CHAPTER 15

DIGITAL TRADE

Article 15.1
Definitions

For the purposes of this Chapter:

"cipher" or **"cryptographic algorithm"** means a mathematical procedure or formula for combining a key with plaintext to create a ciphertext;

"ciphertext" means data in a form that cannot be easily understood without subsequent decryption;

"commercial information and communication technology product" or **"commercial ICT product"** means a product that is designed for commercial applications and whose intended function is information processing and communication by electronic means, including transmission and display, or electronic processing applied to determine or record physical phenomena, or to control physical processes;

"computing facilities" means a computer server or storage device for processing or storing information for commercial use;

"covered person" means:

(a) a covered investment as defined in Article 14.2 (Definitions – Investment);

(b) an investor of a Party as defined in Article 14.2 (Definitions – Investment); or

(c) a service supplier of a Party as defined in Article 9.1 (Definitions – Cross-Border Trade in Services),

but does not include a financial service supplier as defined in Article 11.1 (Definitions – Financial Services);

"cryptography" means the principles, means, or methods for the transformation of data in order to conceal or disguise its content, prevent its undetected modification, or prevent its unauthorised use, and is limited to the transformation of information using one or more secret parameters, for example, crypto variables or associated key management;

"digital innovation" means the development, implementation, or adoption of new or improved digital technologies, digital processes, or digital organisational methods;

"electronic authentication" or **"e-authentication"** means an electronic process or act of verifying that enables the confirmation of:

(a) the electronic identification of a person; or

(b) the origin and integrity of data in electronic form;

"electronic invoicing" or **"e-invoicing"** means the automated creation, exchange, and processing of requests for payments between suppliers and buyers using a structured digital format;

"electronic seal" means data in electronic form used by an enterprise which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;

"electronic signature" means data in electronic form which is attached to or logically associated with other data in electronic form that is:

(a) used to identify the signatory in relation to the data in electronic form; and

(b) used by a signatory to agree on the data in electronic form to which it relates;[1]

"electronic transmission" or **"transmitted electronically"** means a transmission made using an electromagnetic means, including by photonic means;

"emerging technology" means an enabling and innovative technology that has potentially significant application across a wide range of existing and future sectors, including artificial intelligence, distributed ledger technologies, quantum technologies, immersive technologies, sensing technologies, and the Internet of Things;

"encryption" means the conversion of data (plaintext) through the use of a cryptographic algorithm into a ciphertext using the appropriate key;

"key" means a parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that a person with knowledge of the key can reproduce or reverse the operation, but a person without knowledge of the key cannot;

[1] For greater certainty, nothing in this provision prevents a Party from according greater legal effect to an electronic signature that satisfies certain requirements, such as indicating that the electronic data message has not been altered or verifying the identity of the signatory.

"personal information" means information, including data, about an identified or identifiable natural person;

"trade administration documents" means the forms and documents that must be completed by or for an importer or exporter in connection with the import or export of goods; and

"unsolicited commercial electronic message" means an electronic message which is sent for commercial or marketing purposes, without the consent of the recipient or despite the explicit rejection of the recipient, directly to a natural person, or enterprise if provided for in a Party's laws and regulations, via a public telecommunications service. For the purposes of this Agreement, this covers electronic mail, text and multimedia messages (SMS and MMS), and other forms of electronic messages governed by a Party's laws and regulations.[2]

Article 15.2
Objectives

The Parties recognise the economic growth and opportunities provided by digital trade and the importance of:

(a) adopting frameworks that promote consumer confidence in digital trade;

(b) promoting interoperability of regulatory frameworks to facilitate digital trade;

(c) avoiding unnecessary barriers to the use and development of digital trade; and

(d) digital inclusion, including participation of Māori, women, persons with disabilities, rural populations, low socio-economic groups as well as enterprises, individuals, and other groups that disproportionately face barriers to digital trade.

Article 15.3
Scope and General Provisions

1. This Chapter shall apply to measures adopted or maintained by a Party affecting trade enabled by electronic means.

2. This Chapter shall not apply to:

(a) audio-visual services; or

[2] For greater certainty, an unsolicited commercial electronic message does not include a message sent by or on behalf of a Party.

(b) government procurement, except for Article 15.5 (Conclusion of Contracts by Electronic Means), Article 15.7 (Electronic Authentication), and Article 15.9 (Electronic Invoicing).

3. Article 15.12 (Commercial Information and Communication Technology Products that Use Cryptography), Article 15.14 (Cross-Border Transfer of Information by Electronic Means), and Article 15.15 (Location of Computing Facilities) shall not apply to information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection.

4. Article 15.14 (Cross-Border Transfer of Information by Electronic Means) and Article 15.15 (Location of Computing Facilities) shall not apply to aspects of a Party's measures that do not conform with an obligation in Chapter 9 (Cross-Border Trade in Services) or Chapter 14 (Investment), to the extent that such measures are adopted or maintained in accordance with:

(a) Article 9.8 (Non-Conforming Measures – Cross-Border Trade in Services) or Article 14.10 (Non-Conforming Measures – Investment); or

(b) any exception that is applicable to the obligations in Chapter 9 (Cross-Border Trade in Services) and Chapter 14 (Investment).

Article 15.4
Customs Duties

1. Neither Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a person of a Party and a person of the other Party.

2. For greater certainty, paragraph 1 shall not preclude a Party from imposing internal taxes, fees, or other charges on electronic transmissions, including content transmitted electronically, provided that those taxes, fees, or charges are imposed in a manner consistent with this Agreement.

3. The Parties shall cooperate in relevant international fora to promote the adoption of commitments by non-parties not to impose customs duties on electronic transmissions.

Article 15.5
Conclusion of Contracts by Electronic Means

1. Except in circumstances otherwise provided for in its law, a Party shall not adopt or maintain measures that:

(a) deprive an electronic contract of legal effect, enforceability, or validity, solely on the ground that the contract has been made by electronic means; or

(b) otherwise create obstacles for the use of electronic contracts.

2. Recognising the importance of increasing the use of electronic contracts, the Parties should review and reduce the circumstances referred to in paragraph 1.

Article 15.6
Domestic Electronic Transactions Framework

1. Each Party shall maintain a legal framework governing electronic transactions consistent with the principles of the *UNCITRAL Model Law on Electronic Commerce* done at New York on 12 June 1996 or the *United Nations Convention on the Use of Electronic Communications in International Contracts* done at New York on 23 November 2005.

2. Each Party shall endeavour to:

(a) avoid any unnecessary regulatory burden on electronic transactions; and

(b) facilitate input by interested persons in the development of its legal framework for electronic transactions.

3. The Parties recognise the importance of facilitating the use of electronic transferable records. When developing measures relating to electronic transferable records, each Party shall take into account the *UNCITRAL Model Law on Electronic Transferable Records* done at New York on 13 July 2017.

Article 15.7
Electronic Authentication

1. Except in circumstances otherwise provided for under its laws and regulations, neither Party shall deny the legal effect or admissibility as evidence in legal proceedings of an electronic document, an electronic signature, an electronic seal, or the authenticating data resulting from electronic authentication, solely on the ground that it is in electronic form.

2. Neither Party shall adopt or maintain a measure that would:

(a) prohibit parties to an electronic transaction from mutually determining the appropriate electronic authentication method for their transaction; or

(b) prevent parties to an electronic transaction from being able to prove to judicial and administrative authorities that the use of electronic authentication in that transaction complies with the applicable legal requirements.

3. Notwithstanding paragraph 2, a Party may require that for a particular category of transactions, the method of electronic authentication is certified by an authority accredited in accordance with its law or meets certain performance standards which shall be objective, transparent, and non-discriminatory and shall only relate to the specific characteristics of the category of transactions concerned.

4. The Parties shall encourage the use of interoperable electronic authentication, and recognise the benefits of working towards mutual recognition of electronic authentication. To this end, the Parties shall endeavour to share information, where appropriate, on matters related to e-authentication.

5. To the extent provided for under its laws or regulations, a Party shall apply paragraphs 1 to 4 to electronic processes or means of facilitating or enabling electronic transactions, such as electronic time stamps and electronic registered delivery services.

Article 15.8
Digital Identities

1. The Parties recognise that:

(a) the cooperation of the Parties on digital identities will increase regional and global connectivity; and

(b) each Party may have different implementations of, and legal approaches to, digital identities.

2. The Parties shall strengthen cooperation and facilitate initiatives to promote compatibility and interoperability between their respective regimes for digital identities, including exploring:

(a) the development and maintenance of appropriate frameworks to increase technical and service interoperability between each Party's implementation of digital identities;

(b) supporting the development of international frameworks on digital identity regimes;

(c) identifying use cases for the mutual recognition of digital identities; and

(d) the exchange of knowledge and expertise on best practices relating to digital identity policies and regulations, technical implementation and security standards, promotion, and user adoption.

3. For greater certainty, nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective.

Article 15.9
Electronic Invoicing

1. The Parties recognise the importance of e-invoicing to increase the efficiency, accuracy, and reliability of commercial transactions. Each Party also recognises the benefits of ensuring interoperability of e-invoicing systems to support digital trade and that these systems can be used for business-to-business and business-to-consumer digital transactions.

2. Each Party shall ensure that the implementation of measures related to e-invoicing in its jurisdiction is designed to support cross-border interoperability. When developing measures related to e-invoicing, each Party shall take into account international frameworks, guidelines, or recommendations, where these exist.

3. The Parties shall share best practices pertaining to e-invoicing.

Article 15.10
Paperless Trading

1. Each Party shall make trade administration documents that it issues or controls available to the public in electronic form.

2. Each Party shall endeavour to accept a trade administration document submitted electronically as the legal equivalent of the paper version of that document.

3. The Parties shall, where appropriate, cooperate bilaterally and in international fora on matters related to paperless trading, such as enhancing the standardisation and acceptance of electronic trade administration documents.

4. In developing initiatives concerning the use of paperless trading, each Party shall take into account the principles and guidelines agreed by relevant international bodies.

Article 15.11
Unsolicited Commercial Electronic Messages

1. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that:

   (a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; or

   (b) require the consent, as specified according to the laws and regulations of each Party, of recipients to receive commercial electronic messages,

   and otherwise provide for the minimisation of unsolicited commercial electronic messages.

2. Each Party shall ensure that unsolicited commercial electronic messages are clearly identifiable as such, clearly disclose on whose behalf they are made and contain the necessary information to enable recipients to request cessation free of charge and at any time.

3. Each Party shall provide access to either redress or recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained pursuant to paragraphs 1 and 2.

4. The Parties shall endeavour to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.

Article 15.12
Commercial Information and Communication Technology Products that Use Cryptography

1. Neither Party shall impose or maintain a technical regulation or conformity assessment procedure that requires a manufacturer or supplier of a commercial ICT product that uses cryptography, as a condition of the manufacture, sale, distribution, import, or use of that commercial ICT product, to:

   (a) transfer or provide access to any proprietary information relating to cryptography, including by disclosing a particular technology or production process or other information, for example, a private key or other secret parameter, algorithm specification, or other design detail, to that Party or a person in the territory of that Party;

(b) partner or otherwise cooperate with a person in the territory of that Party in the development, manufacture, sale, distribution, import, or use of the commercial ICT product; or

(c) use or integrate a particular cipher or cryptographic algorithm.

2. Notwithstanding paragraph 1 of Article 15.3 (Scope and General Provisions), this Article shall apply to commercial ICT products that use cryptography.[3] This Article shall not apply to:

(a) a Party's law enforcement authorities requiring service suppliers using encryption to provide access to encrypted and unencrypted communications pursuant to that Party's legal procedures;

(b) the regulation of financial instruments;

(c) a requirement that a Party adopts or maintains relating to access to networks, including user devices, that are owned or controlled by that Party, including those of central banks;

(d) measures by a Party adopted or maintained pursuant to supervisory, investigatory, or examination authority relating to financial service suppliers or financial markets;

(e) the manufacture, sale, distribution, import, or use of a commercial ICT product by or for a Party; or

(f) a commercial ICT product other than a good.

Article 15.13
Personal Information Protection

1. The Parties emphasise the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade.

2. Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. In the development of its legal framework for the protection of personal information, each Party shall take into account principles and guidelines of relevant international bodies.

3. The Parties recognise that the principles underpinning a robust personal information protection framework include:

[3] For greater certainty, for the purposes of this Article, a commercial ICT product does not include a financial instrument.

(a) collection limitation;

(b) data quality;

(c) purpose specification;

(d) use limitation;

(e) security safeguards;

(f) openness;

(g) individual participation; and

(h) accountability.

4. Each Party shall adopt non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction.

5. Each Party shall publish information on the personal information protections it provides to users of digital trade, including how:

(a) an individual can pursue a remedy; and

(b) an enterprise can comply with any legal requirements.

6. Each Party shall pursue the development of mechanisms to promote compatibility and interoperability between these different regimes for protecting personal information. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall exchange information on any mechanisms applied in their respective jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility and interoperability between them.

Article 15.14
Cross-Border Transfer of Information by Electronic Means

1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.

2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, if this activity is for the conduct of the business of a covered person.

3. Nothing in this Article shall prevent a Party from adopting or maintaining a measure inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

   (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

   (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.

Article 15.15
Location of Computing Facilities

1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.

2. Neither Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.

3. Nothing in this Article shall prevent a Party from adopting or maintaining a measure inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

   (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

   (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

Article 15.16
Open Internet Access

Subject to their applicable policies, laws, and regulations, each Party recognises the benefits of consumers[4] in their territory having the ability to:

   (a) access, distribute, and use services and applications of their choice available on the Internet, subject to reasonable network management which does not block or slow down traffic based on commercial reasons;

[4] For the purposes of this Article, "consumer" means a natural person or enterprise using the Internet for personal, trade, or business or professional purposes.

(b) connect devices of their choice to the Internet, provided that these devices do not harm the network; and

(c) access information on the network management practices of their Internet access service supplier.

Article 15.17
Open Government Data

1. For the purposes of this Article, government data and information means non-proprietary data and information held by the central level of government and, to the extent provided for under a Party's laws and regulations, by other levels of government.

2 The Parties recognise that facilitating public access to and use of government data and information fosters economic and social development, competitiveness, and innovation. To this end, each Party is encouraged to expand the coverage of government data and information digitally available for public access and use, through engagement and consultation with interested stakeholders, and Māori in the case of New Zealand.

3 To the extent that a Party makes government data and information available to the public, it shall endeavour to ensure that the data and information is in a machine-readable and open format and can be searched, retrieved, used, reused, and redistributed.

4. Each Party shall provide interested persons with the opportunity to request the disclosure of specific government data and information.

5. The Parties shall cooperate, as appropriate, to identify ways in which each Party can expand access to and the use of government data and information that the Party has made public, with a view to enhancing and generating business opportunities, especially for SMEs.

Article 15.18
Cooperation on Cyber Security Matters

1. The Parties recognise the importance of promoting secure digital trade to achieve global prosperity and recognise that threats to cyber security undermine confidence in digital trade.

2. The Parties further recognise the importance of:

(a) building the capabilities of their respective national entities responsible for cyber security incident response, taking into account the evolving nature of cyber security threats;

(b) using and strengthening existing collaboration mechanisms for cooperating to anticipate, identify, and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties, and using those mechanisms to swiftly address cyber security incidents;

(c) workforce development in the area of cyber security, including through possible initiatives relating to mutual recognition of qualifications, and promoting diversity and equality; and

(d) maintaining a dialogue on matters related to cyber security, including for the sharing of information and experiences for awareness and best practices.

3. Given the evolving nature of cyber security threats, the Parties recognise that risk-based approaches may be more effective than prescriptive approaches in addressing those threats including in the context of digital trade. Accordingly, each Party shall encourage enterprises within its jurisdiction to use risk-based approaches that rely on open and transparent industry standards to:

(a) manage cyber security risks and to detect, respond to, and recover from cybersecurity events; and

(b) otherwise improve the cyber security resilience of these enterprises and their customers.

Article 15.19
Digital Innovation and Emerging Technologies

1. The Parties recognise the increasing social and economic importance of digital innovation and emerging technologies, and the importance of the safe and responsible development and use of emerging technologies to foster public trust.

2. The Parties further recognise that digital innovation and emerging technologies:

(a) have important roles in promoting economic competitiveness and facilitating international trade and investment flows; and

(b) may require coordinated action, including between the Parties, across multiple sectors and trade policy areas to maximise their economic and social benefits, including trade between the Parties. When taking that action, the Parties shall take into consideration relevant international frameworks.

3. Each Party shall endeavour to develop governance and policy frameworks for the trusted, safe, and responsible use of emerging technologies. To this end, in developing those frameworks, the Parties recognise the importance of:

(a) taking into account the principles and guidelines of relevant international bodies, such as the OECD and the Global Partnership on Artificial Intelligence;

(b) utilising risk-based or outcome-based approaches to regulation that take into account industry-led standards and risk management best practices; and

(c) having regard to the principles of technological interoperability and technological neutrality.

4. The Parties shall cooperate, as appropriate, on matters related to digital innovation and emerging technologies with respect to trade. This may include:

(a) exchanging information, and sharing experiences and best practices on the development and implementation of law and policies, including matters of enforcement and compliance;

(b) cooperating on developments relating to emerging technologies, including ethical use, industry-led standards, and algorithmic transparency, to address issues such as unintended biases and exacerbation of existing divides, by ensuring human diversity is recognised in the development of technologies; and

(c) participating actively in international fora.

Article 15.20
Digital Inclusion

1. The Parties recognise the importance of digital inclusion, that all people and businesses can participate in, contribute to, and benefit from digital trade. To this end, the Parties recognise the importance of expanding and facilitating digital trade opportunities by removing barriers to participation in digital trade, and that this may require tailored approaches, developed in consultation with Māori, enterprises, individuals, and other groups that disproportionately face such barriers.

2. To promote digital inclusion, the Parties shall cooperate on matters relating to digital inclusion, including participation of Māori, women, persons with disabilities, rural populations, and low socio-economic groups as well as

other individuals and groups that disproportionately face barriers to digital trade. This may include:

(a) enhancing cultural and people-to-people links, including for Māori, through promoting business development services;

(b) identifying and addressing barriers to accessing digital trade opportunities;

(c) improving digital skills and access to online business tools; and

(d) sharing methods and procedures for developing datasets and conducting analysis to identify barriers and trends over time in relation to Māori, women, and other groups which face barriers to digital trade to inform the development of digital trade policies, including developing methods for monitoring their participation in digital trade.

3. The Parties recognise the role played by SMEs, including Māori-led and women-led enterprises, in economic growth and job creation, and the need to address the barriers to participation in digital trade for those entities. To this end, the Parties shall:

(a) foster close cooperation on digital trade between SMEs of the Parties;

(b) encourage their participation in platforms that help link them with international suppliers, buyers, and other potential business partners; and

(c) share best practices in improving digital skills and leveraging digital tools and technology to improve access to capital and credit, participation in government procurement opportunities, and other areas that could help SMEs adapt to digital trade.

4. The Parties also recognise the digital divide between developed and developing countries, and the role for digital trade in promoting economic development and poverty reduction. The Parties shall endeavour to undertake and strengthen cooperation, including through existing mechanisms, to promote the participation of developing countries in digital trade. This may include sharing best practices, active engagement in international fora, and promoting developing countries' participation in, and contribution to, the global development of rules on digital trade, which may include other WTO members as appropriate.

5. The Parties shall also participate actively at the WTO and in other international fora to promote initiatives for advancing digital inclusion in digital trade.

Article 15.21
Cooperation

1. The Parties shall, where appropriate, cooperate and participate actively in international fora, including the WTO, to promote the development of international frameworks for digital trade.

2. In addition to areas of cooperation between the Parties identified in other parts of this Chapter, the Parties shall exchange information on and share experiences and best practices on regulatory matters relating to digital trade.

3. The Parties shall endeavour to cooperate to promote and facilitate collaboration between governmental entities, enterprises, and other non-governmental entities on digital technologies and services, including digital innovation and emerging technologies, in relation to opportunities in trade, investment, and research and development, including in the areas of pandemic preparedness, clean technology, and low emissions technology.

Article 15.22
Review

1. To take into account developments in digital trade, the Parties shall review the operation and implementation of this Chapter and Article 11.7 (Financial Data and Information – Financial Services) within two years of the date of entry into force of this Agreement unless the Parties agree otherwise.

2. In the context of that review, and following the release of the Waitangi Tribunal's Report Wai 2522 dated 19 November 2021, New Zealand:

   (a) reaffirms its continued ability to support and promote Māori interests under this Agreement; and

   (b) affirms its intention to engage Māori to ensure the review outlined in paragraph 1 takes account of the continued need for New Zealand to support Māori to exercise their rights and interests, and meet its responsibilities under Te Tiriti o Waitangi/the Treaty of Waitangi and its principles.