

एफ.आई.पी.एस. (FIPS) 140-2 से एफ.आई.पी.एस FIPS 140-3 में माइग्रेशन पर परामर्श नोट

प्रस्तावना

यह दस्तावेज़ क्रिप्टोग्राफ़िक मॉड्यूलों और उनसे जुड़ी प्रणालियों को एफ.आई.पी.एस. (FIPS) 140-2 से एफ.आई.पी.एस. (FIPS) 140-3 में स्थानांतरित करने की संगठन-स्तरीय योजना और प्रमाणन प्राधिकारी की भूमिका को बताता है। इसका उद्देश्य नियमों का लगातार पालन सुनिश्चित करना, सुरक्षा स्तर बनाए रखना, कार्य में होने वाली बाधाओं को कम करना तथा क्रिप्टोग्राफ़िक नियंत्रणों को नवीन अंतरराष्ट्रीय मानकों (ISO/IEC 19790:2012 और ISO/IEC 24759:2017) के अनुरूप बनाना है।

एफ.आई.पी.एस. (FIPS) 140-2 के अंतर्गत किए गए सत्यापन (वैलिडेशन) अब चरणबद्ध रूप से समाप्त किए जा रहे हैं, और एफ.आई.पी.एस. (FIPS) 140-3 के अंतर्गत नए सत्यापन आवश्यक हैं। यह माइग्रेशन दस्तावेज़ कार्यक्षेत्र (स्कोप), शासन व्यवस्था, समय-सीमा तथा क्रियान्वयन के चरणों को परिभाषित करता है।

पृष्ठभूमि एवं प्रेरक तत्व

एफ.आई.पी.एस. (FIPS) 140-3, एफ.आई.पी.एस. (FIPS) 140-2 का स्थान ले चुका है और नए क्रिप्टोग्राफ़िक मॉड्यूल सत्यापनों के लिए अनिवार्य है।

एफ.आई.पी.एस. (FIPS) 140-3 की आवश्यकता क्यों ?

क्योंकि यह अंतरराष्ट्रीय ISO मानकों के अनुरूप है और अद्यतन आवश्यकताओं को प्रस्तुत करता है, जिससे निम्नलिखित के लिए सुरक्षा में वृद्धि होगी:-

- गैर-आक्रामक (नॉन-इनवेसिव) हमलों से सुरक्षा / उनके प्रभाव को कम करना।
- सॉफ़्टवेयर मॉड्यूल का सत्यापन।
- एंटीपी और यादृच्छिक बिट निर्माण।
- जीवनचक्र आश्वासन।
- अनुपालन और ऑडिट जोखिम में कमी।
- सुधारी गई क्रिप्टोग्राफ़िक आश्वासन और सहनशीलता, गैर-स्वामित्व वाले मानक।
- आधुनिक प्लेटफ़ॉर्म (कंटेनर, वर्चुअलाइजेशन) के साथ समन्वय।

यह दस्तावेज़ भारत में काम करने वाले सभी स्टेकहोल्डर्स, OEMs, डिस्ट्रीब्यूटर्स, वेंडर्स या किसी अन्य व्यक्ति/कंपनी संघ के लिए है, जिन्हें सलाह दी जा रही है कि वे 21 सितंबर 2026 से पहले सभी इन-स्कोप क्रिप्टोग्राफ़िक मॉड्यूल (क्रिप्टो टोकन, HSM, सिक्वोर एलिमेंट्स आदि) के लिए एफ.आई.पी.एस. (FIPS) 140-3 वैलिडेशन प्राप्त करें, ताकि क्रिप्टोग्राफी पर निर्भर उत्पादों और आंतरिक सिस्टम्स के लिए बाधा रहित सेवा सुनिश्चित की जा सके।

उद्देश्य

इस अभ्यास का उद्देश्य है कि 21 सितंबर 2029 तक उपयोग में आने वाले सभी गैर-अनुपालन या पुरानी क्रिप्टोग्राफ़िक घटकों (cryptographic components) को पूर्णतः सेवानिवृत्त या बदल दिया जाए, क्योंकि 21 सितंबर 2026 के बाद एफ.आई.पी.एस. (FIPS) 140-2 के लिए कोई और अपडेट उपलब्ध नहीं होंगे।

इसके अलावा, यह उद्देश्य भी है कि भविष्य के मानकों/अपडेट्स के लिए स्थायी क्रिप्टोग्राफ़िक गवर्नेंस स्थापित की जाए।

स्कोप

यह माइग्रेशन दस्तावेज़ प्रमाणन प्राधिकारी नियंत्रक कार्यालय (सी.सी.ए.) के अधिकार क्षेत्र के अंतर्गत संचालित पी.के.आई. इकोसिस्टम पर लागू होता है और इसमें निम्नलिखित शामिल हैं:-

- सभी सॉफ़्टवेयर, फर्मवेयर, हार्डवेयर, और हाइब्रिड क्रिप्टोग्राफ़िक मॉड्यूल।
- तीसरे पक्ष के उत्पाद और सेवाएँ जो एफ.आई.पी.एस. (FIPS) अनुपालन का दावा करती हैं।
- आंतरिक एप्लिकेशन, प्लेटफ़ॉर्म और इन्फ्रास्ट्रक्चर जो एफ.आई.पी.एस (FIPS)-वैध क्रिप्टोग्राफी पर निर्भर हैं।

यह सुनिश्चित करने के लिए कि स्टेकहोल्डर्स पहले एक सी.बी.ओ.एम. (CBOM) तैयार करें, ताकि विश्वसनीय सप्लाइ चेन स्थापित की जा सके।

संदर्भ: Cert-In द्वारा जारी

[TechnicalGuidelines-on-SBOM,QBOM&CBOM,AIBOM and HBOM ver2.0.pdf](#)

एफ.आई.पी.एस. (FIPS) 140-2 का क्या हुआ ?

***स्रोत NIST:** "सत्यापित मॉड्यूल की प्रयोज्यता

एफ.आई.पी.एस. (FIPS) 140-3 मान्यताएँ वर्तमान में स्वीकार की जा रही हैं। मान्यता मिलने के बाद , मॉड्यूल को 5 साल के लिए सक्रिय सूची में रखा जाएगा (या अंतरिम मान्यताओं के लिए 2 साल) और इन्हें नए और मौजूदा सिस्टम्स में इस्तेमाल किया जा सकता है।

आगे की राह

बेहतर सुरक्षा और अनुपालन सुनिश्चित करने के लिए , प्रमाणन प्राधिकारी नियंत्रक कार्यालय (सी.सी.ए.) सभी प्रमाणन प्राधिकरणों (Certifying Authorities) को सलाह देता है कि वे भारतीय अधिकार क्षेत्र के भीतर उन्नत सुरक्षा सुनिश्चित करने हेतु यथाशीघ्र एफ.आई.पी.एस. (FIPS) 140-3 मॉड्यूल के लाभ को अपनाएँ।

तदनुसार, प्रमाणन प्राधिकरणों (CAs) को यह सुनिश्चित करना चाहिए कि वे 21 सितंबर 2026 तक एफ.आई.पी.एस (FIPS) 140-2 मॉड्यूल में डिजिटल सिग्नेचर सर्टिफिकेट (DSC) जारी करना बंद कर दें। एफ.आई.पी.एस (FIPS) 140-2 मॉड्यूल में 21 सितंबर 2026 को या उससे पहले डाउनलोड किए गए डिजिटल सिग्नेचर सर्टिफिकेट (DSC), डिजिटल सिग्नेचर सर्टिफिकेट (DSC) की वैधता समाप्त होने तक मान्य रहेंगे और उसके बाद उनका उपयोग डिजिटल सिग्नेचर सर्टिफिकेट (DSC) के नवीनीकरण या नए डाउनलोड के लिए नहीं किया जा सकेगा।

एक्सेप्शन- ऐसे मामलों में , जहाँ किसी सक्रिय डिजिटल सिग्नेचर सर्टिफिकेट (DSC) को उसी उपयोगकर्ता के लिए विधिवत प्रक्रिया का पालन करते हुए पुनः जारी करना आवश्यक हो , वहाँ प्रमाणन प्राधिकरण (CA) 21 सितंबर 2026 को या उसके बाद एफ.आई.पी.एस. (FIPS) 140-2 मॉड्यूल में उस डिजिटल सिग्नेचर सर्टिफिकेट (DSC) की शेष वैधता अवधि के लिए (केवल एक बार) उपयोगकर्ता से कोई शुल्क लिए बिना डिजिटल सिग्नेचर सर्टिफिकेट (DSC) जारी कर सकते हैं।

क्रिप्टोग्राफिक मॉड्यूल के OEMs/डिस्ट्रिब्यूटर्स को एफ.आई.पी.एस. (FIPS) 140-2 मॉड्यूल के स्थान पर एफ.आई.पी.एस. (FIPS) 140-3 मॉड्यूल के प्रतिस्थापन से संबंधित बाय-बैक या एक्सचेंज नीति को अपनी-अपनी वेबसाइट पर स्पष्ट रूप से प्रकाशित करने की सलाह दी जाती है।

प्रमाणन प्राधिकरणों (CA's) को एफ.आई.पी.एस. (FIPS) 140-3 मॉड्यूल के लिए अपनी मूल्य सूची अद्यतन करने तथा एक्सचेंज या बाय-बैक दरों को भी प्रकाशित करने की सलाह दी जाती है (यह प्रकाशन प्रमाणन प्राधिकारी नियंत्रक कार्यालय को सूचित कर मार्च 2026 तक प्रकाशित करें)

प्रमाणन प्राधिकरणों (CA's)/OEM/रिलाइंग पार्टियों को यह भी सलाह दी जाती है कि वे अपनी एक्सचेंज नीति और मूल्य सूची के साथ इस परामर्श को व्यापक रूप से प्रचारित करें, ताकि रिलाइंग पार्टियों/सामान्य जनता को इसकी जानकारी मिल सके।

एक्सेप्शन- विशेष मामलों में , जहाँ केवल सरकारी संगठन अपनी सुरक्षा नीति पर विचार करने के बाद एफ.आई.पी.एस. (FIPS) 140-2 मॉड्यूल का उपयोग जारी रखने का निर्णय लेते हैं (लेकिन 21 सितंबर 2029 के बाद नहीं) , ऐसे विशिष्ट सरकारी संगठनों को प्रमाणन प्राधिकरणों (CA's) एफ.आई.पी.एस. 140-2 मॉड्यूल में डिजिटल सिग्नेचर सर्टिफिकेट (DSC) जारी कर सकते हैं। ऐसे मामलों में , प्रमाणन प्राधिकरण (CA) को संबंधित मंत्रालय की स्वीकृति के साथ , रिलाइंग पार्टी के अधिकृत अधिकारी से जोखिम एवं अनुपालन छूट (Risk and Compliance Waiver) प्राप्त करनी होगी (प्रारूप अनुलग्नक-2 में संलग्न है।) प्रमाणन प्राधिकरणों (CA's) को ऐसे संगठनों की एक लिखित सूची तिमाही आधार पर निरंतरता हेतु प्रमाणन प्राधिकारी नियंत्रक कार्यालय (सी.सी.ए.) कार्यालय को सूचित एवं उपलब्ध करानी चाहिए।

यह ध्यान दिया जाए कि प्रमाणन प्राधिकारी नियंत्रक कार्यालय (सी.सी.ए.) ने 1 जनवरी 2026 से एफ.आई.पी.एस. (FIPS) 140-2 मॉड्यूल के लिए नए ऑडिट आवेदन स्वीकार करना बंद कर दिया है।

मुख्य अंतर: एफ.आई.पी.एस. (FIPS) 140-2 बनाम एफ.आई.पी.एस. (FIPS) 140-3

क्षेत्र	एफ.आई.पी.एस. (FIPS) 140-2	एफ.आई.पी.एस. (FIPS) 140-3
बेसिस	प्रोप्रायटरी स्टैंडर्ड	ISO/IEC 19790 & 24759
एल्गोरिदम	वैलिडेशन सी.ए.वी.पी.	सी.एम.वी.पी.अलाइन्ड विद आई.एस.ओ.
टेस्टिंग	वेंडर इंटरप्रिटेशन	स्ट्रिक्ट लैब-ड्रिवन टेस्टिंग
सिक््योरिटी लेवल	1-4	1-4 (क्लैरिफ़ाइड एवं स्ट्रिक्टर)

सॉफ्टवेयर मॉड्यूल्स	लेस प्रिस्क्रिप्टिव	स्ट्रॉन्गर लाइफसाइकल एवं इंटीग्रेटी कंट्रोल्स
लेगेसी एल्गोरिदम	अनेक अनुमत (मेनी अलाउड)	डेप्रिकेटेड या डिसअलाउड
सॉफ्टवेयर इंटीग्रेटी	बेसिक	एक्सप्लिसिट इंटीग्रेटी मैकेनिज़्म
फ़र्मवेयर प्रोटेक्शन	लिमिटेड	मैंडेटरी ऑथेन्टिकेटेड अपडेट्स
की स्टोरेज डेफ़िनिशन	इम्प्लिसिट, लूज़ली डिस्क्राइब्ड	एक्सप्लिसिटली डिफ़ाइन्ड सिक्योरिटी बाउंड्री
स्टोरेज लोकेशन	ऑफ़न वेग	मस्ट बी क्लियरली आइडेंटिफ़ाइड एंड जस्टिफ़ाइड
बाउंड्री एनफ़ोर्समेंट	अस्यूम्ड	फ़ॉर्मली एनफ़ोर्सड एंड वैलिडेटेड
प्लेनटेक्स्ट कीज़ इन मेमोरी	कॉमनली एक्सेप्टेड	स्ट्रॉन्गली रेस्ट्रिक्टेड
प्रोटेक्शन एक्सपेक्शन	रीज़नेबल	एक्सप्लिसिट क्रिप्टोग्राफ़िक प्रोटेक्शन रिक्वायर्ड
एन्क्रिप्शन ऑफ़ स्टोर्ड कीज़	ऑप्शनल इन सम केस	मैंडेटरी अनलेस जस्टिफ़ाइड
की-रैपिंग स्टैंडर्ड्स	फ्लेक्सिबल	स्ट्रिक्ट यूज़ ऑफ़ अप्रूव्ड की-रैपिंग एल्गोरिद्म
एक्सेस कंट्रोल	हार्ड-लेवल	रोल-बेस्ड एंड एनफ़ोर्सिबल

निष्कर्ष

एफ.आई.पी.एस. (FIPS) 140-2 से एफ.आई.पी.एस. (FIPS) 140-3 में माइग्रेट करना एक रणनीतिक सुरक्षा अनुपालन है। सुदृढ़ शासन और प्रमाणन निकायों के साथ प्रारंभिक जुड़ाव के साथ एक संरचित , जोखिम-आधारित दृष्टिकोण अपनाकर , संगठन अनुपालन प्राप्त कर सकता है , साथ ही अपनी क्रिप्टोग्राफ़िक स्थिति को मजबूत कर सकता है और अपने प्लेटफ़ार्मों को भविष्य के लिए तैयार कर सकता है।

अनुलग्नक-1

एफ.आई.पी.एस. FIPS 140-3 मॉड्यूल प्रयोज्यता मैट्रिक्स

रिलाइंग पार्टिज़	अनुपालन	गतिविधि	एक्सेप्शन
ओईएम/डिस्ट्रीब्यूटर	अनिवार्य	एफ.आई.पी.एस. (FIPS) 140-3 मॉड्यूल के लिए CCAs ऑडिट आवश्यक है , जिसे मई 2026 तक पूरा किया जाना चाहिए।	नहीं
प्रमाणन प्राधिकारी	अनिवार्य	एफ.आई.पी.एस. (FIPS) 140-3 का एकीकरण और जुलाई 2026 तक अनुपालन ऑडिट पूरा करना।	नहीं
सरकारी संगठन	संबंधित मंत्रालय की मंजूरी के साथ , यह 21 सितम्बर 2029 तक वैकल्पिक है।	रिस्क एनालिसिस एंड एक्सेपेंस	नो एक्सेप्शन बियाँड कटऑफ़ डेट
अन्य उपयोगकर्ता	वैकल्पिक	--	--

अनुलग्नक-2

[संगठन के आधिकारिक लेटरहेड पर]

दिनांक: [दिन महीना वर्ष]

विषय: एफ.आई.पी.एस. (FIPS) 140-2 मान्य मॉड्यूल के निरंतर उपयोग के लिए प्रमाणन प्राधिकारी नियंत्रक कार्यालय के परामर्श और जोखिम मूल्यांकन की स्वीकृति।

सेवा में,

[प्रमाणन प्राधिकारी / ग्राहक का नाम]

[संगठन का नाम]

विषय: एफ.आई.पी.एस. (FIPS) 140-2 द्वारा मान्य क्रिप्टोग्राफिक मॉड्यूल के निरंतर उपयोग के लिए प्रमाणन प्राधिकारी नियंत्रक कार्यालय के परामर्श और जोखिम मूल्यांकन की स्वीकृति।

प्रिय [महोदय/महोदया/प्राप्तकर्ता का नाम],

यह पत्र औपचारिक रूप से पुष्टि करने के लिए है कि [संगठन का नाम] ने प्रमाणन प्राधिकरण नियंत्रक कार्यालय (सी.सी.ए.) द्वारा जारी एडवाइजरी की समीक्षा की है और उसे समझा है, जो एफ.आई.पी.एस. (FIPS) 140-2 से एफ.आई.पी.एस. (FIPS) 140-3 सत्यापित क्रिप्टोग्राफिक मॉड्यूल में बदलाव और सुरक्षा बढ़ाने के बारे में है।

एडवाइजरी की प्राप्ति और समीक्षा के बाद, [संगठन का नाम] ने हमारे वातावरण में एफ.आई.पी.एस. (FIPS) 140-2 मान्य क्रिप्टोग्राफिक मॉड्यूल के निरंतर उपयोग से जुड़े तकनीकी, परिचालन, सुरक्षा (गोपनीयता, अखंडता और उपलब्धता), नियामक, और व्यावसायिक विचारों को कवर करते हुए अपना स्वयं का स्वतंत्र जोखिम मूल्यांकन और प्रभाव विश्लेषण किया है।

इस मूल्यांकन के आधार पर, और वर्तमान उपयोग, संभावित खतरों, सुरक्षा उपायों, विक्रेता की योजनाओं और सिस्टम के जीवनकाल को ध्यान में रखते हुए, [संगठन का नाम] ने यह तय किया है कि मौजूदा एफ.आई.पी.एस. (FIPS) 140-2 सत्यापित मॉड्यूल का इस्तेमाल अभी भी सही है और इससे हमारे सिस्टम और डेटा की गोपनीयता, सुरक्षा या उपलब्धता को कोई गंभीर खतरा नहीं है।

यह निर्णय निम्नलिखित बातों को ध्यान में रखकर लिया गया है:-

- वर्तमान में उपयोग में होने वाले क्रिप्टोग्राफिक मॉड्यूल एफ.आई.पी.एस. (FIPS) 140-2 के तहत वैध रूप से प्रमाणित हैं और अनुमोदित मोड में काम कर रहे हैं, लेकिन ये 21 सितम्बर 2029 के बाद मान्य नहीं रहेंगे।
- वर्तमान में कोई ज्ञात सुरक्षा कमजोरियाँ नहीं पाई गई हैं, जो एफ.आई.पी.एस. (FIPS) 140-2 मॉड्यूल के निरंतर उपयोग से जोखिम को महत्वपूर्ण रूप से बढ़ा सकती हों।
- पहचाने गए जोखिमों को कम करने के लिए उचित सुरक्षा उपाय लागू किए गए हैं।
- संगठन में एफ.आई.पी.एस. (FIPS) 140-3 सत्यापित मॉड्यूल की ओर एक योजनाबद्ध और नियंत्रित संक्रमण रणनीति पर काम चल रहा है, जिसे नियामक आवश्यकताओं, विक्रेता की उपलब्धता और संचालन संबंधी व्यवहार्यता के अनुसार लागू किया जाएगा।

[संगठन का नाम] यह स्वीकार करता है कि एफ.आई.पी.एस. (FIPS) 140-3 नवीनतम मानक है और अधिक सुरक्षित है। संगठन यह भी पुष्टि करता है कि वह उचित और जोखिम-प्रबंधित समयसीमा के भीतर एफ.आई.पी.एस. (FIPS) 140-3 सत्यापित मॉड्यूल में पूरी तरह से 21 सितम्बर 2029 या उससे पहले ही माइग्रेट करने के लिए प्रतिबद्ध है, यदि नियामक दिशानिर्देशों, खतरे की परिस्थितियों, या सिस्टम वास्तुकला में महत्वपूर्ण बदलाव होते हैं। वर्तमान निर्णय की समय-समय पर समीक्षा की जाएगी।

यह पत्र हमारे उचित जांच-पड़ताल और जोखिम-आधारित निर्णय लेने की प्रक्रिया का औपचारिक दस्तावेज़ (रिकॉर्ड) के रूप में जारी किया गया है।

यदि आपको किसी अतिरिक्त जानकारी या स्पष्टीकरण की आवश्यकता हो, तो कृपया [प्रमाणन प्राधिकारी प्रतिनिधि का नाम, ईमेल और फोन] से संपर्क करने में संकोच न करें।

भवदीय,

[नाम]

[पदनाम]

[संगठन का नाम]

[संपर्क विवरण]

नोट:-हिंदी संस्करण में विसंगति की स्थिति में अंग्रेजी संस्करण मान्य होगा।

Advisory Note on FIPS 140-2 to FIPS 140-3

Migration

Introduction

This document outlines the certifying authority and organisation-wide strategy to migrate cryptographic modules and dependent systems from FIPS 140-2 to FIPS 140-3. The objective is to ensure continued regulatory compliance, maintain security assurance, minimize operational disruption, and align cryptographic controls with current international standards (ISO/IEC 19790:2012 and ISO/IEC 24759:2017).

FIPS 140-2 validations are being sunset, and new validations are required under FIPS 140-3. This migration document defines scope, governance, timelines and execution phases.

Background and Drivers

FIPS 140-3 supersedes FIPS 140-2 and is mandatory for new cryptographic module validations.

Why FIPS 140-3?

As it aligns with international ISO standards and introduces updated requirements, which would enhance security for:

- Non-invasive attack mitigation
- Software module validation
- Entropy and random bit generation
- Lifecycle assurance
- Reduction of compliance and audit risk
- Improved cryptographic assurance and resilience, Non-proprietary Standards.
- Alignment with modern platforms (containers, virtualization).

This document is for all stake holders, OEMs, Distributers, Vendors or any other association of persons/company etc operating in India who are being advised to achieve FIPS 140-3 validation for all in-scope cryptographic modules (Crypto Tokens, HSM, Secure elements etc) before **21 September 2026**, to ensure uninterrupted service for products and internal systems relying on cryptography.

Objectives

The objective of this exercise is to retire or replace non-compliant or obsolete cryptographic components in use, completely by **21 September 2029** as no further updates for FIPS 140-2 would be available after **21 September 2026**.

In addition, the objective is to establish sustainable cryptographic governance for future standards/updates.

Scope

This migration document applies to PKI ecosystem operational under CCA's jurisdiction and includes:

- All software, firmware, hardware, and hybrid cryptographic modules.
- Third-party products and services claiming FIPS compliance.
- Internal applications, platforms, and infrastructure that rely on FIPS-validated cryptography.

By ensuring, the stockholders first prepare a CBOM for establishing a trusted supply chain.

Ref: [TechnicalGuidelines-on-SBOM,QBOM&CBOM,AIBOM and HBOM ver2.0.pdf](#) by Cert-In

What happened to FIPS 140-2

*Source NIST **“Applicability of Validated Modules**

FIPS 140-3 validations are currently being accepted. Upon validation, modules will be placed on the Active list for 5 years (or 2 years for Interim Validations) and may be used for new and existing systems.

Modules validated as conforming to FIPS 140-2 can continue to be accepted by the Federal agencies of both countries for the protection of controlled unclassified information (United States) or Designated Information (Canada) through September 21, 2026. After that time CMVP will place the FIPS 140-2 validated modules on the Historical list, allowing agencies to continue using these modules for existing systems only. Agencies should continue to make use of FIPS 140-2 modules until replacement FIPS 140-3 modules become available”.

Path ahead

For enhanced security and compliance CCA advises all Certifying Authorities to adopt the benefit of FIPS 140-3 modules as early as possible for assuring enhanced security within the Indian jurisdiction.

Accordingly, CAs should ensure to stop issuance of DSC in FIPS 140-2 modules by 21 September 2026. The DSC which are downloaded in FIPS 140-2 modules on or before 21 September 2026 will remain in operation till the expiry of the DSC and no longer be used for renewal or fresh download of DSC thereafter.

Exception – in cases, where an active DSC requires reissuance to the same user, by following due process, CA’s may issue DSC on or after 21 September 2026 in FIPS 140-2 module for the remaining validity of the DSC (one time only) without any cost to user.

OEMs/Distributors of Cryptographic modules are advised to publish buy back or exchange policy clearly on their respective website regarding replacement of FIPS 140-2 modules with FIPS 140-3 modules.

CA’s are advised to update their price list for FIPS 140-3 modules and also publish exchange or buy back rates (with information to O/o CCA, by Mar 2026).

CA’s/OEM/relying parties are also advised to widely publicize this advisory along with their exchange policy and price list to relying parties/public at large.

Exception- for specific cases where in the Government organisation only, after considering their security policy choose to continue with FIPS 140-2 modules (but not after 21 September 2029), CA’s may issue DSC to such specific govt organisation in FIPS 140-2 modules. In such cases CA should collect the risk and compliance waiver from relying party authorised officer with the approval from their concerned Ministry (format attached, annexure -2). CAs should inform and provide a written list of such organisations to the office of CCA on quarterly basis for continuation.

It may be noted that, O/o CCA has stopped accepting fresh audit application for FIPS 140-2 modules w.e.f 1st January 2026.

Key Differences: FIPS 140-2 vs FIPS 140-3

Area	FIPS 140-2	FIPS 140-3
Basis	Proprietary standard	ISO/IEC 19790 & 24759
Algorithm	Validation CAVP	CMVP aligned with ISO
Testing	Vendor interpretation	Strict lab-driven testing
Security Levels	1–4	1–4 (clarified & stricter)
Software Modules Legacy algorithms	Less Prescriptive Many allowed	Stronger lifecycle & integrity controls Deprecated or disallowed
Software integrity	Basic	Explicit integrity mechanism
Firmware protection	Limited	Mandatory authenticated updates
Key storage definition	Implicit, loosely described	Explicitly defined security boundary

Storage location	Often vague	Must be clearly identified and justified
Boundary enforcement Plaintext keys in memory	Assumed Commonly accepted	Formally enforced and validated Strongly restricted
Protection expectation Encryption of stored keys	Reasonable Optional in some cases	Explicit cryptographic protection required Mandatory unless justified
Key-wrapping standards	Flexible	Strict use of approved key-wrapping algorithms
Access controls	High-level	Role-based and enforceable

Conclusion

Migrating from FIPS 140-2 to FIPS 140-3 is a strategic security compliance. By following a structured, risk-based approach with strong governance and early engagement of certification bodies, the organisation can achieve compliance while strengthening its cryptographic posture and future-proofing its platforms.

Annexure-1

FIPS 140-3 module Applicability matrix

Relying Parties	Compliance	Activity	Exception
OEM/Distributor	Mandatory	CCAs Audit requirement to be completed by May 2026 for FIPS 140-3 modules	No
Certifying Authority	Mandatory	Integration of FIPS 140-3 and compliance audit by July 2026	No
Government Organisation	Optional up to 21 sept 2029 With approval from their concern ministry	Risk analysis and acceptance	No exception beyond cutoff date
Other User	Optional	--	--

Annexure -2

[On Organisation Letterhead]

Date: [DD Month YYYY]

Subject: Acknowledgement of CCA Advisory and Risk Assessment for Continued Use of FIPS 140-2 Validated Modules

To

[Certifying Authority / Customer Name]

[Organisation Name]

Subject: Acknowledgement of CCA Advisory and Risk Assessment for Continued Use of FIPS 140-2 Validated Cryptographic Modules

Dear [Sir / Madam / Recipient Name],

This letter is to formally confirm that [Organisation Name] has reviewed and understood the advisory issued by the Controller of Certifying Authorities (CCA) regarding the transition from FIPS 140-2 to FIPS 140-3 validated cryptographic modules which enhance security.

Following receipt and review of the advisory, [Organisation Name] has conducted its own independent risk assessment and impact analysis covering technical, operational, security (Confidentiality, integrity & availability), regulatory, and business considerations associated with the continued use of FIPS 140-2 validated cryptographic modules in our environment.

Based on this assessment, and considering the current scope of usage, threat landscape, compensating controls, vendor roadmaps, and system lifecycle constraints, [Organisation Name] has determined that the continued use of existing FIPS 140-2 validated modules remains appropriate at this time and does not introduce unacceptable risk to confidentiality, integrity, or availability of our systems and data.

This decision has been taken with the following considerations:

- The cryptographic modules in use remain validly certified under FIPS 140-2 and are operating in approved modes but not after 21 Sept 2029.
- No known vulnerabilities so far / as on date have been identified that would materially increase risk due to the continued use of FIPS 140-2 modules.
- Appropriate compensating security controls are in place to mitigate identified risks.
- A planned and controlled transition strategy towards FIPS 140-3 validated modules is under evaluation in the organisation and will be implemented in alignment with regulatory expectations, vendor availability, and operational feasibility.

[Organisation Name] acknowledges that FIPS 140-3 represents the latest standard, is more secure and confirms its commitment to completely migrate to FIPS 140-3 validated modules within an appropriate and risk-managed timeframe latest by 21 sept 2029, or earlier if there are material changes in regulatory guidance, threat conditions, or system architecture. The current decision shall be periodically reviewed.

This letter is issued as a formal record of our due diligence and risk-based decision-making process.

Should you require any additional information or clarification, please feel free to contact [Certifying Authority representative name, email and phone].

Yours faithfully,

[Name]

[Designation]

[Organisation Name]

[Contact Information]

