No. 2026-4, July2026
ISSN: 2086-8154

Economic Research Institute for ASEAN and East Asia

ERIA POLICY BRIEF

ICT Products that Use Cryptography in ASEAN: Balancing Digital Trade and Regulatory Objectives in DEFA

Key Messages:

- Broad application of crypthography regulation to commercial ICT products can increase compliance costs, delay market entry, and disproportionately affect MSMEs and digital start-ups.
- Recent FTAs and DEAs increasingly seek to balance ease of market entry with legitimate government oversight, including lawful access, financial supervision, and national security.
- If ASEAN includes provisions on ICT products that use cryptography in DEFA, they should support digital trade while preserving regulatory flexibility and strengthening implementation capacity amongst ASEAN Member States.

Cryptography is embedded in a wide range of internationally traded information and communication technology (ICT) products, including smartphones, laptops, and software applications, even when encryption is not their primary function. As a result, national cryptography laws and controls may increasingly affect a broad range of commercial ICT products.

This policy brief examines the intersection of cryptography-related regulations in ASEAN and provisions in free trade agreements (FTAs) and digital economy agreements (DEAs). It shows that licensing requirements, import and export controls, and conformity assessment procedures, when applied too broadly to ICT products that use cryptography, can raise compliance costs and unintentionally restrict trade. The brief reviews how recent FTAs and DEAs address ICT products that use cryptography, highlighting common prohibitions on mandatory disclosure of encryption information, forced localisation, and prescribed algorithms, alongside clear carve-outs for regulatory and judicial access. Based on these developments, the brief offers policy considerations for ASEAN Member States (AMS) in assessing whether and how to include provisions on ICT products that use cryptography in the ASEAN Digital Economy Framework.

Introduction

Cryptography is the science of secure communication. It ensures that data can be accessed only by intended recipients and remains hidden from third parties. Cryptography serves three principal purposes: protecting data privacy through encryption, verifying data authenticity, and maintaining data integrity.

Cryptographic products, such as encryption software and hardware security modules, are designed primarily to perform these cryptographic functions. However, as cryptographic functions have become embedded in ICT products that are traded internationally and widely used in everyday life, trade rules increasingly affect ICT products that use cryptography, which incorporate cryptographic functionality as a secondary feature. These include, for example, smartphones, laptops, virtual private network (VPN) software, and certain recording or imaging devices that rely on encryption to secure communications, data storage, or authentication, even though cryptography is not their primary function.

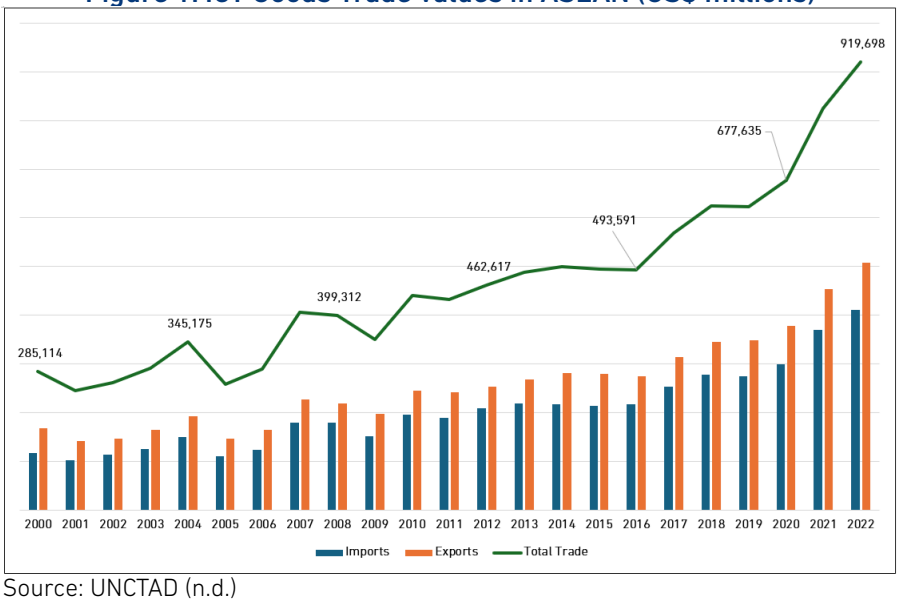
As a dual-use technology, cryptography is subject to import and export controls, as well as licensing requirements, in many jurisdictions. In many countries, cryptography laws form part of broader national frameworks regulating the import and use of ICT goods with built-in encryption functions. As a result, manufacturers and foreign suppliers have raised concerns that national cryptography policies and regulations may create significant compliance costs when applied broadly to commercial ICT products. Furthermore, the broad application of these measures may not sufficiently distinguish between commercial, public sector, and critical infrastructure applications.

Please cite this content as:
ERIA (2026), 'ICT Products that Use Cryptography in ASEAN: Balancing Digital Trade and Regulatory Objectives in DEFA'. ERIA Policy Brief 2026-4. Jakarta: ERIA. Available at: https://www.eria.org/publications/ict-products-that-use-cryptography-in-asean--balancing-digital-trade-and-regulatory-objectives-in-defa

Figure 1 demonstrates the growing trade in ICT goods across ASEAN, which reached a record high of US$919.7 billion in 2022, exceeding the European Union's US$818.1 billion. ASEAN accounted for 15% of global ICT goods trade that year. These trends highlight the importance of facilitating trade in ICT goods to support the development of regional ICT supply chains and enhance ASEAN's competitiveness. While these figures do not represent trade in cryptographic products per se, they illustrate the substantial trade value of ICT goods that increasingly rely on embedded cryptographic functions.

At the multilateral level, the WTO Technical Barriers to Trade (TBT) Agreement allows technical specifications for cryptographic products, provided they are based on international standards and are not 'more trade-restrictive than necessary'. The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) protects intellectual property rights (IPRs) related to cryptography but does not regulate its use directly. Meanwhile, the General Agreement on Tariffs and Trade (GATT) and the General Agreement on Trade in Services (GATS) require most-favoured-nation (MFN) treatment and national treatment where

Figure 1. ICT Goods Trade Values in ASEAN (US$ millions)



Source: UNCTAD (n.d.)

commitments have been scheduled. In practice, however, additional technical regulations and conformity assessment procedures, alongside strict licensing requirements and import and export controls, may increase compliance costs for foreign manufacturers, suppliers, and importers of ICT products that use cryptography.

Consequently, recent free trade agreements (FTAs) and digital economy agreements (DEAs) have introduced more detailed provisions limiting the application of certain measures affecting ICT products that use cryptography. For ASEAN, careful consideration should be given to the inclusion of such commitments in the Digital Economy Framework Agreement (DEFA), balancing digital trade facilitation with the preservation of legitimate regulatory authority.

Why Governments Regulate Cryptography

A. Access and Security

Governments may require lawful access to encrypted information, such as emails, digital financial records, or other encrypted data, for supervisory or investigatory purposes, including financial supervision and law enforcement to combat cybercrime. In Australia, for instance, the Cybercrime Act 2001 allows authorities to compel individuals to disclose encryption keys or passwords, with non-compliance punishable by imprisonment. This illustrates the ongoing debate between ensuring national security and preserving the integrity of encryption systems for privacy and trust in digital communications. Law enforcement access must therefore be accompanied by assurances that proprietary cryptographic information remains protected from disclosure – a concern that the private sector has sought to address in recent trade agreements. For DEFA, this indicates that any provisions on ICT products that use cryptography would need to preserve ASEAN Member States' lawful access functions whilst avoiding overly broad disclosure requirements that extend beyond what security objectives actually require.

B. Financal Supervision and Market Confidence

Cryptography secures banking systems, payment networks, and financial transactions by ensuring authentication, confidentiality, and integrity. Financial regulators, such as central banks, require supervisory and investigatory powers to oversee institutions and safeguard market stability, but such oversight should be limited to prudential regulation and financial integrity rather than broad disclosure of cryptographic design. Recognising the sensitivity of this sector, many FTAs and DEAs exclude government measures relating to financial institutions from the application of cryptography provisions. This suggests one design principle for DEFA: maintaining an appropriate balance between supervisory authority and strong encryption is necessary to preserve both regulatory trust and market confidence. Carve-outs for financial supervision are therefore not a weakening of trade disciplines but a necessary safeguard.

C. Quantum Computing and Future Security Risks

Governments also regulate cryptography in anticipation of risks associated with advances in quantum computing.

Cryptographically relevant quantum computers, whilst still some distance from maturity, could eventually undermine widely used public-key cryptography, exposing communications and financial transactions collected today to future decryption (BSI, 2022). Policy responses have accordingly focused on cryptographic inventorying and the development of post-quantum standards through processes led by institutions such as the US National Institute of Standards and Technology (NIST), giving rise to the concept of crypto-agility: the capacity of ICT products to update cryptographic algorithms as standards evolve (OECD, 2024). As quantum computing continues to develop, policymakers will also need to consider its implications for cryptographic policies, although this falls outside the scope of this policy brief.

Laws and Regulations Relating to Cryptography in ASEAN

A. Import/Export Controls and Licensing

Some ASEAN Member States impose licensing or import/export controls on ICT products that use cryptography. In Singapore, the Strategic Goods (Control) Act and its 2019 Order classify certain encryption technologies as strategic goods subject to export licensing. Malaysia's Strategic Trade Act 2010 (Sections 7 and 9) similarly restricts the import and export of controlled technologies, including encryption products.

Viet Nam's *Law on Cyberinformation Security* (Articles 31 and 34) requires businesses trading in civil cryptographic products to obtain a licence from the Government Cipher Committee. The law also conditions import and export licences on the products being certified as conforming to national standards. Article 36 further requires organisations and individuals to declare their use of encryption products supplied by unlicensed traders.

B. Technical Standards and Conformity Assessments for ICT Products

Before certain ICT products can be sold domestically, some ASEAN Member States require them to obtain mandatory conformity certification before they can be imported. These procedures are intended to ensure that products meet prescribed encryption standards, such as those applicable to certain civil cryptographic products under IPsec and TLS security groups. Certification is typically issued by accredited domestic bodies, although some governments accept certification from international third-party bodies where domestic capacity is limited. The majority of ASEAN Member States, however, do not maintain comparable conformity assessment requirements for these products.

When licensing and conformity assessment requirements are applied too broadly, they may be interpreted to cover commercial ICT products that use cryptography only as a secondary function. This can result in time-consuming and resource-intensive compliance processes that significantly increase costs, not only for large firms but also for micro, small, and medium-sized enterprises (MSMEs) and technology start-ups with limited capacity to navigate complex licensing and conformity assessment requirements.

ICT Products that Use Cryptography in FTAs

Recent FTAs and DEAs have addressed ICT products that use cryptography because governments are seeking to strike a balance between facilitating digital trade and preserving regulatory authority. For ASEAN policymakers, these agreements are relevant as examples of how other economies have attempted to manage this trade-off. They also provide insight into how DEFA could reduce unnecessary regulatory barriers affecting regional digital supply chains whilst maintaining flexibility for legitimate public policy objectives.

A. Prohibitions on Market Entry Conditions and Their Implications

In general, cryptography provisions allow governments to adopt technical regulations and conformity assessment procedures, but prohibit additional conditions that restrict market entry. Three prohibitions are common across the agreements reviewed, each carrying implications for DEFA.

The first bars governments from requiring disclosure of encryption keys, algorithm designs, or other confidential cryptographic information to protect companies' intellectual property and ensure user privacy. At the same time, legitimate law enforcement and regulatory oversight may require lawful access where necessary, requiring an appropriate balance between data protection and public safety (van Daalen, 2023). This prohibition complements related FTA provisions protecting source code from mandatory disclosure.

The second prohibits governments from requiring firms to establish joint ventures or partnerships with local entities as a condition for the manufacture, sale, or import of ICT products that use cryptography. This rule seeks to prevent forced localisation practices and allow firms to retain control over proprietary technologies. In Malaysia, Viet Nam, and Indonesia, for example, majority or full foreign ownership in telecommunications is restricted or requires joint ventures with state-owned or local firms. It is worth noting that the text proposal under the WTO JSI negotiations on ICT products that use cryptography reflected local partnership requirements only in the context of mandatory disclosure and transfer of cryptographic information, although the scope extends to measures beyond technical regulations.

The third bars governments from mandating specific encryption algorithms for commercial products, except for government or central bank systems. This provision prevents the imposition of national or proprietary standards that could restrict competition and predominantly favour domestic suppliers better able to meet national standards. However, when national standards deviate from internationally recognised frameworks such as the National Institute of Standards and Technology (NIST) cryptographic standards or ISO/IEC 19790, they may inadvertently increase vulnerabilities to security breaches and hinder interoperability across markets. Allowing firms to choose their own cryptographic solutions can therefore promote interoperability and market-driven cybersecurity, although it may also challenge regulators to maintain consistent oversight and lawful access where necessary (Riebe et al., 2022). For ASEAN, this consideration is relevant as businesses increasingly operate across multiple markets. If DEFA were to include a similar prohibition, it could help reduce compliance costs, support interoperability across ASEAN markets, and strengthen regional digital ecosystems whilst still allowing governments to pursue legitimate security objectives.

B. Scope Limitations, Carve-outs, and Regulatory Access

Whilst the prohibitions define what governments may not do, their application is bounded by carve-outs that preserve regulatory authority. These prohibitions typically apply only to products designed for commercial applications. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), through an annex to its Technical Barriers to Trade chapter, the Singapore–Australia Digital Economy Agreement (SADEA), and the Korea–Singapore Digital Partnership Agreement (KSDPA) explicitly exclude products developed by or for governments and preserve supervisory powers over financial institutions and networks. The UK–Singapore Digital Economy Agreement (UKSDEA) explicitly carves out law enforcement, financial regulation, and government-controlled networks.

Most, if not all, FTA and DEA commitments also recognise legitimate regulatory and judicial access in accordance with the Parties' legal procedures. For instance, the UKSDEA permits regulators and courts to require proprietary cryptographic information for investigations or competition remedies, subject to appropriate safeguards. For DEFA, these carve-outs in recent agreements suggest that both objectives can be accommodated through carefully designed scope limitations and exceptions.

Policy Recommendations

The preceding discussion suggests that the policy question for ASEAN is how DEFA can enhance regulatory coherence and provide added value in supporting trade in ICT goods whilst preserving legitimate regulatory space. At the same time, provisions on ICT products that use cryptography would represent a novel discipline in ASEAN's regional trade architecture, given that the Regional Comprehensive Economic Partnership (RCEP) and the upgraded ASEAN–Australia–New Zealand Free Trade Area (AANZFTA) do not address this issue. Unlike some ASEAN Member States (AMS) that have already accepted comparable commitments through the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) or the Digital Economy Partnership Agreement (DEPA), others have limited experience with such disciplines and maintain different regulatory approaches. Both dimensions – DEFA's role as a potential first in ASEAN's regional trade architecture, and the diversity of AMS experience – suggest that this issue should be approached with care, given its technical complexity, security sensitivity, and novelty for some AMS. Should provisions relating to ICT products that use cryptography be considered for DEFA, the following recommendations are put forward to facilitate digital trade, preserve regulatory authority, and support effective implementation across AMS.

1. Facilitate Digital Trade and Protect Innovation

- To protect innovation, provisions should prohibit requirements for manufacturers or suppliers of commercial ICT products that use cryptography to disclose private keys, cryptographic algorithms, or production processes as a condition of market access.
- Address burdensome compliance procedures for importing ICT products that use cryptography by simplifying existing import licensing and conformity assessment regimes to reduce compliance costs. Transparent, proportionate, and non-discriminatory procedures aligned with international standards can lower administrative burdens whilst maintaining national security oversight.

2. Preserve legitimate regulatory authority

- Explicitly preserve government authority by carving out exceptions for lawful access, including judicial proceedings, competition law enforcement, financial supervision, and government-controlled networks, whilst ensuring that safeguards prevent misuse and that regulatory access does not undermine trade secret protections.
- Given the binding nature of these commitments, DEFA could consider allowing sufficient policy space and transitional flexibility for AMS that are still developing their cryptography frameworks.

3. Support implementation and regulatory co-operation

- Considering the varied national approaches to encryption regulation, encourage information exchange, capacity building, and the sharing of good practices on encryption governance, particularly in regulatory and supervisory approaches. This would help reduce unnecessary regulatory divergence and strengthen trust in regional digital markets.
- Incorporate knowledge-sharing and capacity-building programmes into DEFA implementation on the relationship between cryptography laws and trade, with private sector engagement to better understand how manufacturers, importers, distributors, and end-users may be affected by the scope of such regulations.

Acknowlegements

This Policy Brief was prepared by Mahirah Mahusin and Hilmy Prilliadi.

References

BSI (2022), *Quantum-safe Cryptography – Fundamentals, Current Developments and Recommendations*.

OECD (2024), *Key Concepts and Current Technical Trends in Cryptography for Policy Makers*.

OHCHR (2015), *The Use of Encryption and Anonymity in Digital Communications*.

Riebe, T., Kühn, P. Imperatori, and C. Reuter (2022), 'U.S. Security Policy: The Dual-Use Regulation of Cryptography and its Effects on Surveillance', *European Journal for Security Research*, 7(1), pp.39–65. https://doi.org/10.1007/s41125-022-00080-0

UNCTAD (n.d.), UNCTADstat Data centre. Https://Unctadstat.Unctad.Org/Datacentre/.

van Daalen, O.L. (2023), 'The Right to Encryption: Privacy as Preventing Unlawful Access', *Computer Law & Security Review*, 49, 105804. https://doi.org/10.1016/j.clsr.2023.105804

ERIA
Sentral Senayan II, 5th, 6th, 15th floors
Jalan Asia Afrika No. 8
Senayan, Central Jakarta 10270, Indonesia
Tel: (62-21) 57974460
E-mail: contactus@eria.org