เทคโนโลยีสารสนเทศได้อย่างชัดเจนและน่าเชื่อถือ ซึ่งเป็นเป้าหมายที่ชุมชนเกณฑ์ทั่วไประบุไว้ เมื่อจัดให้มีการประเมินแบบอิสระเกี่ยวกับความสามารถของผลิตภัณฑ์ในการปฏิบัติตามมาตรฐานด้านความปลอดภัย การรับรองเกณฑ์ทั่วไปจึงทำให้ลูกค้ามีความมั่นใจมากขึ้นเกี่ยวกับความปลอดภัยของผลิตภัณฑ์เทคโนโลยีสารสนเทศและตัดสินใจได้อย่างรอบคอบมากขึ้น

ประเทศสมาชิกได้ตกลงที่จะยอมรับการรับรองผลิตภัณฑ์เทคโนโลยีสารสนเทศด้วยความเชื่อมั่นในระดับเดียวกันผ่าน CCRA การประเมินที่จำเป็นก่อนการรับรองจะครอบคลุมและรวมถึง:

- โปรไฟล์การปกป้อง (PP)
- เป้าหมายความปลอดภัย (ST)
- ข้อกำหนดฟังก์ชั่นความปลอดภัย (SFR)
- ข้อกำหนดการรับประกันความปลอดภัย (SAR)
- ระดับการรับประกันการประเมิน (EAL)

โปรไฟล์การปกป้อง (PP) เป็นเอกสารที่ระบุข้อกำหนดด้านความปลอดภัยสำหรับคลาสของประเภทอุปกรณ์ (เช่น อุปกรณ์เคลื่อนที่) ซึ่งใช้สำหรับแสดงการเปรียบเทียบระหว่างการประเมินของผลิตภัณฑ์ IT ภายในคลาสเดียวกัน การเป็นสมาชิกของ CCRA รวมถึงการเพิ่มขึ้นของ PP ที่ได้รับการรับรองมีการเพิ่มขึ้นทุกปีอย่างต่อเนื่อง การทำความตกลงนี้อนุญาตให้นักพัฒนาผลิตภัณฑ์ใช้การรับรองเดียวภายใต้แบบแผนการอนุญาตการรับรองแบบใดแบบหนึ่งและกำหนดให้ได้รับการยอมรับจากผู้ลงนามทุกๆ คนที่ใช้การรับรอง

เป้าหมายความปลอดภัย (ST) กำหนดว่า**อะไรบ้าง**ที่จะได้รับการประเมินเมื่อผลิตภัณฑ์ IT ได้รับการรับรอง ST หมายถึง**ข้อกำหนดฟังก์ชั่นความปลอดภัย (SFR)** ที่เฉพาะเจาะจงยิ่งขึ้น ซึ่งใช้สำหรับการประเมิน ST อย่างละเอียดยิ่งขึ้น

เกณฑ์ทั่วไป (CC) ยังรวมถึง**ข้อกำหนดการรับประกันความปลอดภัย**อีกด้วย ตัววัดหนึ่งที่มักถูกระบุอยู่เป็นประจำก็คือ**ระดับการรับประกันการประเมิน (EAL)** โดย EAL จะรวมกลุ่มชุดของ SAR ที่เกิดขึ้นบ่อยครั้งเข้าด้วยกันและอาจถูกระบุอยู่ใน PP และ ST เพื่อรองรับการเปรียบเทียบ

PP ก่อนหน้านี้จำนวนมากถูกเก็บถาวรและแทนที่ด้วย PP แบบมุ่งเป้าซึ่งได้รับการพัฒนาและมุ่งเน้นโซลูชั่นและสภาพแวดล้อมที่เฉพาะเจาะจง ในความพยายามจากหลายฝ่ายที่จะให้มีการยอมรับร่วมกันระหว่างสมาชิก CCRA ทั้งหมดต่อไป ชุมชนเทคนิคสากล (iTC) ได้ถูกจัดตั้งขึ้นเพื่อพัฒนาและรักษาไว้ซึ่ง**โปรไฟล์การปกป้องเชิงร่วมมือ (cPP)** ซึ่งมีการพัฒนาตั้งแต่เริ่มต้นโดยมีแผนของผู้ลงนาม CCRA ร่วมด้วย PP แบบมุ่งเป้าสำหรับกลุ่มผู้ใช้และการจัดการการยอมรับร่วมกันที่นอกเหนือจาก CCRA จะได้รับการพัฒนาต่อไปโดยผู้ที่ได้รับประโยชน์ร่วมกันที่เหมาะสม

Apple เริ่มใช้การรับรองภายใต้ CCRA ที่ได้รับการอัปเดตกับ cPP ที่เลือกตั้งแต่ต้นปี 2558 ตั้งแต่นั้นมา Apple ก็ได้รับการรับรองเกณฑ์ทั่วไปสำหรับการเปิดตัว iOS ครั้งใหญ่ในแต่ละครั้งและได้ขยายความครอบคลุมให้รวมถึงการรับประกันความปลอดภัยที่ได้จาก PP ใหม่

Apple มีบทบาทเชิงรุกในชุมชนเทคนิคที่มุ่งเน้นการประเมินเทคโนโลยีความปลอดภัยของอุปกรณ์เคลื่อนที่ ซึ่งรวมถึง iTC ที่รับผิดชอบในการพัฒนาและอัปเดต cPP Apple ยังคงประเมินและใช้การรับรองกับ PP และ cPP ที่มีอยู่ในปัจจุบันอย่างต่อเนื่อง

การรองรับแพลตฟอร์ม Apple สำหรับตลาดอเมริกาเหนือปกติแล้วจะดำเนินการโดยความร่วมมือในการรับประกันข้อมูลแห่งชาติ (NIAP) ที่เก็บบันทึกรายการโปรเจ็กต์ที่อยู่ระหว่างการประเมินแต่ยังไม่ได้รับรอง

นอกเหนือจากใบรับรองแพลตฟอร์มทั่วไปแล้ว ยังมีการออกใบรับรองอื่นๆ เพื่อแสดงข้อกำหนดด้านความปลอดภัยที่เฉพาะเจาะจงสำหรับตลาดบางแห่งอีกด้วย

การรับรองความปลอดภัยสำหรับ iOS

ความเป็นมาของการรับรอง iOS

Apple ได้เข้าไปมีส่วนร่วมเชิงรุกในการตรวจสอบความถูกต้องโมดูลซอฟต์แวร์และฮาร์ดแวร์แบบฝังในของ Apple ในการเปิดตัวระบบปฏิบัติการครั้งใหญ่ในแต่ละครั้ง การตรวจสอบความถูกต้องของความสอดคล้องสามารถดำเนินการได้เฉพาะกับเวอร์ชั่นสุดท้ายที่เปิดตัวเท่านั้น

สถานะการตรวจสอบความถูกต้องของโมดูลการเข้ารหัส iOS

โปรแกรมการตรวจสอบความถูกต้องโมดูลการเข้ารหัส (CMVP) ยังคงใช้สถานะการตรวจสอบความถูกต้องของโมดูลการเข้ารหัสภายใต้รายการที่แยกออกจากกันสามรายการซึ่งขึ้นอยู่กับสถานะปัจจุบันของแต่ละรายการ:

- ในการที่จะได้รับการระบุอยู่ในรายการการปรับใช้อยู่ระหว่างการทดสอบของ CMVP ห้องปฏิบัติการจะต้องทำสัญญากับ Apple ในการดำเนินการทดสอบ
- หลังจากที่การทดสอบเสร็จสมบูรณ์โดยห้องปฏิบัติการ และเมื่อห้องปฏิบัติการได้แนะนำการตรวจสอบความถูกต้องโดย CMVP และได้ชำระค่าธรรมเนียม CMVP แล้ว จากนั้นโมดูลจะถูกเพิ่มไปยังรายการโมดูลในกระบวนการ (MIP) รายการ MIP จะติดตามความคืบหน้าของความพยายามในการตรวจสอบความถูกต้องของ CMVP ซึ่งแบ่งเป็นสี่ระยะ:
  - **รอการตรวจสอบ:** รอการกำหนดทรัพยากรของ CMVP
  - **อยู่ในระหว่างการตรวจสอบ:** ทรัพยากรของ CMVP อยู่ในระหว่างดำเนินการกิจกรรมการตรวจสอบความถูกต้อง
  - **ดำเนินการร่วมกัน:** ห้องปฏิบัติการและ CMVP กำลังแก้ไขปัญหาที่พบ
  - **สรุป:** กิจกรรมและระเบียบแบบแผนที่เกี่ยวข้องกับการออกการรับรอง
- หลังจากการตรวจสอบความถูกต้องโดย CMVP โมดูลจะได้รับการรับรองความสอดคล้องและถูกเพิ่มไปยังรายการโมดูลการเข้ารหัสที่ได้รับการตรวจสอบความถูกต้องแล้ว ซึ่งประกอบด้วย:
  - โมดูลที่ได้รับการตรวจสอบความถูกต้องแล้วจะถูกทำเครื่องหมายว่าใช้งานอยู่
  - หลังจาก 5 ปี โมดูลจะถูกทำเครื่องหมายเป็นประวัติ
  - ถ้าการรับรองโมดูลถูกเพิกถอนด้วยเหตุผลบางประการ โมดูลจะถูกทำเครื่องหมายว่าถูกเพิกถอน

ในปี 2563 CMVP ได้นำมาตรฐานสากล ISO/IEC 19790 มาใช้เป็นพื้นฐานสำหรับ FIPS 140-3

การรับรอง FIPS 140-3

สถานะปัจจุบัน

พื้นที่ผู้ใช้ของ iOS 14 (2563), พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยได้รับการทดสอบโดยเสร็จสมบูรณ์ในห้องปฏิบัติการแล้วและได้รับคำแนะนำจากห้องปฏิบัติการในการตรวจสอบความถูกต้องกับ CMVP รายการจะได้รับการระบุอยู่บนรายการโมดูลในกระบวนการ

พื้นที่ผู้ใช้ของ iOS 15 (2564), พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยกำลังอยู่ระหว่างการทดสอบในห้องปฏิบัติการ รายการจะได้รับการระบุอยู่บนรายการการปรับใช้อยู่ระหว่างการทดสอบ

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** iOS 15 **สภาพแวดล้อม:** Apple Silicon, ผู้ใช้, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** iOS 15 **สภาพแวดล้อม:** Apple Silicon, เคอร์เนล, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ iOS 15 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (A9–A14) **ระดับความปลอดภัยโดยรวม:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ iOS 15 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (A13, A14, A15) **ระดับความปลอดภัยโดยรวม:** 2 **ระดับความปลอดภัยทางกายภาพ:** 3
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** iOS 14 **สภาพแวดล้อม:** Apple Silicon, ผู้ใช้, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** iOS 14 **สภาพแวดล้อม:** Apple Silicon, เคอร์เนล, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ iOS 14 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (A9-A14) **ระดับความปลอดภัยโดยรวม:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ iOS 14 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (A13-A14) **ระดับความปลอดภัยโดยรวม:** 2 **ระดับความปลอดภัยทางกายภาพ:** 3

การรับรอง FIPS 140-2

ตารางด้านล่างจะแสดงโมดูลการเข้ารหัสที่อยู่ในระหว่างการทดสอบในตอนนี้และได้รับการทดสอบแล้วในด้านความสอดคล้องกับ FIPS 140-2 ในห้องปฏิบัติการ

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 23 มีนาคม 2564	**การรับรอง:** 3856 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v10.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** iOS 13 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 23 มีนาคม 2564	**การรับรอง:** 3855 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v10.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** iOS 13 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 5 กุมภาพันธ์ 2564	**การรับรอง:** 3811 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v10.0 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ iOS 13 **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 23 เมษายน 2562	**การรับรอง:** 3438 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v9.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** iOS 12 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 11 เมษายน 2562	**การรับรอง:** 3433 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v9.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** iOS 12 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 10 กันยายน 2562	**การรับรอง:** 3523 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v9.0 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ iOS 12 **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 9/3/2561, 22/5/2561, 6/7/2561	**การรับรอง:** 3148 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v8.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** iOS 11 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 9/3/2561, 17/5/2561, 3/7/2561	**การรับรอง:** 3147 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v8.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** iOS 11 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 10 กันยายน 2562	**การรับรอง:** 3223 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v1.0 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ iOS 11 **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2559 **วันที่ตรวจสอบความถูกต้อง:** 1 กุมภาพันธ์ 2560	**การรับรอง:** 2828 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** iOS Corecrypto Kernel Module v7.0 ของ Apple **ระบบปฏิบัติการ:** iOS 10 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2559 **วันที่ตรวจสอบความถูกต้อง:** 1 กุมภาพันธ์ 2560	**การรับรอง:** 2827 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** iOS Corecrypto Kernel Module v7.0 ของ Apple **ระบบปฏิบัติการ:** iOS 10 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1

เวอร์ชั่นก่อนหน้านี้

การรับรองที่มีอายุมากกว่า 5 ปีจะถูก CMVP ระบุไว้เป็นสถานะประวัติ iOS เวอร์ชั่นก่อนหน้าเหล่านี้มีการตรวจสอบความถูกต้องโมดูลการเข้ารหัส:

- iOS 9 (โมดูล corecrypto v6.0)
- iOS 8 (โมดูล corecrypto v5.0)
- iOS 7 (โมดูล corecrypto v4.0)
- iOS 6 (โมดูล corecrypto v3.0)

ความเป็นมาของการรับรองเกณฑ์ทั่วไป (CC)

Apple ได้เข้าไปมีส่วนร่วมเชิงรุกในการประเมิน iOS ในการเปิดตัวระบบปฏิบัติการครั้งใหญ่ในแต่ละครั้ง การประเมินจะต้องดำเนินการกับระบบปฏิบัติการเวอร์ชั่นสุดท้ายที่เปิดตัวเป็นสาธารณะเท่านั้น ก่อนหน้า iPadOS 13.1 iPadOS มีชื่อว่า iOS

สถานะการรับรองเกณฑ์ทั่วไป (CC)

แบบแผนของสหรัฐอเมริกาที่ดำเนินการโดย NIAP จะเก็บรักษารายการของผลิตภัณฑ์ในการประเมิน ซึ่งรายการนี้จะประกอบไปด้วยผลิตภัณฑ์ที่อยู่ระหว่างการประเมินกับห้องปฏิบัติการการทดสอบเกณฑ์ทั่วไป (CCTL) ที่ได้รับการรับรองจาก NIAP ในสหรัฐอเมริกาและผลิตภัณฑ์ที่ผ่านการประชุมเริ่มงานการประเมิน (หรือเทียบเท่า) ซึ่งผู้บริหารของ CCEVS ได้ยอมรับผลิตภัณฑ์เข้าสู่การประเมินอย่างเป็นทางการแล้ว

หลังผลิตภัณฑ์ได้รับการรับรองแล้ว NIAP ใส่การรับรองที่สามารถใช้งานได้ในตอนนี้ไว้บนรายการข้อร้องเรียนผลิตภัณฑ์ขององค์กร การรับรองเหล่านี้จะถูกตรวจสอบด้านความสอดคล้องกับนโยบายการรับประกันการซ่อมในปัจจุบันหลังจาก 2 ปี หลังจากวันรับประกันการซ่อมหมดอายุแล้ว NIAP จะย้ายการแสดงการรับรองไปยังรายการผลิตภัณฑ์ที่ถูกเก็บถาวรขององค์กร

พอร์ทัลเกณฑ์ทั่วไปจะแสดงการรับรองที่สามารถยอมรับร่วมกันได้ภายใต้การจัดการรับรองเกณฑ์ทั่วไป (CCRA) พอร์ทัล CC อาจเก็บผลิตภัณฑ์ไว้บนรายการผลิตภัณฑ์ที่ได้รับการรับรองเป็นเวลา 5 ปี โดยการบันทึกจะถูกเก็บไว้โดยพอร์ทัล CC สำหรับการรับรองที่ถูกเก็บถาวร

ตารางด้านล่างจะแสดงการรับรองที่อยู่ในระหว่างการประเมินในห้องปฏิบัติการในตอนนี้ หรือการรับรองที่ได้รับการรับรองแล้วว่าสอดคล้องกับเกณฑ์ทั่วไป

สถานะปัจจุบัน

การทดสอบในห้องปฏิบัติการสำหรับการประเมินกับ NIAP สำหรับ iOS 15 กำลังดำเนินการอยู่ สำหรับข้อมูลล่าสุด ให้ดูที่ผลิตภัณฑ์ในการประเมิน (NIAP) และรายการผลิตภัณฑ์ที่เป็นไปตามข้อกำหนด

ระบบปฏิบัติการ / วันที่ออกการรับรอง	ID แบบแผน / เอกสาร	ชื่อเรื่อง / โปรไฟล์การปกป้อง
ระบบปฏิบัติการ: iOS 15 **วันที่ออกการรับรอง:** —	**ID แบบแผน:** ยังไม่ได้รับรอง **เอกสาร:** —	**ชื่อเรื่อง:** iOS 15 ของ Apple: iPhone **โปรไฟล์การปกป้อง:** พื้นฐานอุปกรณ์เคลื่อนที่ (รอยืนยัน PP-โมดูล)
ระบบปฏิบัติการ: iOS 14 **วันที่ออกการรับรอง:** 1 กันยายน 2564	**ID แบบแผน:** 11146 **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** iOS 14 ของ Apple: iPhone **โปรไฟล์การปกป้อง:** พื้นฐานอุปกรณ์เคลื่อนที่, โมดูลลูกข่าย VPN, โมดูล PP ลูกข่าย WLAN, EP เอเจ็นต์ MDM
ระบบปฏิบัติการ: iOS 13 **วันที่ออกการรับรอง:** 6 พฤศจิกายน 2563	**ID แบบแผน:** 11036 **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** iOS 13 ของ Apple บน iPhone **โปรไฟล์การปกป้อง:** พื้นฐานอุปกรณ์เคลื่อนที่, โมดูลลูกข่าย VPN, EP ลูกข่าย WLAN, EP เอเจ็นต์ MDM

การรับรองเกณฑ์ทั่วไปของ iOS ที่ถูกเก็บถาวร

iOS เวอร์ชั่นก่อนหน้าเหล่านี้มีการตรวจสอบความถูกต้องเกณฑ์ทั่วไป เวอร์ชั่นเหล่านี้ถูกเก็บถาวรโดย NIAP ตามนโยบายของ NIAP:

ระบบปฏิบัติการ / วันที่ออกการรับรอง	ID แบบแผน / เอกสาร	ชื่อเรื่อง / โปรไฟล์การปกป้อง
ระบบปฏิบัติการ: iOS 12 **วันที่ออกการรับรอง:** 14 มีนาคม 2562	**ID แบบแผน:** 10937 **เอกสาร:** เป้าหมายความปลอดภัย แนวทาง	**ชื่อเรื่อง:** iPhone ที่ใช้ iOS 12 **โปรไฟล์การปกป้อง:** พื้นฐานอุปกรณ์เคลื่อนที่, โมดูลลูกข่าย VPN, EP ลูกข่าย LAN ไร้สาย, EP เอเจ็นต์ MDM
ระบบปฏิบัติการ: iOS 11 **วันที่ออกการรับรอง:** 17 กรกฎาคม 2561	**ID แบบแผน:** 10851 **เอกสาร:** เป้าหมายความปลอดภัย แนวทาง	**ชื่อเรื่อง:** iOS 11 ของ Apple **โปรไฟล์การปกป้อง:** พื้นฐานอุปกรณ์เคลื่อนที่, EP ลูกข่าย LAN ไร้สาย, EP เอเจ็นต์ MDM

ระบบปฏิบัติการ / วันที่ออกการรับรอง	ID แบบแผน / เอกสาร	ชื่อเรื่อง / โปรไฟล์การปกป้อง
ระบบปฏิบัติการ: iOS 10 **วันที่ออกการรับรอง:** 27 กรกฎาคม 2560	**ID แบบแผน:** 10782 **เอกสาร:** เป้าหมายความปลอดภัย, แนวทาง	**ชื่อเรื่อง:** iOS 10.2 บนอุปกรณ์ iPhone และ iPad **โปรไฟล์การปกป้อง:** พื้นฐานอุปกรณ์เคลื่อนที่, EP ลูกข่าย LAN ไร้สาย, EP เอเจ็นต์ MDM
ระบบปฏิบัติการ: iOS 10 **วันที่ออกการรับรอง:** 27 กรกฎาคม 2560	**ID แบบแผน:** 10792 **เอกสาร:** เป้าหมายความปลอดภัย, แนวทาง	**ชื่อเรื่อง:** ลูกข่าย VPN ของ iOS 10.2 บนอุปกรณ์ iPhone และ iPad **โปรไฟล์การปกป้อง:** PP ลูกข่าย VPN
ระบบปฏิบัติการ: iOS 9 **วันที่ออกการรับรอง:** 14 ตุลาคม 2559	**ID แบบแผน:** 10725 **เอกสาร:** เป้าหมายความปลอดภัย, แนวทาง	**ชื่อเรื่อง:** iOS 9.3.2 ที่มีเอเจ็นต์ MDM **โปรไฟล์การปกป้อง:** พื้นฐานอุปกรณ์เคลื่อนที่, EP เอเจ็นต์ MDM
ระบบปฏิบัติการ: iOS 9 **วันที่ออกการรับรอง:** 13 ตุลาคม 2559	**ID แบบแผน:** 10714 **เอกสาร:** เป้าหมายความปลอดภัย, แนวทาง	**ชื่อเรื่อง:** ชื่อเรื่อง: ลูกข่าย VPN ของ OS บนอุปกรณ์ iPhone และ iPad **โปรไฟล์การปกป้อง:** PP ลูกข่าย VPN
ระบบปฏิบัติการ: iOS 9 **วันที่ออกการรับรอง:** 28 มกราคม 2559	**ID แบบแผน:** 10695 **เอกสาร:** เป้าหมายความปลอดภัย, แนวทาง	**ชื่อเรื่อง:** iOS 9 **โปรไฟล์การปกป้อง:** ความรู้พื้นฐานเกี่ยวกับอุปกรณ์เคลื่อนที่

การรับรองความปลอดภัยสำหรับ iPadOS

ความเป็นมาของการรับรอง iPadOS

Apple ได้เข้าไปมีส่วนร่วมเชิงรุกในการตรวจสอบความถูกต้องของระบบปฏิบัติการของ Apple สำหรับการเปิดตัวระบบปฏิบัติการครั้งใหญ่ในแต่ละครั้ง โดยใช้โปรไฟล์การปกป้องเชิงร่วมมือที่เหมาะสมและระดับความปลอดภัย FIPS 140-3 การตรวจสอบความถูกต้องของความสอดคล้องสามารถดำเนินการได้เฉพาะกับเวอร์ชั่นสุดท้ายที่เปิดตัวเท่านั้น

หมายเหตุ: ในปี 2562 ระบบปฏิบัติการสำหรับอุปกรณ์ iPad ได้รับการรีแบรนด์ใหม่เป็น iPadOS ก่อนหน้า iPadOS 13.1 iPadOS มีชื่อว่า iOS

สถานะการตรวจสอบความถูกต้องของโมดูลการเข้ารหัส iPadOS

โปรแกรมการตรวจสอบความถูกต้องโมดูลการเข้ารหัส (CMVP) ยังคงใช้สถานะการตรวจสอบความถูกต้องของโมดูลการเข้ารหัสภายใต้รายการที่แยกออกจากกันสามรายการซึ่งขึ้นอยู่กับสถานะปัจจุบันของแต่ละรายการ:

- ในการที่จะได้รับการระบุอยู่ในรายการการปรับใช้อยู่ระหว่างการทดสอบของ CMVP ห้องปฏิบัติการจะต้องทำสัญญากับ Apple ในการดำเนินการทดสอบ
- หลังจากที่การทดสอบเสร็จสมบูรณ์โดยห้องปฏิบัติการ และเมื่อห้องปฏิบัติการได้แนะนำการตรวจสอบความถูกต้องโดย CMVP และได้ชำระค่าธรรมเนียม CMVP แล้ว จากนั้นโมดูลจะถูกเพิ่มไปยังรายการโมดูลในกระบวนการ (MIP) รายการ MIP จะติดตามความคืบหน้าของความพยายามในการตรวจสอบความถูกต้องของ CMVP ซึ่งแบ่งเป็นสี่ระยะ:
  - **รอการตรวจสอบ:** รอการกำหนดทรัพยากรของ CMVP
  - **อยู่ในระหว่างการตรวจสอบ:** ทรัพยากรของ CMVP อยู่ในระหว่างดำเนินการกิจกรรมการตรวจสอบความถูกต้อง
  - **ดำเนินการร่วมกัน:** ห้องปฏิบัติการและ CMVP กำลังแก้ไขปัญหาที่พบ
  - **สรุป:** กิจกรรมและระเบียบแบบแผนที่เกี่ยวข้องกับการออกการรับรอง
- หลังจากการตรวจสอบความถูกต้องโดย CMVP โมดูลจะได้รับการรับรองความสอดคล้องและถูกเพิ่มไปยังรายการโมดูลการเข้ารหัสที่ได้รับการตรวจสอบความถูกต้องแล้ว ซึ่งประกอบด้วย:
  - โมดูลที่ได้รับการตรวจสอบความถูกต้องแล้วจะถูกทำเครื่องหมายว่าใช้งานอยู่
  - หลังจาก 5 ปี โมดูลจะถูกทำเครื่องหมายเป็นประวัติ
  - ถ้าการรับรองโมดูลถูกเพิกถอนด้วยเหตุผลบางประการ โมดูลจะถูกทำเครื่องหมายว่าถูกเพิกถอน

ในปี 2563 CMVP ได้นำมาตรฐานสากล ISO/IEC 19790 มาใช้เป็นพื้นฐานสำหรับ FIPS 140-3

การรับรอง FIPS 140-3

สถานะปัจจุบัน

พื้นที่ผู้ใช้ของ iPadOS 14 (2563), พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยได้รับการทดสอบโดยเสร็จสมบูรณ์ในห้องปฏิบัติการแล้วและได้รับคำแนะนำจากห้องปฏิบัติการในการตรวจสอบความถูกต้องกับ CMVP รายการจะได้รับการระบุอยู่บนรายการโมดูลในกระบวนการ

พื้นที่ผู้ใช้ของ iPadOS 15 (2564), พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยกำลังอยู่ระหว่างการทดสอบในห้องปฏิบัติการ รายการจะได้รับการระบุอยู่บนรายการการปรับใช้อยู่ระหว่างการทดสอบ

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** iPadOS 15 **สภาพแวดล้อม:** Apple Silicon, ผู้ใช้, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** iPadOS 15 **สภาพแวดล้อม:** Apple Silicon, เคอร์เนล, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ iPadOS 15 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (A9-A14, M1) **ระดับความปลอดภัยโดยรวม:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ iPadOS 15 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (A9-A14, M1) **ระดับความปลอดภัยโดยรวม:** 2 **ระดับความปลอดภัยทางกายภาพ:** 3
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** iPadOS 14 **สภาพแวดล้อม:** Apple Silicon, ผู้ใช้, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** iPadOS 14 **สภาพแวดล้อม:** Apple Silicon, เคอร์เนล, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ iPadOS 14 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (A9-A14, M1) **ระดับความปลอดภัยโดยรวม:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ iPadOS 14 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (A9-A14, M1) **ระดับความปลอดภัยโดยรวม:** 2 **ระดับความปลอดภัยทางกายภาพ:** 3

การรับรอง FIPS 140-2

ตารางด้านล่างจะแสดงโมดูลการเข้ารหัสที่อยู่ในระหว่างการทดสอบในตอนนี้และได้รับการทดสอบแล้วในด้านความสอดคล้องกับ FIPS 140-2 ในห้องปฏิบัติการ

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 23 มีนาคม 2564	**การรับรอง:** 3856 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v10.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** iPadOS 13 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 23 มีนาคม 2564	**การรับรอง:** 3855 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v10.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** iPadOS 13 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 5 กุมภาพันธ์ 2564	**การรับรอง:** 3811 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัย Corecrypto ของ Apple v10.0 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ iPadOS 13 **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 23 เมษายน 2562	**การรับรอง:** 3438 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v9.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** iOS 12 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 11 เมษายน 2562	**การรับรอง:** 3433 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v9.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** iOS 12 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 10 กันยายน 2562	**การรับรอง:** 3523 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v9.0 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ iOS 12 **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 9/3/2561, 22/5/2561, 6/7/2561	**การรับรอง:** 3148 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v8.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** iOS 11 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 9/3/2561, 17/5/2561, 3/7/2561	**การรับรอง:** 3147 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v8.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** iOS 11 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 10 กันยายน 2562	**การรับรอง:** 3223 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v1.0 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ iOS 11 **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2559 **วันที่ตรวจสอบความถูกต้อง:** 1 กุมภาพันธ์ 2560	**การรับรอง:** 2828 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** iOS Corecrypto Kernel Module v7.0 ของ Apple **ระบบปฏิบัติการ:** iOS 10 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2559 **วันที่ตรวจสอบความถูกต้อง:** 1 กุมภาพันธ์ 2560	**การรับรอง:** 2827 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** iOS Corecrypto Kernel Module v7.0 ของ Apple **ระบบปฏิบัติการ:** iOS 10 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1

เวอร์ชั่นก่อนหน้านี้

การรับรองที่มีอายุมากกว่า 5 ปีจะถูก CMVP ระบุไว้เป็นสถานะประวัติ iOS เวอร์ชั่นก่อนหน้าเหล่านี้มีการตรวจสอบความถูกต้องโมดูลการเข้ารหัส:

- iOS 9 (โมดูล corecrypto v6.0)
- iOS 8 (โมดูล corecrypto v5.0)
- iOS 7 (โมดูล corecrypto v4.0)
- iOS 6 (โมดูล corecrypto v3.0)

ความเป็นมาของการรับรองเกณฑ์ทั่วไป (CC)

Apple ได้เข้าไปมีส่วนร่วมเชิงรุกในการประเมิน iPadOS ในการเปิดตัวระบบปฏิบัติการครั้งใหญ่ในแต่ละครั้ง การประเมินจะต้องดำเนินการกับระบบปฏิบัติการเวอร์ชั่นสุดท้ายที่เปิดตัวเป็นสาธารณะเท่านั้น

สถานะการรับรองเกณฑ์ทั่วไป (CC)

แบบแผนของสหรัฐอเมริกาที่ดำเนินการโดย NIAP จะเก็บรักษารายการของผลิตภัณฑ์ในการประเมิน ซึ่งรายการนี้จะประกอบไปด้วยผลิตภัณฑ์ที่อยู่ระหว่างการประเมินกับห้องปฏิบัติการการทดสอบเกณฑ์ทั่วไป (CCTL) ที่ได้รับการรับรองจาก NIAP ในสหรัฐอเมริกาและผลิตภัณฑ์ที่ผ่านการประชุมเริ่มงานการประเมิน (หรือเทียบเท่า) ซึ่งผู้บริหารของ CCEVS ได้ยอมรับผลิตภัณฑ์เข้าสู่การประเมินอย่างเป็นทางการแล้ว

หลังผลิตภัณฑ์ได้รับการรับรองแล้ว NIAP ใส่การรับรองที่สามารถใช้งานได้ในตอนนี้ไว้บนรายการข้อร้องเรียนผลิตภัณฑ์ขององค์กร การรับรองเหล่านี้จะถูกตรวจสอบด้านความสอดคล้องกับนโยบายการรับประกันการซ่อมในปัจจุบันหลังจาก 2 ปี หลังจากวันรับประกันการซ่อมหมดอายุแล้ว NIAP จะย้ายการแสดงการรับรองไปยังรายการผลิตภัณฑ์ที่ถูกเก็บถาวรขององค์กร

พอร์ทัลเกณฑ์ทั่วไปจะแสดงการรับรองที่สามารถยอมรับร่วมกันได้ภายใต้การจัดการรับรองเกณฑ์ทั่วไป (CCRA) พอร์ทัล CC อาจเก็บผลิตภัณฑ์ไว้บนรายการผลิตภัณฑ์ที่ได้รับการรับรองเป็นเวลา 5 ปี โดยการบันทึกจะถูกเก็บไว้โดยพอร์ทัล CC สำหรับการรับรองที่ถูกเก็บถาวร

ตารางด้านล่างจะแสดงการรับรองที่อยู่ในระหว่างการประเมินในห้องปฏิบัติการในตอนนี้ หรือการรับรองที่ได้รับการรับรองแล้วว่าสอดคล้องกับเกณฑ์ทั่วไป

สถานะปัจจุบัน

การทดสอบในห้องปฏิบัติการสำหรับการประเมินกับ NIAP สำหรับ iPadOS 15 กำลังดำเนินการอยู่ สำหรับข้อมูลล่าสุด ให้ดูที่ผลิตภัณฑ์ในการประเมิน (NIAP) และรายการผลิตภัณฑ์ที่เป็นไปตามข้อกำหนด

ระบบปฏิบัติการ / วันที่ออกการรับรอง	ID แบบแผน / เอกสาร	ชื่อเรื่อง / โปรไฟล์การปกป้อง
ระบบปฏิบัติการ: iPadOS 15 **วันที่ออกการรับรอง:** 14 มีนาคม 2562	**ID แบบแผน:** — **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** iPad ที่ใช้ iOS 12 **โปรไฟล์การปกป้อง:** พื้นฐานอุปกรณ์เคลื่อนที่, โมดูลลูกข่าย VPN, EP ลูกข่าย LAN ไร้สาย, EP เอเจ็นต์ MDM
ระบบปฏิบัติการ: iPadOS 14 **วันที่ออกการรับรอง:** 1 กันยายน 2564	**ID แบบแผน:** 11147 **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** iPadOS 14 ของ Apple: iPad **โปรไฟล์การปกป้อง:** พื้นฐานอุปกรณ์เคลื่อนที่, โมดูลลูกข่าย VPN, EP ลูกข่าย LAN ไร้สาย, EP เอเจ็นต์ MDM
ระบบปฏิบัติการ: iPadOS 13 **วันที่ออกการรับรอง:** 6 พฤศจิกายน 2563	**ID แบบแผน:** 11036 **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** iPadOS 13 บนอุปกรณ์เคลื่อนที่ iPad **โปรไฟล์การปกป้อง:** พื้นฐานอุปกรณ์เคลื่อนที่, โมดูลลูกข่าย VPN, EP ลูกข่าย LAN ไร้สาย, EP เอเจ็นต์ MDM

เวอร์ชั่นก่อนหน้านี้

iOS เวอร์ชั่นก่อนหน้าเหล่านี้มีการตรวจสอบความถูกต้องเกณฑ์ทั่วไป เวอร์ชั่นเหล่านี้ถูกเก็บถาวรโดย NIAP ตามนโยบายของ NIAP:

- iOS 12 (ID แบบแผน: 10937)
- iOS 11 (ID แบบแผน: 10851)
- iOS 10 (ID แบบแผน: 107782, 10792)
- iOS 9 (ID แบบแผน: 10725, 10714, 10695)

การรับรองความปลอดภัยสำหรับ macOS

ความเป็นมาของการรับรอง macOS

Apple ได้เข้าไปมีส่วนร่วมเชิงรุกในการตรวจสอบความถูกต้องของระบบปฏิบัติการของ Apple สำหรับการเปิดตัวระบบปฏิบัติการครั้งใหญ่ในแต่ละครั้ง โดยใช้โปรไฟล์การปกป้องเชิงร่วมมือที่เหมาะสมและระดับความปลอดภัย FIPS 140-3 การตรวจสอบความถูกต้องของความสอดคล้องสามารถดำเนินการได้เฉพาะกับเวอร์ชั่นสุดท้ายที่เปิดตัวเท่านั้น

สถานะการตรวจสอบความถูกต้องโมดูลการเข้ารหัส macOS

โปรแกรมการตรวจสอบความถูกต้องโมดูลการเข้ารหัส (CMVP) ยังคงใช้สถานะการตรวจสอบความถูกต้องของโมดูลการเข้ารหัสภายใต้รายการที่แยกออกจากกันสามรายการซึ่งขึ้นอยู่กับสถานะปัจจุบันของแต่ละรายการ:

- ในการที่จะได้รับการระบุอยู่ในรายการการปรับใช้อยู่ระหว่างการทดสอบของ CMVP ห้องปฏิบัติการจะต้องทำสัญญากับ Apple ในการดำเนินการทดสอบ
- หลังจากที่การทดสอบเสร็จสมบูรณ์โดยห้องปฏิบัติการ และเมื่อห้องปฏิบัติการได้แนะนำการตรวจสอบความถูกต้องโดย CMVP และได้ชำระค่าธรรมเนียม CMVP แล้ว จากนั้นโมดูลจะถูกเพิ่มไปยังรายการโมดูลในกระบวนการ (MIP) รายการ MIP จะติดตามความคืบหน้าของความพยายามในการตรวจสอบความถูกต้องของ CMVP ซึ่งแบ่งเป็นสี่ระยะ:
  - **รอการตรวจสอบ:** รอการกำหนดทรัพยากรของ CMVP
  - **อยู่ในระหว่างการตรวจสอบ:** ทรัพยากรของ CMVP อยู่ในระหว่างดำเนินการกิจกรรมการตรวจสอบความถูกต้อง
  - **ดำเนินการร่วมกัน:** ห้องปฏิบัติการและ CMVP กำลังแก้ไขปัญหาที่พบ
  - **สรุป:** กิจกรรมและระเบียบแบบแผนที่เกี่ยวข้องกับการออกการรับรอง
- หลังจากการตรวจสอบความถูกต้องโดย CMVP โมดูลจะได้รับการรับรองความสอดคล้องและถูกเพิ่มไปยังรายการโมดูลการเข้ารหัสที่ได้รับการตรวจสอบความถูกต้องแล้ว ซึ่งประกอบด้วย:
  - โมดูลที่ได้รับการตรวจสอบความถูกต้องแล้วจะถูกทำเครื่องหมายว่าใช้งานอยู่
  - หลังจาก 5 ปี โมดูลจะถูกทำเครื่องหมายเป็นประวัติ
  - ถ้าการรับรองโมดูลถูกเพิกถอนด้วยเหตุผลบางประการ โมดูลจะถูกทำเครื่องหมายว่าถูกเพิกถอน

ในปี 2563 CMVP ได้นำมาตรฐานสากล ISO/IEC 19790 มาใช้เป็นพื้นฐานสำหรับ FIPS 140-3

สำหรับคอมพิวเตอร์ Mac ของ Apple ตารางที่ด้านล่างจะแสดงโมดูลการเข้ารหัสต่างๆ ที่สามารถใช้งานได้กับเทคโนโลยีของ Mac

โมดูลการเข้ารหัส	คอมพิวเตอร์ Mac ที่ใช้ Apple Silicon	คอมพิวเตอร์ Mac ที่มีชิป Apple T2 Security	คอมพิวเตอร์ Mac ที่ใช้ Intel ที่ไม่มีชิป Apple T2 Security
พื้นที่ผู้ใช้ของ Apple Silicon	✓		
เคอร์เนลของ Apple Silicon	✓		
พื้นที่ผู้ใช้ของ Intel		✓	✓
เคอร์เนลของ Intel		✓	✓
การจัดเก็บกุญแจอย่างปลอดภัย	✓	✓	

การรับรอง FIPS 140-3

ในปี 2563 Apple ได้เปิดตัวคอมพิวเตอร์ Mac ที่ใช้ Apple Silicon การนำโมดูลการเข้ารหัสมาใช้งานกับคอมพิวเตอร์ Mac ที่ใช้ Apple Silicon หรือที่ใช้ Intel จะระบุอยู่ในคอลัมน์ข้อมูลโมดูลในตารางด้านล่าง

หมายเหตุ: ชิป Apple T2 Security มีอยู่ในคอมพิวเตอร์ Mac ที่ใช้ Intel หลายๆ รุ่น สำหรับข้อมูลเกี่ยวกับการรับรองชิป T2 ให้ดูที่ การรับรองความปลอดภัยสำหรับชิป Apple T2 Security

ลูกข่าย SSH สำหรับ macOS

สามารถกำหนดค่า OpenSSH ให้ใช้โมดูลที่ได้รับการตรวจสอบความถูกต้อง FIPS 140-3 สำหรับอัลกอริธึม FIPS 140-3 ที่เลือกได้ องค์กรสามารถเรียกใช้ตัวติดตั้งที่มีการลงชื่อและรับรองซึ่งมีให้จาก Apple ด้วยรหัสผ่าน **FIPS**140**Mode** ได้ ตัวติดตั้งจะเก็บสองไฟล์ไว้บน Mac:

- **fips_ssh_config:** อยู่ใน /private/etc/ssh/ssh_config.d/
- **fips_sshd_config:** อยู่ใน /private/etc/ssh/sshd_config.d/

จากนั้น macOS จะใช้ไฟล์เหล่านี้เพื่อจำกัดรหัสที่ใช้ได้กับ OpenSSH สำหรับไฟล์ที่ได้รับการตรวจสอบความถูกต้องโดย NIST เท่านั้น และจะช่วยให้มั่นใจได้ว่าลูกข่าย OpenSSH ใช้โมดูลการเข้ารหัสที่ได้รับการตรวจสอบความถูกต้องและมีแพลตฟอร์มมาให้ ผู้ดูแลระบบยังสามารถสร้างไฟล์ของตัวเองได้ด้วย โปรดดูหน้าคู่มือ `apple_ssh_and_fips` ใน macOS 12.0.1 ขึ้นไป สำหรับข้อมูลเพิ่มเติม

สถานะปัจจุบัน

พื้นที่ผู้ใช้ของ macOS 11 Big Sur, พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยได้รับการทดสอบโดยเสร็จสมบูรณ์ในห้องปฏิบัติการแล้วและได้รับคำแนะนำจากห้องปฏิบัติการในการตรวจสอบความถูกต้องกับ CMVP รายการจะได้รับการระบุอยู่บนรายการโมดูลในกระบวนการ

พื้นที่ผู้ใช้ของ macOS 12 Monterey, พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยกำลังอยู่ระหว่างการทดสอบในห้องปฏิบัติการ รายการจะได้รับการระบุอยู่บนรายการการปรับใช้อยู่ระหว่างการทดสอบ

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12.0 **ระบบปฏิบัติการ:** macOS 12 Monterey บน Apple Silicon **สภาพแวดล้อม:** Apple Silicon, ผู้ใช้, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12.0 **ระบบปฏิบัติการ:** macOS 12 Monterey บน Apple Silicon **สภาพแวดล้อม:** Apple Silicon, เคอร์เนล, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12.0 **ระบบปฏิบัติการ:** macOS 12 Monterey บน Intel **สภาพแวดล้อม:** Intel, ผู้ใช้, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12.0 **ระบบปฏิบัติการ:** macOS 12 Monterey บน Intel **สภาพแวดล้อม:** Intel, เคอร์เนล, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12.0 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ macOS 12 Monterey บน Apple Silicon, sepOS ที่เผยแพร่พร้อมกับ macOS 12 Monterey บน Intel ที่มี T2 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (M1 และ T2) **ระดับความปลอดภัย:** 2

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12.0 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ macOS 12 Monterey บน Apple Silicon **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (M1) **ระดับความปลอดภัย:** 2 **ระดับความปลอดภัยทางกายภาพ:** 3
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** macOS 11 Big Sur บน Intel **สภาพแวดล้อม:** Intel, ผู้ใช้, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** macOS 11 Big Sur บน Intel **สภาพแวดล้อม:** Intel, เคอร์เนล, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** macOS 11 Big Sur บน Apple Silicon **สภาพแวดล้อม:** Apple Silicon, ผู้ใช้, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** macOS 11 Big Sur บน Apple Silicon **สภาพแวดล้อม:** Apple Silicon, เคอร์เนล, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ macOS 11 Big Sur บน Apple Silicon, sepOS ที่เผยแพร่พร้อมกับ macOS 11 Big Sur บน Intel **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (M1) **ระดับความปลอดภัย:** 2

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ macOS 11 Big Sur บน Apple Silicon **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (M1) **ระดับความปลอดภัย:** 2 **ระดับความปลอดภัยทางกายภาพ:** 3

การรับรอง FIPS 140-2

ตารางด้านล่างจะแสดงโมดูลการเข้ารหัสที่อยู่ในระหว่างการทดสอบในตอนนี้และได้รับการทดสอบแล้วในด้านความสอดคล้องกับ FIPS 140-2 ในห้องปฏิบัติการ

พื้นที่ผู้ใช้ของ macOS 10.15 Catalina, พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยได้รับการทดสอบโดยเสร็จสมบูรณ์ในห้องปฏิบัติการแล้วและได้รับคำแนะนำจากห้องปฏิบัติการในการตรวจสอบความถูกต้องกับ CMVP รายการจะได้รับการระบุอยู่บนรายการโมดูลในกระบวนการ

หมายเหตุ: ชิป Apple T2 Security มีอยู่ในคอมพิวเตอร์ Mac ที่ใช้ Intel หลายๆ รุ่น สำหรับข้อมูลเกี่ยวกับการรับรองชิป T2 ให้ดูที่ การรับรองความปลอดภัยสำหรับชิป Apple T2 Security

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 24 มีนาคม 2564	**การรับรอง:** 3859 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto User Space Module สำหรับ Intel (ccv10) **ระบบปฏิบัติการ:** macOS 10.15 Catalina **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 24 มีนาคม 2564	**การรับรอง:** 3858 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v10.0 ของ Apple สำหรับ Intel (ccv10) **ระบบปฏิบัติการ:** macOS 10.15 Catalina **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 12 เมษายน 2562	**การรับรอง:** 3402 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v9.0 ของ Apple สำหรับ Intel **ระบบปฏิบัติการ:** macOS 10.14 Mojave **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 12 เมษายน 2562	**การรับรอง:** 3431 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v9.0 ของ Apple สำหรับ Intel **ระบบปฏิบัติการ:** macOS 10.14 Mojave **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 22 มีนาคม 2561	**การรับรอง:** 3155 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v8.0 ของ Apple สำหรับ Intel **ระบบปฏิบัติการ:** macOS 10.13 High Sierra **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 22 มีนาคม 2561	**การรับรอง:** 3156 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v8.0 ของ Apple สำหรับ Intel **ระบบปฏิบัติการ:** macOS 10.13 High Sierra **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1

เวอร์ชั่นก่อนหน้านี้

OS X และ macOS เวอร์ชั่นก่อนหน้าเหล่านี้มีการตรวจสอบความถูกต้องโมดูลการเข้ารหัส ส่วนเวอร์ชั่นที่มีอายุมากกว่า 5 ปีจะถูก CMVP ระบุไว้เป็นสถานะประวัติ:

- macOS 10.12 Sierra
- OS X 10.11 El Capitan
- OS X 10.10 Yosemite
- OS X 10.9 Mavericks
- OS X 10.8 Mountain Lion
- OS X 10.7 Lion
- OS X 10.6 Snow Leopard

ความเป็นมาของการรับรองเกณฑ์ทั่วไป (CC)

Apple ได้เข้าไปมีส่วนร่วมเชิงรุกในการประเมิน macOS ในการเปิดตัวระบบปฏิบัติการครั้งใหญ่ในแต่ละครั้ง การประเมินจะต้องดำเนินการกับระบบปฏิบัติการเวอร์ชั่นสุดท้ายที่เปิดตัวเป็นสาธารณะเท่านั้น

สถานะการรับรองเกณฑ์ทั่วไป (CC)

แบบแผนของสหรัฐอเมริกาที่ดำเนินการโดย NIAP จะเก็บรักษารายการของผลิตภัณฑ์ในการประเมิน ซึ่งรายการนี้จะประกอบไปด้วยผลิตภัณฑ์ที่อยู่ระหว่างการประเมินกับห้องปฏิบัติการการทดสอบเกณฑ์ทั่วไป (CCTL) ที่ได้รับการรับรองจาก NIAP ในสหรัฐอเมริกาและผลิตภัณฑ์ที่ผ่านการประชุมเริ่มงานการประเมิน (หรือเทียบเท่า) ซึ่งผู้บริหารของ CCEVS ได้ยอมรับผลิตภัณฑ์เข้าสู่การประเมินอย่างเป็นทางการแล้ว

หลังผลิตภัณฑ์ได้รับการรับรองแล้ว NIAP ใส่การรับรองที่สามารถใช้งานได้ในตอนนี้ไว้บนรายการข้อร้องเรียนผลิตภัณฑ์ขององค์กร การรับรองเหล่านี้จะถูกตรวจสอบด้านความสอดคล้องกับนโยบายการรับประกันการซ่อมในปัจจุบันหลังจาก 2 ปี หลังจากวันรับประกันการซ่อมหมดอายุแล้ว NIAP จะย้ายการแสดงการรับรองไปยังรายการผลิตภัณฑ์ที่ถูกเก็บถาวรขององค์กร

พอร์ทัลเกณฑ์ทั่วไปจะแสดงการรับรองที่สามารถยอมรับร่วมกันได้ภายใต้การจัดการรับรองเกณฑ์ทั่วไป (CCRA) พอร์ทัล CC อาจเก็บผลิตภัณฑ์ไว้บนรายการผลิตภัณฑ์ที่ได้รับการรับรองเป็นเวลา 5 ปี โดยการบันทึกจะถูกเก็บไว้โดยพอร์ทัล CC สำหรับการรับรองที่ถูกเก็บถาวร

ตารางด้านล่างจะแสดงการรับรองที่อยู่ในระหว่างการประเมินในห้องปฏิบัติการในตอนนี้ หรือการรับรองที่ได้รับการรับรองแล้วว่าสอดคล้องกับเกณฑ์ทั่วไป

สถานะปัจจุบัน

การประเมินด้วย NIAP สำหรับ macOS 11 และ macOS 12 โดยใช้โปรไฟล์การปกป้องสำหรับระบบปฏิบัติการเพื่อวัตถุประสงค์ทั่วไปและการเข้ารหัสดิสก์แบบเต็มรูปแบบ (FDE) (AA และ EE) กำลังอยู่ในระหว่างการพัฒนา

สำหรับข้อมูลล่าสุด ให้ดูที่ผลิตภัณฑ์ในการประเมิน (NIAP) และรายการผลิตภัณฑ์ที่เป็นไปตามข้อกำหนด

ระบบปฏิบัติการ / วันที่ออกการรับรอง	ID แบบแผน / เอกสาร	ชื่อเรื่อง / โปรไฟล์การปกป้อง
ระบบปฏิบัติการ: macOS 12 Monterey **วันที่ออกการรับรอง:** —	**ID แบบแผน:** ยังไม่ได้รับรอง **เอกสาร:** —	**ชื่อเรื่อง:** Apple FileVault 2 กับ macOS 12 Monterey **โปรไฟล์การปกป้อง:** CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E (รอยืนยัน PP)
ระบบปฏิบัติการ: macOS 12 Monterey **วันที่ออกการรับรอง:** —	**ID แบบแผน:** ยังไม่ได้รับรอง **เอกสาร:** —	**ชื่อเรื่อง:** macOS 12 Monterey **โปรไฟล์การปกป้อง:** PP_OS_V4.21 (รอยืนยัน PP)
ระบบปฏิบัติการ: macOS 11 Big Sur **วันที่ออกการรับรอง:** —	**ID แบบแผน:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** Apple FileVault 2 กับ macOS 11 Big Sur **โปรไฟล์การปกป้อง:** CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
ระบบปฏิบัติการ: macOS 11 Big Sur **วันที่ออกการรับรอง:** —	**ID แบบแผน:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** Apple macOS 11 Big Sur **โปรไฟล์การปกป้อง:** PP_OS_V4.21
ระบบปฏิบัติการ: macOS 10.15 Catalina **วันที่ออกการรับรอง:** 29 เมษายน 2564	**ID แบบแผน:** 11078 **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** Apple FileVault 2 บนคอมพิวเตอร์ T2 ที่ใช้ macOS 10.15 Catalina **โปรไฟล์การปกป้อง:** CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
ระบบปฏิบัติการ: macOS 10.15 Catalina **วันที่ออกการรับรอง:** 23 กันยายน 2563	**ID แบบแผน:** 11077 **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** macOS 10.15 Catalina **โปรไฟล์การปกป้อง:** PP_OS_V4.21

การรับรองความปลอดภัยสำหรับ tvOS

ความเป็นมาของการรับรอง tvOS

Apple ได้เข้าไปมีส่วนร่วมเชิงรุกในการตรวจสอบความถูกต้องของโมดูลการเข้ารหัสที่เกี่ยวข้องกับการเปิดตัว tvOS ครั้งใหญ่ในแต่ละครั้ง การตรวจสอบความถูกต้องของความสอดคล้องสามารถดำเนินการได้เฉพาะกับเวอร์ชั่นสุดท้ายที่เปิดตัวเท่านั้น

สถานะการตรวจสอบความถูกต้องโมดูลการเข้ารหัส tvOS

โปรแกรมการตรวจสอบความถูกต้องโมดูลการเข้ารหัส (CMVP) ยังคงใช้สถานะการตรวจสอบความถูกต้องของโมดูลการเข้ารหัสภายใต้รายการที่แยกออกจากกันสามรายการซึ่งขึ้นอยู่กับสถานะปัจจุบันของแต่ละรายการ:

- ในการที่จะได้รับการระบุอยู่ในรายการการปรับใช้อยู่ระหว่างการทดสอบของ CMVP ห้องปฏิบัติการจะต้องทำสัญญากับ Apple ในการดำเนินการทดสอบ
- หลังจากที่การทดสอบเสร็จสมบูรณ์โดยห้องปฏิบัติการ และเมื่อห้องปฏิบัติการได้แนะนำการตรวจสอบความถูกต้องโดย CMVP และได้ชำระค่าธรรมเนียม CMVP แล้ว จากนั้นโมดูลจะถูกเพิ่มไปยังรายการโมดูลในกระบวนการ (MIP) รายการ MIP จะติดตามความคืบหน้าของความพยายามในการตรวจสอบความถูกต้องของ CMVP ซึ่งแบ่งเป็นสี่ระยะ:
  - **รอการตรวจสอบ:** รอการกำหนดทรัพยากรของ CMVP
  - **อยู่ในระหว่างการตรวจสอบ:** ทรัพยากรของ CMVP อยู่ในระหว่างดำเนินการกิจกรรมการตรวจสอบความถูกต้อง
  - **ดำเนินการร่วมกัน:** ห้องปฏิบัติการและ CMVP กำลังแก้ไขปัญหาที่พบ
  - **สรุป:** กิจกรรมและระเบียบแบบแผนที่เกี่ยวข้องกับการออกการรับรอง
- หลังจากการตรวจสอบความถูกต้องโดย CMVP โมดูลจะได้รับการรับรองความสอดคล้องและถูกเพิ่มไปยังรายการโมดูลการเข้ารหัสที่ได้รับการตรวจสอบความถูกต้องแล้ว ซึ่งประกอบด้วย:
  - โมดูลที่ได้รับการตรวจสอบความถูกต้องแล้วจะถูกทำเครื่องหมายว่าใช้งานอยู่
  - หลังจาก 5 ปี โมดูลจะถูกทำเครื่องหมายเป็นประวัติ
  - ถ้าการรับรองโมดูลถูกเพิกถอนด้วยเหตุผลบางประการ โมดูลจะถูกทำเครื่องหมายว่าถูกเพิกถอน

ในปี 2563 CMVP ได้นำมาตรฐานสากล ISO/IEC 19790 มาใช้เป็นพื้นฐานสำหรับ FIPS 140-3

การรับรอง FIPS 140-3

สถานะปัจจุบัน

พื้นที่ผู้ใช้ของ tvOS 14 (2563), พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยได้รับการทดสอบโดยเสร็จสมบูรณ์ในห้องปฏิบัติการแล้วและได้รับคำแนะนำจากห้องปฏิบัติการในการตรวจสอบความถูกต้องกับ CMVP รายการจะได้รับการระบุอยู่บนรายการโมดูลในกระบวนการ

พื้นที่ผู้ใช้ของ tvOS 15 (2564), พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยกำลังอยู่ระหว่างการทดสอบในห้องปฏิบัติการ รายการจะได้รับการระบุอยู่บนรายการการปรับใช้อยู่ระหว่างการทดสอบ

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** tvOS 15 **สภาพแวดล้อม:** Apple Silicon, ผู้ใช้, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** tvOS 15 **สภาพแวดล้อม:** Apple Silicon, เคอร์เนล, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ tvOS 15 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (A10, A12) **ระดับความปลอดภัยโดยรวม:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** tvOS 14 **สภาพแวดล้อม:** Apple Silicon, ผู้ใช้, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** tvOS 14 **สภาพแวดล้อม:** Apple Silicon, เคอร์เนล, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ tvOS 14 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (A10, A12) **ระดับความปลอดภัยโดยรวม:** 2

การรับรอง FIPS 140-2

ตารางด้านล่างจะแสดงโมดูลการเข้ารหัสที่อยู่ในระหว่างการทดสอบในตอนนี้และได้รับการทดสอบแล้วในด้านความสอดคล้องกับ FIPS 140-2 ในห้องปฏิบัติการ

พื้นที่ผู้ใช้ของ tvOS 13 (2562), พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยได้รับการทดสอบโดยเสร็จสมบูรณ์ในห้องปฏิบัติการแล้วและได้รับคำแนะนำจากห้องปฏิบัติการในการตรวจสอบความถูกต้องกับ CMVP รายการจะได้รับการระบุอยู่บนรายการโมดูลในกระบวนการ

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 23 มีนาคม 2564	**การรับรอง:** 3856 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v10.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** tvOS 13 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 23 มีนาคม 2564	**การรับรอง:** 3855 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v10.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** tvOS 13 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 5 กุมภาพันธ์ 2564	**การรับรอง:** 3811 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v10.0 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ tvOS 13 **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 23 เมษายน 2562	**การรับรอง:** 3438 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v9.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** tvOS 12 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 11 เมษายน 2562	**การรับรอง:** 3433 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v9.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** tvOS 12 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 10 กันยายน 2562	**การรับรอง:** 3523 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v9.0 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ tvOS 12 **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 9/3/2561, 22/5/2561, 6/7/2561	**การรับรอง:** 3148 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v8.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** tvOS 11 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 9/3/2561, 17/5/2561, 3/7/2561	**การรับรอง:** 3147 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v8.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** tvOS 11 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 10 กันยายน 2562	**การรับรอง:** 3223 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v1.0 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ tvOS 11 **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2

การรับรองความปลอดภัยสำหรับ watchOS

ความเป็นมาของการรับรอง watchOS

Apple ได้เข้าไปมีส่วนร่วมเชิงรุกในการตรวจสอบความถูกต้องของโมดูลการเข้ารหัสที่เกี่ยวข้องกับการเปิดตัว watchOS ครั้งใหญ่ในแต่ละครั้ง การตรวจสอบความถูกต้องของความสอดคล้องสามารถดำเนินการได้เฉพาะกับเวอร์ชั่นสุดท้ายที่เปิดตัวเท่านั้น

สถานะการตรวจสอบความถูกต้องโมดูลการเข้ารหัส watchOS

โปรแกรมการตรวจสอบความถูกต้องโมดูลการเข้ารหัส (CMVP) ยังคงใช้สถานะการตรวจสอบความถูกต้องของโมดูลการเข้ารหัสภายใต้รายการที่แยกออกจากกันสามรายการซึ่งขึ้นอยู่กับสถานะปัจจุบันของแต่ละรายการ:

- ในการที่จะได้รับการระบุอยู่ในรายการการปรับใช้อยู่ระหว่างการทดสอบของ CMVP ห้องปฏิบัติการจะต้องทำสัญญากับ Apple ในการดำเนินการทดสอบ
- หลังจากที่การทดสอบเสร็จสมบูรณ์โดยห้องปฏิบัติการ และเมื่อห้องปฏิบัติการได้แนะนำการตรวจสอบความถูกต้องโดย CMVP และได้ชำระค่าธรรมเนียม CMVP แล้ว จากนั้นโมดูลจะถูกเพิ่มไปยังรายการโมดูลในกระบวนการ (MIP) รายการ MIP จะติดตามความคืบหน้าของความพยายามในการตรวจสอบความถูกต้องของ CMVP ซึ่งแบ่งเป็นสี่ระยะ:
  - **รอการตรวจสอบ:** รอการกำหนดทรัพยากรของ CMVP
  - **อยู่ในระหว่างการตรวจสอบ:** ทรัพยากรของ CMVP อยู่ในระหว่างดำเนินการกิจกรรมการตรวจสอบความถูกต้อง
  - **ดำเนินการร่วมกัน:** ห้องปฏิบัติการและ CMVP กำลังแก้ไขปัญหาที่พบ
  - **สรุป:** กิจกรรมและระเบียบแบบแผนที่เกี่ยวข้องกับการออกการรับรอง
- หลังจากการตรวจสอบความถูกต้องโดย CMVP โมดูลจะได้รับการรับรองความสอดคล้องและถูกเพิ่มไปยังรายการโมดูลการเข้ารหัสที่ได้รับการตรวจสอบความถูกต้องแล้ว ซึ่งประกอบด้วย:
  - โมดูลที่ได้รับการตรวจสอบความถูกต้องแล้วจะถูกทำเครื่องหมายว่าใช้งานอยู่
  - หลังจาก 5 ปี โมดูลจะถูกทำเครื่องหมายเป็นประวัติ
  - ถ้าการรับรองโมดูลถูกเพิกถอนด้วยเหตุผลบางประการ โมดูลจะถูกทำเครื่องหมายว่าถูกเพิกถอน

ในปี 2563 CMVP ได้นำมาตรฐานสากล ISO/IEC 19790 มาใช้เป็นพื้นฐานสำหรับ FIPS 140-3

การรับรอง FIPS 140-3

สถานะปัจจุบัน

พื้นที่ผู้ใช้ของ watchOS 7 (2563), พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยได้รับการทดสอบโดยเสร็จสมบูรณ์ในห้องปฏิบัติการแล้วและได้รับคำแนะนำจากห้องปฏิบัติการในการตรวจสอบความถูกต้องกับ CMVP รายการจะได้รับการระบุอยู่บนรายการโมดูลในกระบวนการ

พื้นที่ผู้ใช้ของ watchOS 8 (2564), พื้นที่เคอร์เนล และการจัดเก็บกุญแจอย่างปลอดภัยกำลังอยู่ระหว่างการทดสอบในห้องปฏิบัติการ รายการจะได้รับการระบุอยู่บนรายการการปรับใช้อยู่ระหว่างการทดสอบ

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** watchOS 8 **สภาพแวดล้อม:** Apple Silicon, ผู้ใช้, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** watchOS 8 **สภาพแวดล้อม:** Apple Silicon, เคอร์เนล, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ watchOS 8 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (S3, S4, S5, S6) **ระดับความปลอดภัยโดยรวม:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2564 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v12 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ watchOS 8 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (S6) **ระดับความปลอดภัยโดยรวม:** 2 **ระดับความปลอดภัยทางกายภาพ:** 3
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** watchOS 7 **สภาพแวดล้อม:** Apple Silicon, ผู้ใช้, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** watchOS 7 **สภาพแวดล้อม:** Apple Silicon, เคอร์เนล, ซอฟต์แวร์ **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัยโดยรวม:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ watchOS 7 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (S3, S4, S5, S6) **ระดับความปลอดภัยโดยรวม:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2563 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Apple Corecrypto Module v11.1 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ watchOS 7 **สภาพแวดล้อม:** Apple Silicon, การจัดเก็บกุญแจอย่างปลอดภัย, ฮาร์ดแวร์ **ประเภท:** ฮาร์ดแวร์ (S6) **ระดับความปลอดภัยโดยรวม:** 2 **ระดับความปลอดภัยทางกายภาพ:** 3

การรับรอง FIPS 140-2

ตารางด้านล่างจะแสดงโมดูลการเข้ารหัสที่อยู่ในระหว่างการทดสอบในตอนนี้และได้รับการทดสอบแล้วในด้านความสอดคล้องกับ FIPS 140-2 ในห้องปฏิบัติการ

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** 3856 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v10.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** watchOS 6 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** —	**การรับรอง:** 3855 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v10.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** watchOS 6 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1

วันที่	การรับรอง / เอกสาร	ข้อมูลโมดูล
วันที่เปิดตัวระบบปฏิบัติการ: 2562 **วันที่ตรวจสอบความถูกต้อง:** 5 กุมภาพันธ์ 2564	**การรับรอง:** 3811 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v10.0 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ watchOS 6 **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 23 เมษายน 2562	**การรับรอง:** 3438 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v9.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** watchOS 5 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 11 เมษายน 2562	**การรับรอง:** 3433 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v9.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** watchOS 5 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2561 **วันที่ตรวจสอบความถูกต้อง:** 10 กันยายน 2562	**การรับรอง:** 3523 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v9.0 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ watchOS 5 **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 9/3/2561, 22/5/2561, 6/7/2561	**การรับรอง:** 3148 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto User Module v8.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** watchOS 4 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 9/3/2561, 17/5/2561, 3/7/2561	**การรับรอง:** 3147 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** Corecrypto Kernel Module v8.0 ของ Apple สำหรับ ARM **ระบบปฏิบัติการ:** watchOS 4 **ประเภท:** ซอฟต์แวร์ **ระดับความปลอดภัย:** 1
วันที่เปิดตัวระบบปฏิบัติการ: 2560 **วันที่ตรวจสอบความถูกต้อง:** 10 กันยายน 2562	**การรับรอง:** 3223 **เอกสาร:** การรับรอง นโยบายความปลอดภัย แนวทางเจ้าหน้าที่เข้ารหัส	**ชื่อเรื่อง:** โมดูลการเข้ารหัสการจัดเก็บกุญแจอย่างปลอดภัยของ Apple v1.0 **ระบบปฏิบัติการ:** sepOS ที่เผยแพร่พร้อมกับ watchOS 4 **ประเภท:** ฮาร์ดแวร์ **ระดับความปลอดภัย:** 2

การรับรองความปลอดภัยด้านซอฟต์แวร์

ภาพรวมการรับรองความปลอดภัยด้านซอฟต์แวร์ของ Apple

Apple มีการรับรองการตรวจสอบความถูกต้องด้านความสอดคล้องกับมาตรฐานการประมวลผลข้อมูลสหรัฐอเมริกากลาง (FIPS) 140-2/-3 สำหรับ sepOS และเฟิร์มแวร์ T2 รวมถึงการรับรองอื่นๆ ด้วย Apple เริ่มต้นจาก**โครงสร้างการรับรอง**ที่สามารถปรับใช้ได้ในวงกว้างกับแพลตฟอร์มที่หลากหลายตามความเหมาะสม หนึ่งในโครงสร้างดังกล่าวคือการตรวจสอบความถูกต้องของ corecrypto ที่ใช้ในการปรับใช้โมดูลการเข้ารหัสของซอฟต์แวร์และฮาร์ดแวร์ภายในระบบปฏิบัติการที่พัฒนาโดย Apple โครงสร้างที่สองคือการรับรอง Secure Enclave ซึ่งฝังอยู่ในอุปกรณ์ Apple หลายๆ รุ่น โครงสร้างที่สามคือการรับรอง Secure Element (SE) ที่พบได้ในอุปกรณ์ Apple ทุกเครื่องที่มี Touch ID และอุปกรณ์ที่มี Face ID โครงสร้างการรับรองฮาร์ดแวร์เหล่านี้สร้างรากฐานสำหรับการรับรองความปลอดภัยของแพลตฟอร์มที่กว้างขึ้น

การรับรองผลิตภัณฑ์: (เกณฑ์ทั่วไป ISO/IEC 15408)

เกณฑ์ทั่วไป (ISO/IEC 15408) เป็นมาตรฐานที่หลายองค์กรใช้เป็นพื้นฐานในการดำเนินการประเมินความปลอดภัยของผลิตภัณฑ์ IT

สำหรับการรับรองที่อาจรู้จักกันในชื่อการจัดการรับรองเกณฑ์ทั่วไป (CCRA) ระดับสากล ให้ดูที่พอร์ทัลเกณฑ์ทั่วไป มาตรฐานเกณฑ์ทั่วไปยังอาจมีการใช้ภายนอก CCRA โดยแบบแผนการตรวจสอบความถูกต้องระดับชาติและระดับส่วนตัวอีกด้วย ในยุโรป การยอมรับร่วมกันอยู่ภายใต้ข้อตกลง SOG-IS เช่นเดียวกันกับ CCRA

เป้าหมายก็เพื่อให้ชุดมาตรฐานความปลอดภัยที่ผ่านการรับรองในระดับสากลสามารถประเมินความสามารถด้านการรักษาความปลอดภัยของผลิตภัณฑ์เทคโนโลยีสารสนเทศได้อย่างชัดเจนและน่าเชื่อถือ ซึ่งเป็นเป้าหมายที่ชุมชนเกณฑ์ทั่วไประบุไว้ เมื่อจัดให้มีการประเมินแบบอิสระเกี่ยวกับความสามารถของผลิตภัณฑ์ในการปฏิบัติตามมาตรฐานด้านความปลอดภัย การรับรองเกณฑ์ทั่วไปจึงทำให้ลูกค้ามีความมั่นใจมากขึ้นเกี่ยวกับความปลอดภัยของผลิตภัณฑ์เทคโนโลยีสารสนเทศและตัดสินใจได้อย่างรอบคอบมากขึ้น

ประเทศสมาชิกได้ตกลงที่จะยอมรับการรับรองผลิตภัณฑ์เทคโนโลยีสารสนเทศด้วยความเชื่อมั่นในระดับเดียวกันผ่าน CCRA การประเมินที่จำเป็นก่อนการรับรองจะครอบคลุมและรวมถึง:

- โปรไฟล์การปกป้อง (PP)
- เป้าหมายความปลอดภัย (ST)
- ข้อกำหนดฟังก์ชั่นความปลอดภัย (SFR)
- ข้อกำหนดการรับประกันความปลอดภัย (SAR)
- ระดับการรับประกันการประเมิน (EAL)

โปรไฟล์การปกป้อง (PP) เป็นเอกสารที่ระบุข้อกำหนดด้านความปลอดภัยสำหรับคลาสของประเภทอุปกรณ์ (เช่น อุปกรณ์เคลื่อนที่) ซึ่งใช้สำหรับแสดงการเปรียบเทียบระหว่างการประเมินของผลิตภัณฑ์ IT ภายในคลาสเดียวกัน การเป็นสมาชิกของ CCRA รวมถึงการเพิ่มขึ้นของ PP ที่ได้รับการรับรองมีการเพิ่มขึ้นทุกปีอย่างต่อเนื่อง การทำความตกลงนี้อนุญาตให้นักพัฒนาผลิตภัณฑ์ใช้การรับรองเดียวภายใต้แบบแผนการอนุญาตการรับรองแบบใดแบบหนึ่งและกำหนดให้ได้รับการยอมรับจากผู้ลงนามทุกๆ คนที่ใช้การรับรอง

เป้าหมายความปลอดภัย (ST) กำหนดว่า**อะไรบ้าง**ที่จะได้รับการประเมินเมื่อผลิตภัณฑ์ IT ได้รับการรับรอง ST หมายถึง**ข้อกำหนดฟังก์ชั่นความปลอดภัย (SFR)** ที่เฉพาะเจาะจงยิ่งขึ้น ซึ่งใช้สำหรับการประเมิน ST อย่างละเอียดยิ่งขึ้น

เกณฑ์ทั่วไป (CC) ยังรวมถึง**ข้อกำหนดการรับประกันความปลอดภัย**อีกด้วย ตัววัดหนึ่งที่มักถูกระบุอยู่เป็นประจำก็คือ**ระดับการรับประกันการประเมิน (EAL)** โดย EAL จะรวมกลุ่มชุดของ SAR ที่เกิดขึ้นบ่อยครั้งเข้าด้วยกันและอาจถูกระบุอยู่ใน PP และ ST เพื่อรองรับการเปรียบเทียบ

PP ก่อนหน้านี้จำนวนมากถูกเก็บถาวรและแทนที่ด้วย PP แบบมุ่งเป้าซึ่งได้รับการพัฒนาและมุ่งเน้นโซลูชั่นและสภาพแวดล้อมที่เฉพาะเจาะจง ในความพยายามจากหลายฝ่ายที่จะให้มีการยอมรับร่วมกันระหว่างสมาชิก CCRA ทั้งหมดต่อไป ชุมชนเทคนิคสากล (iTC) ได้ถูกจัดตั้งขึ้นเพื่อพัฒนาและรักษาไว้ซึ่งโปรไฟล์การปกป้องเชิงร่วมมือ (cPP) ซึ่งมีการพัฒนาตั้งแต่เริ่มต้นโดยมีแผนของผู้ลงนาม CCRA ร่วมด้วย PP แบบมุ่งเป้าสำหรับกลุ่มผู้ใช้และการจัดการการยอมรับร่วมกันที่นอกเหนือจาก CCRA จะได้รับการพัฒนาต่อไปโดยผู้ที่ได้รับประโยชน์ร่วมกันที่เหมาะสม

Apple เริ่มใช้การรับรองภายใต้ CCRA ที่ได้รับการอัปเดตกับ cPP ที่เลือกตั้งแต่ต้นปี 2558 ตั้งแต่นั้นมา Apple ก็ได้รับการรับรองเกณฑ์ทั่วไปสำหรับการเปิดตัว iOS ครั้งใหญ่ในแต่ละครั้งและได้ขยายความครอบคลุมให้รวมถึงการรับประกันความปลอดภัยที่ได้จาก PP ใหม่

Apple มีบทบาทเชิงรุกในชุมชนเทคนิคที่มุ่งเน้นการประเมินเทคโนโลยีความปลอดภัยของอุปกรณ์เคลื่อนที่ ซึ่งรวมถึง iTC ที่รับผิดชอบในการพัฒนาและอัปเดต cPP Apple ยังคงประเมินและใช้การรับรองกับ PP และ cPP ที่มีอยู่ในปัจจุบันอย่างต่อเนื่อง

การรองรับแพลตฟอร์ม Apple สำหรับตลาดอเมริกาเหนือปกติแล้วจะดำเนินการโดยความร่วมมือในการรับประกันข้อมูลแห่งชาติ (NIAP) ที่เก็บบันทึกรายการโปรเจ็กต์ที่อยู่ระหว่างการประเมินแต่ยังไม่ได้รับรอง

นอกเหนือจากใบรับรองแพลตฟอร์มทั่วไปแล้ว ยังมีการออกใบรับรองอื่นๆ เพื่อแสดงข้อกำหนดด้านความปลอดภัยที่เฉพาะเจาะจงสำหรับตลาดบางแห่งอีกด้วย

การรับรองความปลอดภัยสำหรับแอปของ Apple

ความเป็นมาของการรับรองแอปของ Apple

Apple ได้เข้าไปมีส่วนร่วมเชิงรุกในการรับรองความปลอดภัยสำหรับแอปของ Apple โดยใช้โปรไฟล์การปกป้อง (PP) เกณฑ์ทั่วไปที่เหมาะสม การประเมินเหล่านี้ดำเนินการบนการรับรองฮาร์ดแวร์และระบบปฏิบัติการที่ Apple ได้รับ

ในปี 2561 Apple ได้เริ่มต้นการประเมินความปลอดภัยแอปพลิเคชันสำหรับแอปพลิเคชันที่สำคัญซึ่งทำงานบน iOS 11 กับเบราว์เซอร์ Safari และแอปรายชื่อ Apple ยังคงใช้งานการประเมินเหล่านี้ต่อบนแอปที่ทำงานบน iOS 12, iOS 13 และ iPadOS 13.1 ในปี 2564 จะมีการเพิ่มความครอบคลุมสำหรับแอปที่ใช้งาน macOS 11 สถานะการรับรองโมดูลการเข้ารหัส

แอปของ Apple ที่แสดงรายการที่นี่จะใช้โมดูลการเข้ารหัสสำหรับระบบปฏิบัติการที่สามารถใช้ได้ โปรดดูที่ การรับรองความปลอดภัยสำหรับ iOS, การรับรองความปลอดภัยสำหรับ iPadOS และ การรับรองความปลอดภัยสำหรับ macOS สำหรับข้อมูลเพิ่มเติม

สถานะการรับรองเกณฑ์ทั่วไป (CC)

แบบแผนของสหรัฐอเมริกาที่ดำเนินการโดย NIAP จะเก็บรักษารายการของผลิตภัณฑ์ในการประเมิน ซึ่งรายการนี้จะประกอบไปด้วยผลิตภัณฑ์ที่อยู่ระหว่างการประเมินกับห้องปฏิบัติการการทดสอบเกณฑ์ทั่วไป (CCTL) ที่ได้รับการรับรองจาก NIAP ในสหรัฐอเมริกาและผลิตภัณฑ์ที่ผ่านการประชุมเริ่มงานการประเมิน (หรือเทียบเท่า) ซึ่งผู้บริหารของ CCEVS ได้ยอมรับผลิตภัณฑ์เข้าสู่การประเมินอย่างเป็นทางการแล้ว

หลังผลิตภัณฑ์ได้รับการรับรองแล้ว NIAP ใส่การรับรองที่สามารถใช้งานได้ในตอนนี้ไว้บนรายการข้อร้องเรียนผลิตภัณฑ์ขององค์กร การรับรองเหล่านี้จะถูกตรวจสอบด้านความสอดคล้องกับนโยบายการรับประกันการซ่อมในปัจจุบันหลังจาก 2 ปี หลังจากวันรับประกันการซ่อมหมดอายุแล้ว NIAP จะย้ายการแสดงการรับรองไปยังรายการผลิตภัณฑ์ที่ถูกเก็บถาวรขององค์กร

พอร์ทัลเกณฑ์ทั่วไปจะแสดงการรับรองที่สามารถยอมรับร่วมกันได้ภายใต้การจัดการรับรองเกณฑ์ทั่วไป (CCRA) พอร์ทัล CC อาจเก็บผลิตภัณฑ์ไว้บนรายการผลิตภัณฑ์ที่ได้รับการรับรองเป็นเวลา 5 ปี โดยการบันทึกจะถูกเก็บไว้โดยพอร์ทัล CC สำหรับการรับรองที่ถูกเก็บถาวร

ตารางด้านล่างจะแสดงการรับรองที่อยู่ในระหว่างการประเมินในห้องปฏิบัติการในตอนนี้ หรือการรับรองที่ได้รับการรับรองแล้วว่าสอดคล้องกับเกณฑ์ทั่วไป

สถานะปัจจุบัน

- การประเมินกับ NIAP ที่มีการเผยแพร่ว่ากำลังอยู่ในระหว่างการประเมินจะแสดงอยู่บนผลิตภัณฑ์ในการประเมิน (NIAP)
- การประเมินที่ดำเนินการเสร็จและตรวจสอบความถูกต้องแล้วจะระบุอยู่ในรายการข้อร้องเรียนผลิตภัณฑ์ NIAP

ระบบปฏิบัติการ / วันที่ออกการรับรอง	ID แบบแผน / เอกสาร	ชื่อเรื่อง / โปรไฟล์การปกป้อง
ระบบปฏิบัติการ: macOS 11 Big Sur **วันที่ออกการรับรอง:** —	**ID แบบแผน:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** macOS 11 Big Sur: รายชื่อ **โปรไฟล์การปกป้อง:** PP สำหรับ SW แอปพลิเคชัน, EP สำหรับเว็บเบราว์เซอร์
ระบบปฏิบัติการ: macOS 11 Big Sur **วันที่ออกการรับรอง:** —	**ID แบบแผน:** ยังไม่ได้รับรอง **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** macOS 11 Big Sur: Safari **โปรไฟล์การปกป้อง:** PP สำหรับ SW แอปพลิเคชัน, EP สำหรับเว็บเบราว์เซอร์
ระบบปฏิบัติการ: iOS 14, iPadOS 14 **วันที่ออกการรับรอง:** 20 สิงหาคม 2564	**ID แบบแผน:** 11191 **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** iOS 14 และ iPadOS 14 ของ Apple: รายชื่อ **โปรไฟล์การปกป้อง:** PP สำหรับ SW แอปพลิเคชัน, EP สำหรับเว็บเบราว์เซอร์
ระบบปฏิบัติการ: iOS 14, iPadOS 14 **วันที่ออกการรับรอง:** —	**ID แบบแผน:** 11192 **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** iOS 14 และ iPadOS 14 ของ Apple: Safari **โปรไฟล์การปกป้อง:** PP สำหรับ SW แอปพลิเคชัน, EP สำหรับเว็บเบราว์เซอร์

ระบบปฏิบัติการ / วันที่ออกการรับรอง	ID แบบแผน / เอกสาร	ชื่อเรื่อง / โปรไฟล์การปกป้อง
ระบบปฏิบัติการ: iOS 13, iPadOS 13 **วันที่ออกการรับรอง:** 5 มิถุนายน 2563	**ID แบบแผน:** 11060 **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** iOS 13 และ iPadOS 13 ของ Apple: Safari **โปรไฟล์การปกป้อง:** PP สำหรับ SW แอปพลิเคชัน, EP สำหรับเว็บเบราว์เซอร์
ระบบปฏิบัติการ: iOS 13, iPadOS 13 **วันที่ออกการรับรอง:** 5 มิถุนายน 2563	**ID แบบแผน:** 11050 **เอกสาร:** การรับรอง เป้าหมายความปลอดภัย แนวทาง รายงานการตรวจสอบความถูกต้อง รายงานกิจกรรมการรับประกัน	**ชื่อเรื่อง:** iOS 13 และ iPadOS 13 ของ Apple: รายชื่อ **โปรไฟล์การปกป้อง:** PP สำหรับ SW แอปพลิเคชัน

การรับรองเกณฑ์ทั่วไปที่ถูกเก็บถาวรสำหรับแอปของ Apple

ระบบปฏิบัติการ / วันที่ออกการรับรอง	ID แบบแผน / เอกสาร	ชื่อเรื่อง / โปรไฟล์การปกป้อง
ระบบปฏิบัติการ: iOS 12 **วันที่ออกการรับรอง:** 12 มิถุนายน 2562	**ID แบบแผน:** 10960 **เอกสาร:** เป้าหมายความปลอดภัย แนวทาง	**ชื่อเรื่อง:** Safari iOS 12 **โปรไฟล์การปกป้อง:** PP สำหรับ SW แอปพลิเคชัน, EP สำหรับเว็บเบราว์เซอร์
ระบบปฏิบัติการ: iOS 12 **วันที่ออกการรับรอง:** 28 กุมภาพันธ์ 2562	**ID แบบแผน:** 10961 **เอกสาร:** เป้าหมายความปลอดภัย แนวทาง	**ชื่อเรื่อง:** รายชื่อ iOS 12 **โปรไฟล์การปกป้อง:** PP สำหรับ SW แอปพลิเคชัน
ระบบปฏิบัติการ: iOS 11 **วันที่ออกการรับรอง:** 9 พฤศจิกายน 2561	**ID แบบแผน:** 10916 **เอกสาร:** เป้าหมายความปลอดภัย แนวทาง	**ชื่อเรื่อง:** Safari iOS 11 **โปรไฟล์การปกป้อง:** PP สำหรับ SW แอปพลิเคชัน, EP สำหรับเว็บเบราว์เซอร์
ระบบปฏิบัติการ: iOS 11 **วันที่ออกการรับรอง:** 13 กันยายน 2561	**ID แบบแผน:** 10915 **เอกสาร:** เป้าหมายความปลอดภัย แนวทาง	**ชื่อเรื่อง:** รายชื่อ iOS 11 **โปรไฟล์การปกป้อง:** PP สำหรับ SW แอปพลิเคชัน

การรับรองความปลอดภัยสำหรับบริการอินเทอร์เน็ตของ Apple

Apple ยังคงดำเนินการรับรองที่เป็นไปตามกฎเกณฑ์ของมาตรฐาน ISO/IEC 27001 และ ISO/IEC 27018 เพื่อให้ลูกค้าของ Apple สามารถจัดการกับข้อผูกพันตามระเบียบข้อบังคับและตามสัญญาของตนได้ การรับรองเหล่านี้ช่วยให้ลูกค้าของเราสามารถพิสูจน์ยืนยันได้อย่างอิสระเกี่ยวกับวิธีปฏิบัติของ Apple ด้านความปลอดภัยและความเป็นส่วนตัวของข้อมูลสำหรับระบบในขอบเขต

ISO/IEC 27001 และ ISO/IEC 27018 เป็นส่วนหนึ่งของกลุ่มมาตรฐานระบบการจัดการความปลอดภัยของข้อมูล (ISMS) ที่เผยแพร่โดยองค์การระหว่างประเทศว่าด้วยการมาตรฐาน (ISO) ในฐานะที่เป็นส่วนหนึ่งของ ISMS ของ Apple ข้อกำหนดการควบคุม Annex A ทั้งหมดถูกรวมอยู่ในแถลงการณ์การนำมาใช้งานตามที่กำหนดไว้ในมาตรฐาน ISO/IEC 27001 และ ISO/IEC 27018 Apple ดำเนินการพิสูจน์ยืนยันอิสระโดยผู้ให้บริการจดทะเบียนที่ได้รับการรับรองเป็นรายปี

ISO/IEC 27001

ISO/IEC 27001 คือมาตรฐานระบบการจัดการความปลอดภัยของข้อมูลที่กำหนดข้อกำหนดสำหรับการจัดตั้ง การปรับใช้ การรักษา และการปรับปรุงระบบการจัดการความปลอดภัยของข้อมูลขององค์กรอย่างต่อเนื่อง มาตรฐาน ISO/IEC 27001 ประกอบด้วยโดเมนความปลอดภัยที่การรับรอง ISO/IEC ของ Apple ครอบคลุมดังต่อไปนี้:

- นโยบายความปลอดภัยของข้อมูล
- การจัดการความปลอดภัยของข้อมูล
- การจัดการสินทรัพย์
- ความปลอดภัยด้านทรัพยากรบุคคล
- ความปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
- การจัดการการสื่อสารและการดำเนินการ
- การควบคุมการเข้าถึง
- การจัดหา การพัฒนา และการบำรุงรักษาระบบข้อมูล
- การจัดการเหตุการณ์ความปลอดภัยของข้อมูล
- การจัดการความต่อเนื่องของธุรกิจ
- การปฏิบัติตามกฎเกณฑ์

ISO/IEC 27018

ISO/IEC 27018 เป็นหลักการปฏิบัติสำหรับการปกป้องข้อมูลที่สามารถระบุตัวบุคคลได้ (PII) ในสภาพแวดล้อมคลาวด์สาธารณะ มาตรฐาน ISO/IEC 27018 ประกอบด้วยโดเมนความปลอดภัยที่การรับรอง ISO/IEC ของ Apple ครอบคลุมดังต่อไปนี้:

- ความยินยอมและทางเลือก
- ความถูกต้องและข้อกำหนดของวัตถุประสงค์
- ข้อจำกัดในการรวบรวมข้อมูล
- การเก็บและใช้ข้อมูลเท่าที่จำเป็น
- ข้อจำกัดในการใช้ การเก็บรักษา และการเปิดเผย
- ความแม่นยำและคุณภาพ
- ความตรงไปตรงมา ความโปร่งใส และการแจ้งให้ทราบ
- การมีส่วนร่วมและการเข้าถึงตัวบุคคล
- ภาระรับผิดชอบ
- ความปลอดภัยของข้อมูล
- การปฏิบัติตามกฎเกณฑ์ความเป็นส่วนตัว

ISO/IEC 27001 และ ISO/IEC 27018 ครอบคลุมถึงบริการต่างๆ ของ Apple

การรับรอง ISO/IEC 27001 และ ISO/IEC 27018 ของ Apple จะครอบคลุมถึงบริการต่อไปนี้:

- การสนทนาทางธุรกิจของ Apple
- Apple Business Manager
- บริการการแจ้งผลักข้อมูลของ Apple (APNs)
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- iTunes
- บริการ iWork
- Apple ID ที่มีการจัดการ
- แอปงานชั้นเรียน
- Siri

การรับรอง

สามารถดูหลักฐานการรับรอง ISO/IEC 27001 และ 27018 ของ Apple ได้ที่ผู้ให้บริการจดทะเบียนของเรา:

ในการดูการรับรองของ Apple ให้ไปที่การค้นหาการรับรองและไคลเอ็นต์ไดเรกทอรีบนเว็บไซต์สถาบันมาตรฐานอังกฤษ (BSI) ป้อน Apple ในช่องการค้นหาบริษัท คลิกปุ่มค้นหา จากนั้นเลือกผลลัพธ์การค้นหาเพื่อดูการรับรอง

หมายเหตุ: ข้อมูลเกี่ยวกับผลิตภัณฑ์ที่ไม่ได้ผลิตโดย Apple หรือเว็บไซต์อิสระที่ไม่ได้ถูกควบคุมหรือทดสอบโดย Apple นั้นเป็นการนำเสนอที่ไม่ได้เป็นการแนะนำหรือการรับรองใดๆ Apple ไม่ขอรับผิดชอบใดๆ ในส่วนที่เกี่ยวกับการเลือก ประสิทธิภาพ หรือการใช้งานเว็บไซต์หรือผลิตภัณฑ์ของบริษัทอื่น Apple ไม่ได้รับรองความถูกต้องและความเชื่อถือได้ของข้อมูลของเว็บไซต์ของบริษัทอื่น ติดต่อผู้จำหน่ายเพื่อรับข้อมูลเพิ่มเติม

โปรเจ็กต์การปฏิบัติตามกฎเกณฑ์ความปลอดภัยของ macOS

โปรเจ็กต์การปฏิบัติตามกฎเกณฑ์ความปลอดภัยของ macOS (mSCP) คือความพยายามแบบโอเพนซอร์ส ในการมอบแนวทางเชิงโปรแกรมในการสร้างแนวทางด้านความปลอดภัย โปรเจ็กต์นี้เป็นโปรเจ็กต์ร่วมกันระหว่างเจ้าหน้าที่ความปลอดภัยด้าน IT ระดับปฏิบัติการสังกัดรัฐบาลกลางจากสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST), องค์การบริหารการบินและอวกาศแห่งชาติ (NASA), สำนักงานด้านระบบข้อมูลกลาโหม (DISA) และห้องปฏิบัติการระดับชาติ ลอส อลาโมส (LANL) โปรเจ็กต์ใช้ชุดการควบคุม macOS ที่ผ่านการทดสอบและตรวจสอบความถูกต้องแล้วและจับคู่ชุดการควบคุมเหล่านี้กับคู่มือความปลอดภัยที่โปรเจ็กต์รองรับ นอกจากนี้แล้ว โปรเจ็กต์นี้ยังสามารถใช้เป็นแหล่งข้อมูลสำหรับสร้างพื้นฐานการควบคุมความปลอดภัยแบบกำหนดเองสำหรับการควบคุมความปลอดภัยด้านเทคนิคอย่างง่ายดายด้วยการใช้คลังของการทำงานเชิงอะตอมที่ได้รับการทดสอบและตรวจสอบความถูกต้องแล้วได้อีกด้วย (การตั้งค่าการกำหนดค่า) โปรเจ็กต์นี้จะส่งออกเอกสาร สคริปต์ โปรไฟล์การกำหนดค่า และเช็คลิสต์การตรวจสอบแบบกำหนดเองที่อิงตามพื้นฐานที่ใช้

mSCP สามารถสร้างเนื้อหาข้อมูลออกสำหรับใช้ร่วมกับเครื่องมือการจัดการและเครื่องมือความปลอดภัยเพื่อให้ปฏิบัติตามกฎเกณฑ์ได้สำเร็จ การตั้งค่าการกำหนดค่าในโปรเจ็กต์นี้จะรองรับพื้นฐานแนวทางต่างๆ ดังต่อไปนี้:

องค์กร	พื้นฐานที่รองรับ
การตีพิมพ์พิเศษ (SP) 800-53 ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) เป็นการควบคุมความปลอดภัยที่แนะนำสำหรับระบบข้อมูลรัฐบาลกลางและองค์กร, แก้ไขครั้งที่ 5	800-53 สูง, 800-53 ปานกลาง, 800-53 ต่ำ
การตีพิมพ์พิเศษ (SP) 800-171 ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) เป็นการปกป้องข้อมูลที่ไม่จัดเป็นความลับที่มีการควบคุมในระบบซึ่งไม่ได้เป็นของรัฐบาลกลางหรือองค์กร, แก้ไขครั้งที่ 2	800-171
macOS 11 STIG ของสำนักงานด้านระบบข้อมูลกลาโหม (DISA), คู่มือการปรับใช้ทางเทคนิคด้านความปลอดภัยของ Apple macOS 11	STIG
ขั้นตอนของคณะกรรมการระบบความปลอดภัยแห่งชาติ (CNSSI) 1253 เป็นการจัดประเภทความปลอดภัยและการเลือกการควบคุมสำหรับระบบความปลอดภัยแห่งชาติ	1253

ข้อมูลเพิ่มเติม:

- พื้นฐานสำหรับทบทวนกฎเกณฑ์ทั้งหมดในโปรเจ็กต์สามารถดูได้ที่นี่
- ในการเรียนรู้เพิ่มเติมเกี่ยวกับโปรเจ็กต์และการใช้งาน ให้ดูที่ wiki โปรเจ็กต์การปฏิบัติตามกฎเกณฑ์ความปลอดภัยของ macOS
- ในการตั้งค่าโปรเจ็กต์สำหรับการใช้งาน ให้ดูที่: การทำความรู้จักกับโปรเจ็กต์การปฏิบัติตามกฎเกณฑ์ความปลอดภัยของ macOS ตอนที่ 1 และการทำความรู้จักกับโปรเจ็กต์การปฏิบัติตามกฎเกณฑ์ความปลอดภัยของ macOS ตอนที่ 2
- ถ้าคุณสนใจที่จะสนับสนุนการพัฒนาโปรเจ็กต์นี้ ให้ดูที่ แนวทางผู้ร่วมสนับสนุน

ประวัติการแก้ไขเอกสาร

วันที่	เนื้อหาสรุป
27 ตุลาคม 2564	หัวข้อที่อัปเดต: • การรับรองความปลอดภัยสำหรับหน่วยประมวลผล Secure Enclave • การรับรองความปลอดภัยสำหรับ iOS • การรับรองความปลอดภัยสำหรับ macOS
17 สิงหาคม 2564	หัวข้อที่อัปเดต: • การรับรองความปลอดภัยสำหรับหน่วยประมวลผล Secure Enclave • การรับรองความปลอดภัยสำหรับชิป Apple T2 Security • การรับรองความปลอดภัยสำหรับ iOS • การรับรองความปลอดภัยสำหรับ iPadOS • การรับรองความปลอดภัยสำหรับ macOS • การรับรองความปลอดภัยสำหรับ tvOS • การรับรองความปลอดภัยสำหรับ watchOS • การรับรองความปลอดภัยสำหรับแอปของ Apple • การรับรองความปลอดภัย • โปรเจ็กต์การปฏิบัติตามกฎเกณฑ์ความปลอดภัยของ macOS
26 เมษายน 2564	หัวข้อที่เพิ่ม: • โปรเจ็กต์การปฏิบัติตามกฎเกณฑ์ความปลอดภัยของ macOS หัวข้อที่อัปเดต: • การรับรองความปลอดภัยสำหรับชิป Apple T2 Security: การรับรอง FIPS 140-2 ใหม่ เลขที่ 3811 • การรับรองความปลอดภัยสำหรับหน่วยประมวลผล Secure Enclave: การรับรอง FIPS 140-2 ใหม่ เลขที่ 3811 และตารางใหม่สำหรับการรับรองเพิ่มเติม • การรับรองความปลอดภัยสำหรับ iOS: การรับรอง FIPS 140-2 ใหม่ เลขที่ 3811, ID แบบแผน 11146 ของ iOS 14 อยู่ในการประเมิน • การรับรองความปลอดภัยสำหรับ iPadOS: การรับรอง FIPS 140-2 ใหม่ เลขที่ 3811, ID แบบแผน 11147 ของ iPadOS 14 อยู่ในการประเมิน • การรับรองความปลอดภัยสำหรับ macOS: การรับรอง FIPS 140-2 ใหม่ เลขที่ 3811 • การรับรองความปลอดภัยสำหรับ tvOS: การรับรอง FIPS 140-2 ใหม่ เลขที่ 3811 • การรับรองความปลอดภัยสำหรับ watchOS: การรับรอง FIPS 140-2 ใหม่ เลขที่ 3811 • การรับรองความปลอดภัยสำหรับแอปของ Apple: รายการอัปเดตสำหรับสถานะเกณฑ์ทั่วไป และตารางใหม่สำหรับการรับรองเกณฑ์ทั่วไปที่ถูกเก็บถาวร

อภิธานศัพท์

การเข้ารหัสดิสก์แบบเต็มรูปแบบ (FDE) การเข้ารหัสข้อมูลทั้งหมดบนดิสก์โวลุ่มการจัดเก็บข้อมูล

การจัดการรับรองเกณฑ์ทั่วไป (CCRA) การจัดการการยอมรับร่วมกันที่วางรากฐานนโยบายและข้อกำหนดสำหรับการยอมรับใบรับรองที่ออกโดยสอดคล้องกับซีรีส์ ISO/IEC 15408 หรือมาตรฐานเกณฑ์ทั่วไปในระดับสากล

การปรับใช้อยู่ระหว่างการทดสอบ (IUT) โมดูลการเข้ารหัสที่อยู่ในระหว่างการทดสอบในห้องปฏิบัติการ

การรักษาความปลอดภัยระบบข้อมูลกลุ่มเจ้าหน้าที่อาวุโส (SOG-IS) กลุ่มที่จัดการข้อตกลงการยอมรับร่วมกันระหว่างหลายประเทศในทวีปยุโรป

เกณฑ์ทั่วไป (CC) มาตรฐานที่วางรากฐานให้กับแนวคิดและหลักการทั่วไปของการประเมินความปลอดภัยด้าน IT และระบุโมเดลทั่วไปสำหรับการประเมิน และมีแค็ตตาล็อกของข้อกำหนดความปลอดภัยในภาษาที่เป็นมาตรฐานด้วย

ความร่วมมือในการรับประกันข้อมูลแห่งชาติ (NIAP) องค์กรของรัฐบาลสหรัฐอเมริกาที่ทำหน้าที่ในการดำเนินการปรับใช้มาตรฐานเกณฑ์ทั่วไปและจัดการแบบแผนการตรวจสอบความถูกต้องและการประเมินเกณฑ์ทั่วไป (CCEVS) ของ NIAP ในสหรัฐอเมริกา

ชุมชนเทคนิคสากล (iTC) กลุ่มที่มีหน้าที่ในการพัฒนาโปรไฟล์การปกป้องหรือโปรไฟล์การปกป้องเชิงร่วมมือภายใต้การสนับสนุนของการจัดการรับรองเกณฑ์ทั่วไป (CCRA)

แถลงการณ์การนำมาใช้งาน (SOA) เอกสารที่อธิบายเกี่ยวกับตัวควบคุมความปลอดภัยที่ปรับใช้ในขอบเขตของ ISMS ซึ่งจัดทำขึ้นเพื่อสนับสนุนการรับรอง ISO/IEC 27001

บริการการแจ้งผลักข้อมูลของ Apple (APNs) บริการของ Apple ที่ครอบคลุมทั่วโลก ซึ่งจะนำส่งการแจ้งเตือนแบบผลักข้อมูลไปที่อุปกรณ์ Apple

เป้าหมายความปลอดภัย (ST) เอกสารที่ระบุปัญหาด้านความปลอดภัยและข้อกำหนดความปลอดภัยสำหรับแต่ละผลิตภัณฑ์

โปรแกรมการตรวจสอบความถูกต้องโมดูลการเข้ารหัส (CMVP) องค์กรที่ดำเนินการโดยรัฐบาลสหรัฐอเมริกาและแคนาดาเพื่อตรวจสอบความถูกต้องของความสอดคล้องกับมาตรฐาน FIPS 140-3

โปรแกรมการตรวจสอบความถูกต้องอัลกอริทึมการเข้ารหัส (CAVP) องค์กรที่ดำเนินการโดย NIST ซึ่งจัดทำการทดสอบเพื่อตรวจสอบความถูกต้องของอัลกอริทึมการเข้ารหัสที่ได้รับการรับรอง (ตัวอย่างเช่น รับรองจาก FIPS และ แนะนำโดย NIST) และส่วนประกอบแต่ละส่วนของอัลกอริธึม

โปรไฟล์การปกป้อง (PP) เอกสารที่ระบุปัญหาด้านความปลอดภัยและข้อกำหนดความปลอดภัยสำหรับผลิตภัณฑ์แต่ละคลาส

โปรไฟล์การปกป้องเชิงร่วมมือ (cPP) โปรไฟล์การปกป้องที่ได้รับการพัฒนาโดยชุมชนเทคนิคสากลซึ่งเป็นกลุ่มของผู้เชี่ยวชาญที่ได้รับหน้าที่ในการสร้าง cPP

มาตรฐานการประมวลผลข้อมูลสหรัฐอเมริกากลาง (FIPS) การเผยแพร่ที่จัดทำโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ ไม่ว่าจะเป็นการเผยแพร่เมื่อมีการร้องขอตามกฎหมายหรือเมื่อมีการร้องขอซึ่งมีผลบังคับจากรัฐบาลกลางเพื่อความปลอดภัยทางไซเบอร์ หรือทั้งคู่

โมดูลการเข้ารหัส ฮาร์ดแวร์ ซอฟต์แวร์ และ/หรือเฟิร์มแวร์ที่มีฟังก์ชั่นการเข้ารหัสและตรงตามข้อกำหนดของมาตรฐานโมดูลการเข้ารหัสที่ได้กำหนดไว้

โมดูลในกระบวนการ (MIP) รายการที่เก็บรักษาโดยโปรแกรมการตรวจสอบความถูกต้องโมดูลการเข้ารหัส (CMVP) ของโมดูลการเข้ารหัสที่ปัจจุบันอยู่ในกระบวนการตรวจสอบความถูกต้องของ CMVP

ระดับความปลอดภัย (SL) ระดับความปลอดภัยโดยรวมสี่ระดับ (1–4) ซึ่งกำหนดไว้ใน ISO/IEC 19790 เพื่ออธิบายถึงชุดของข้อกำหนดความปลอดภัยที่ใช้ได้ ระดับที่ 4 คือระดับที่เข้มงวดที่สุด

ระบบการจัดการความปลอดภัยของข้อมูล (ISMS) ชุดของนโยบายความปลอดภัยของข้อมูลและขั้นตอนที่กำหนดกรอบของโปรแกรมความปลอดภัยที่ออกแบบมาเพื่อปกป้องขอบเขตของข้อมูลและระบบโดยการจัดการความปลอดภัยของข้อมูลอย่างเป็นระบบตลอดทั้งวงจรชีวิตของข้อมูลและ/หรือระบบ

ระบบบนชิป (SoC) วงจรรวม (IC) ที่รวมองค์ประกอบหลายส่วนไว้ในชิปชิ้นเดียว

ลูกข่าย VPN IPsec ลูกข่ายในโปรไฟล์การปกป้องที่มอบการเชื่อมต่อ Ipsec ที่ปลอดภัยระหว่างแพลตฟอร์มโฮสต์จริงหรือเสมือนและตำแหน่งที่ตั้งระยะไกล

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) ส่วนหนึ่งของกระทรวงพาณิชย์ของสหรัฐอเมริกาที่มีหน้าที่ในการพัฒนามาตรการทางด้านวิทยาศาสตร์ มาตรฐาน และเทคโนโลยี

หน่วยประมวลผล Secure Enclave (SEP) หน่วยประมวลผลร่วมที่สร้างขึ้นภายในระบบบนชิป (SoC)

Apple Business Manager พอร์ทัลบนเว็บที่เรียบง่ายสำหรับผู้ดูแลระบบ IT ซึ่งมอบวิธีที่รวดเร็วและมีประสิทธิภาพเพื่อให้องค์กรสามารถปรับใช้อุปกรณ์ของ Apple ที่ได้ซื้อจาก Apple โดยตรงหรือจากตัวแทนจำหน่ายที่ได้รับอนุญาตจาก Apple หรือผู้ให้บริการ องค์กรสามารถลงทะเบียนอุปกรณ์ในโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) โดยอัตโนมัติได้โดยไม่ต้องแตะหรือเตรียมอุปกรณ์ก่อนที่ผู้ใช้จะได้รับ

Apple School Manager พอร์ทัลบนเว็บที่เรียบง่ายสำหรับผู้ดูแลระบบ IT ซึ่งมอบวิธีที่รวดเร็วและมีประสิทธิภาพเพื่อให้องค์กรสามารถปรับใช้อุปกรณ์ของ Apple ที่ได้ซื้อจาก Apple โดยตรงหรือจากตัวแทนจำหน่ายที่ได้รับอนุญาตจาก Apple หรือผู้ให้บริการ องค์กรสามารถลงทะเบียนอุปกรณ์ในโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) โดยอัตโนมัติได้โดยไม่ต้องแตะหรือเตรียมอุปกรณ์ก่อนที่ผู้ใช้จะได้รับ

corecrypto คลังที่มีการปรับใช้ของการเข้ารหัสแบบดั้งเดิมในระดับต่ำ โปรดทราบว่า corecrypto จะไม่มีอินเทอร์เฟซการเขียนโปรแกรมสำหรับนักพัฒนาโดยตรงและจะถูกใช้งานผ่าน API ที่มีให้กับนักพัฒนา ซอร์สโค้ด corecrypto มีการเปิดเผยต่อสาธารณะเพื่อให้สามารถตรวจสอบความถูกต้องคุณสมบัติด้านความปลอดภัยและการทำงานที่ถูกต้องได้

Mobile Device Management (MDM) บริการที่ช่วยให้ผู้ใช้จัดการอุปกรณ์ที่ลงทะเบียนจากระยะไกล หลังจากลงทะเบียนอุปกรณ์แล้ว ผู้ใช้สามารถใช้บริการ MDM ผ่านเครือข่ายเพื่อกำหนดค่าการตั้งค่าและดำเนินการงานอื่นๆ บนอุปกรณ์โดยไม่ต้องโต้ตอบกับผู้ใช้ได้

Secure Element (SE) ชิปซิลิคอนที่ฝังอยู่ในอุปกรณ์หลายๆ รุ่นของ Apple ซึ่งรองรับฟังก์ชั่นต่างๆ เช่น Apple Pay

sepOS เฟิร์มแวร์ Secure Enclave ซึ่งอิงจากไมโครเคอร์เนล L4 เวอร์ชั่นที่ Apple กำหนดเอง

T2 ชิปความปลอดภัยของ Apple ที่มีอยู่ในคอมพิวเตอร์ Mac ที่ใช้ Intel บางรุ่นตั้งแต่ปี 2560

Apple Inc.

Apple
One Apple Park Way
Cupertino, CA 95014
สหรัฐฯ
apple.com

TH028-00499-B