Digital Trade Standards Workshop Day 2

Standards Australia

Sydney

Wednesday 17 October 2018

Summary of Day 1 and Overview of Day 2

Standards Australia

Workshop Day 1 – technical presentations and findings

- Digital Trade is relevant to all of us and impacts all sectors of the economy
- ISO/IEC JTC 1 is broad reaching in content and engagement
- Data is the basis of digital trade
- Good governance is at the heart of any successful organisation
- Blockchain and distributed ledger technologies can provide transparency and greater financial stability
- Innovation is driving greater delivery of digital services for consumers and the market

Workshop Day 1 – country presentations

- Strengths in:
  - Government-led digital agenda's
  - Smart-phone, internet and social media penetration
  - Innovation working to meet consumer expectations and drive development
- Challenges:
  - Coordination between public and private sector
  - Cash-on-Delivery economies
  - Limited manpower to engage in and manage standards systems
  - Value-add of standards not understood

Workshop Day 1 – international standards

- Opportunities for increased engagement and coordination
- Standards can help build trust of infrastructure and services
- Standards to support the critical elements of digital trade
  - Reliable infrastructure
  - Data
  - Interoperability (language)
  - Electronic transactions

Digital Trade and Services

Ms Jane Drake-Brockman
Australian Services Roundtable

Australian Services Roundtable

Jane Drake-Brockman

Digital Trade & Trade in (digitally-enabled) Services

17 October 2018

ASIA-PACIFIC SERVICES COALITION (APSC)

Fostering cooperation towards high-quality growth and efficiency in services.

Offering a forum for public-private dialogue on the services agenda in APEC and beyond.

Asia-Pacific Services Coalition

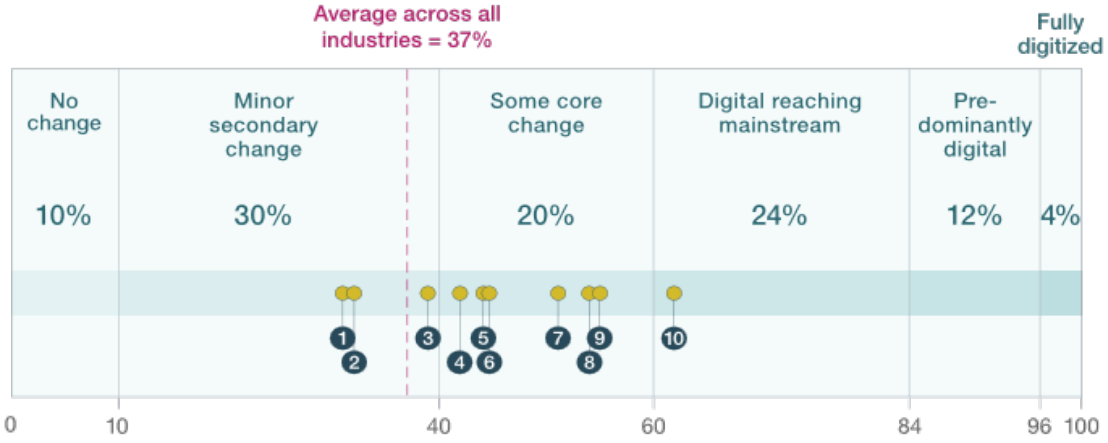
- Australian Services Roundtable
- **ABAC Brunei**
- Canadian Services Coalition
- China Association for Trade in Services
- Federation of Korean Industries
- Hong Kong Coalition of Service Industries
- **Indonesia Services Dialogue**
- Japan Services Network
- **Malaysian Service Providers' Confederation**
- Business New Zealand
- Business Council of Papua New Guinea
- Lima Chamber of Commerce Services Committee
- Pacific Basin Economic Cooperation Council
- **Philippine Services Coalition**
- **Singapore Business Federation**
- Sociedad de Fomento Fabril de Chile
- TW Coalition of Service Industries, Chinese Taipei
- U.S. Coalition of Services Industries

Non-APEC Groups

- National Business Association of Colombia, Colombia
- **ASEAN Service Providers' Confederation**
- Latin American Services Exporters Association
- European Services Forum

Digital is penetrating all sectors, but to varying degrees.

Perception of digital penetration by industry,[1] % of respondents



Selected industries[2]

1. Consumer packaged goods (31%)
2. Automotive and assembly (32%)
3. Financial services (39%)
4. Professional services (42%)
5. Telecom (44%)
6. Travel, transport, and logistics (44%)
7. Healthcare systems and services (51%)
8. High tech (54%)
9. Retail (55%)
10. Media and entertainment (62%)

[1]Data reflect average of respondents' ratings on degree of change in the past three years within each industry across 5 dimensions (products, marketing and distribution, processes, supply chains, and new entrants at the ecosystem level).

[2]For consumer packaged goods, n = 85; automotive and assembly, n = 112; financial services, n = 310; professional services, n = 307; telecom, n = 55; travel, transport, and logistics, n = 103; healthcare systems and services, n = 78; high tech, n = 348; retail, n = 89; and media and entertainment, n = 86.

McKinsey&Company

Digital technology hastened the process of services globalisation.

- Services industries were slow to globalise. Traditionally, services providers were constrained by an inability to capture, store and possess the value of the intangible. There were few opportunities to create step by step "pathways" to market as services tend to be delivered and consumed **simultaneously.**
- The application of digital technology allows services firms to segment out any business function in which services knowledge can be digitised/commoditised/packaged as a "product", ownership can be established, production can be scaled up and trade can take place separately from production.
- In effect, all services can now be traded, including cross-border via the internet
- B2B services intermediates in global value chains (generally known as knowledge-intensive business services) are **the fastest growing component of world trade** today.

Digital “data” has become the core intermediate services input

- All firms in all sectors are using intermediate inputs of digitized “knowledge-intensive business services”.
- These services inputs are themselves fragmenting to the core essential valuable ingredient of “data” inputs. Once processed, whether by human or artificial intelligence, data is becoming the essential ingredient in value-added.
- A digital unit of “data” is packaged, storeable, tradeable, knowledge ie it is ultimately a service – services expertise/knowledge packed into digital form – a key factor of production in all digitally-enabled business in both the goods and the services sectors
- **4 - 31% of services inputs are estimated to be ‘data’ related** (ECIPE).
- Increasingly, competitiveness not only in services but in *all* industries is becoming a function of **access to data** - and the *speed* of access to both.
- All services industries, indeed all industries, are increasingly dependent on **cross-border data flows**.

Governance of digital trade will become the main trade game

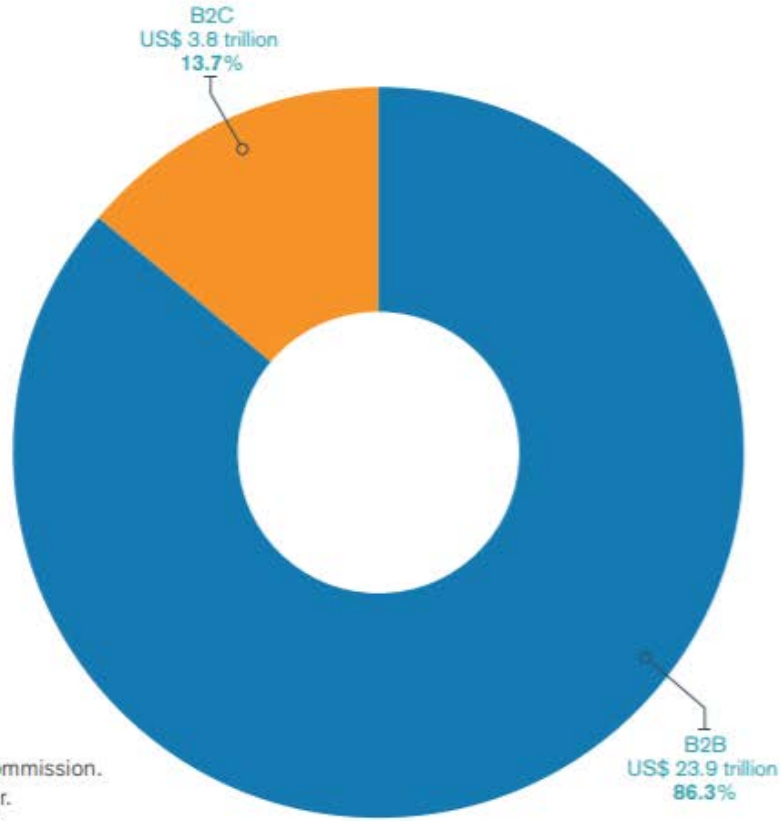
- E commerce in goods is fundamentally dependent of course on the supporting ICT services infrastructure for all e commerce plus the associated postal, transportation and financial services.
- Recent UNCTAD data shows moreover that cross border e commerce in services dwarfs e commerce in goods ie digitally-enabled services (e services) increasingly account for the bulk of “digital trade”
- Recent UNCTAD data also shows that B2B dwarfs B2C e commerce (6-10 times larger).

Global e-commerce totalled US$ 27.7 trillion in 2016, up from US$ 19.3 trillion in 2012.

Chart 2.19

Value of e-commerce markets, 2016

(US$ trillion and percentage share)



Source: US International Trade Commission.
Note: B2C: Business-to-consumer.
B2B: Business-to-business.

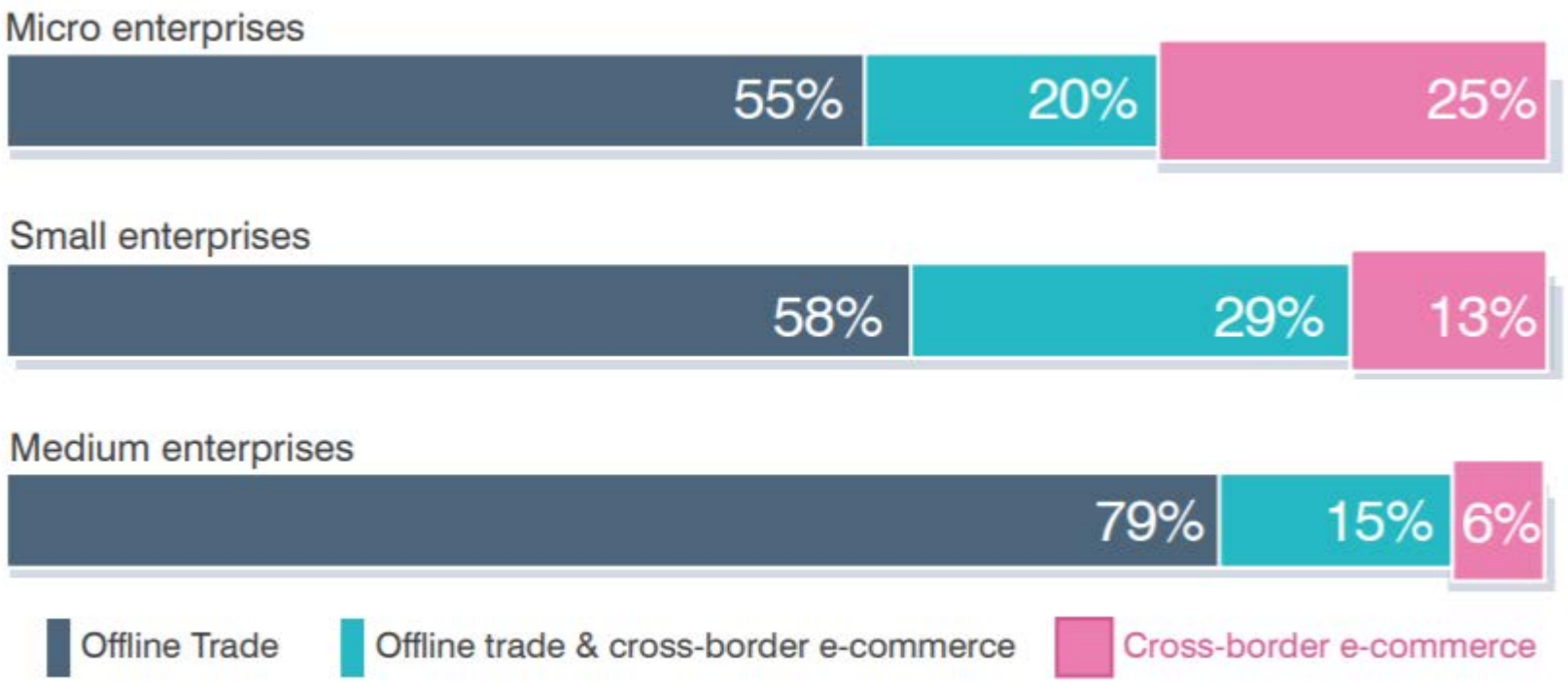
6x

Business-to-business (B2B) e-commerce is six times larger than business-to-consumer (B2C) e-commerce.

Digital “trade” is highly inclusive

- The global evidence is that digitisation of trade offers opportunities for greater economic inclusion and gender equality; for SMES and MSMEs, for women entrepreneurs, for youth, for remote and rural communities.
- E-commerce lowers the international market entry threshold for firms; 82% of companies that started trading thanks to the Internet are micro and small.
- Companies that do offline trade are still dominated by men-owned companies, whereas for those who do only online trade, the share of women-owned companies doubles.

E-commerce helps SMEs internationalise



2X The share of women-owned enterprises doubles when moving from traditional offline trade to cross-border e-commerce

Trade in services will overtake trade in goods

- World Bank data shows that global trade in goods is in long term decline and will continue to shrink. Trade in Services has a long term growth trajectory.
- New technologies such as 3DP will dramatically shorten the length of the cross-border goods value chain and increase the length of the cross-border services value chain
- Over the next two decades, many “goods” will transform towards services (CAD files) and take physical format only at the final point of consumption.
- 3 D printing (additive manufacturing) lies at the heart of this transition, expected to replace more than 50% of manufacturing processes.

Efforts at standardisation, regulatory cooperation and trade governance are lagging badly behind business needs for today's digital reality

80% of the emerging governance issues in e commerce are estimated to relate to services rather than goods

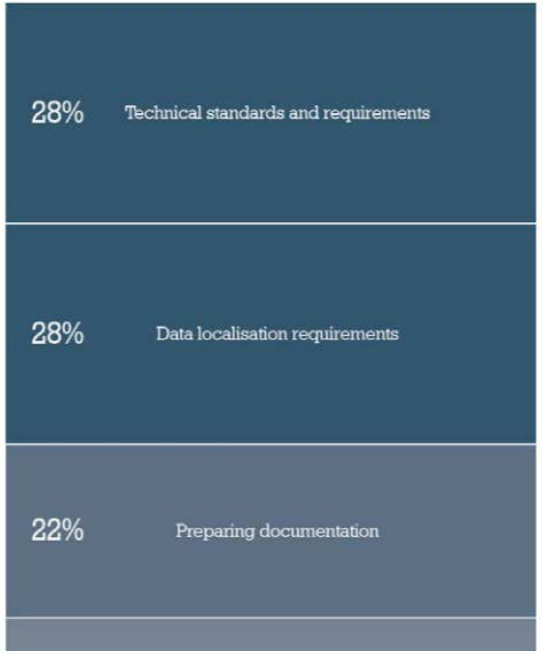
Business worries that the regional market is fragmenting, reducing the potential opportunities

Business Bottlenecks and Barriers

Figure 6 Bottlenecks in establishing an online business

Figure 9 Bottlenecks in cross-border delivery of goods

Figure 10 Bottlenecks in cross-border delivery of services



- For cross-border delivery of services (Figure 10), SME respondents to an ITC survey said their major challenges included: **difficulty to adjust services to technical standards and requirements in the destination market, data localization requirements,** difficulty to prepare required documentation (e.g. contracts, obtain licenses in the destination market) and lack of language skills.

Data localisation requirements impose high compliance cost burdens on firms doing international business – impossible for MSMEs to meet – prohibitive even for the largest firms

Figure 14 How data localization requirements affect cross-border e-commerce

Danger sign for trade
Bad news for regional integration

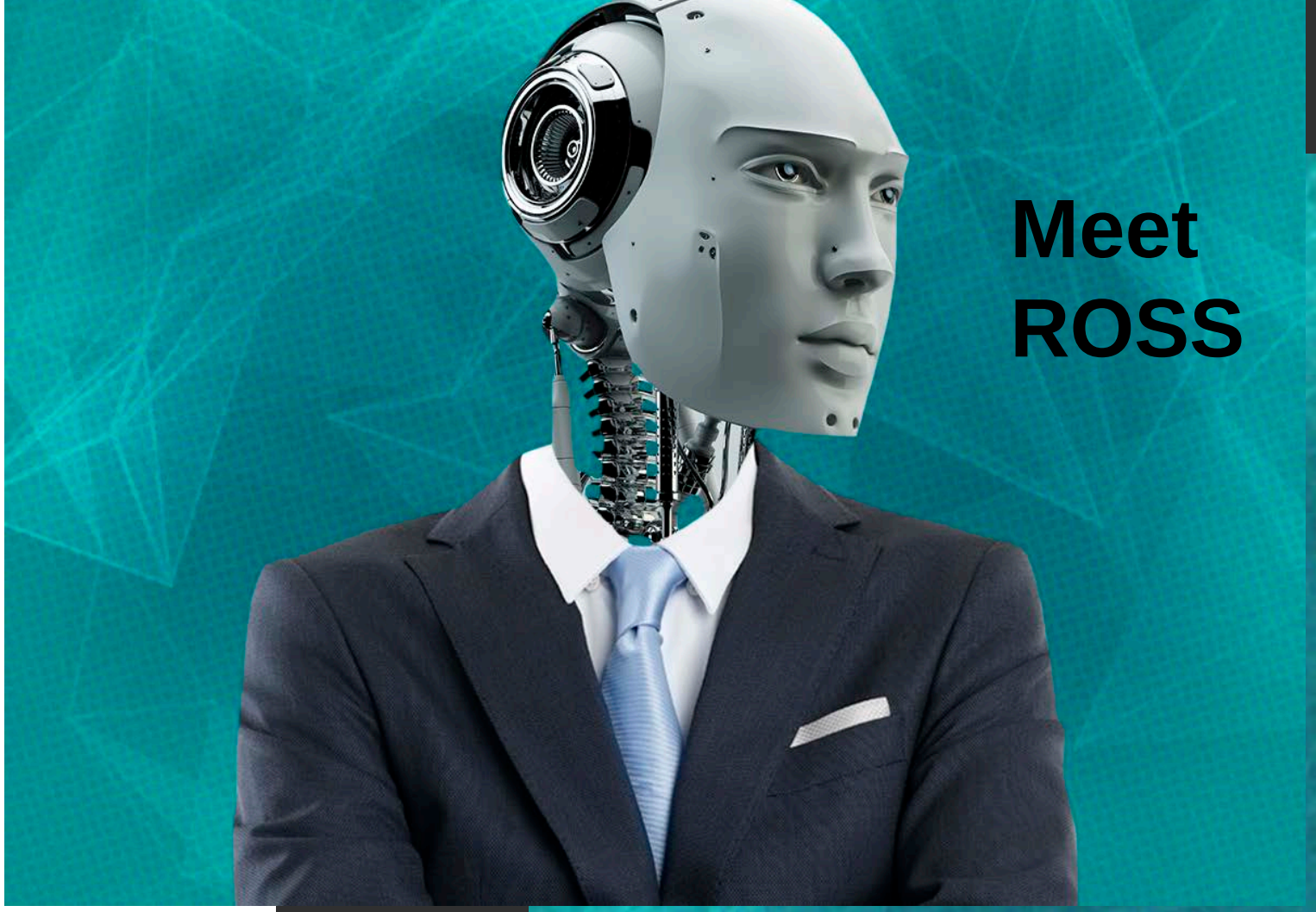
- The 2018 OECD Services Trade Restrictiveness Index (STRI) update shows that the **regulatory environment affecting digital trade is becoming more restrictive globally.**
- There is an observed tightening of measures affecting key services sectors relevant for digital trade, such as **telecommunications services**.
- There is an increase in tightening of measures affecting the temporary movement of natural persons who travel as services suppliers & tightening of conditions on foreign investment screening in services & **increasing requirements affecting cross-border data flows** & **data localisation**
- http://www.oecd.org/trade/services-trade/STRI-Policy-trends-up-to-2018.pdf

These restrictions add compliance cost burdens on business, reducing competitiveness

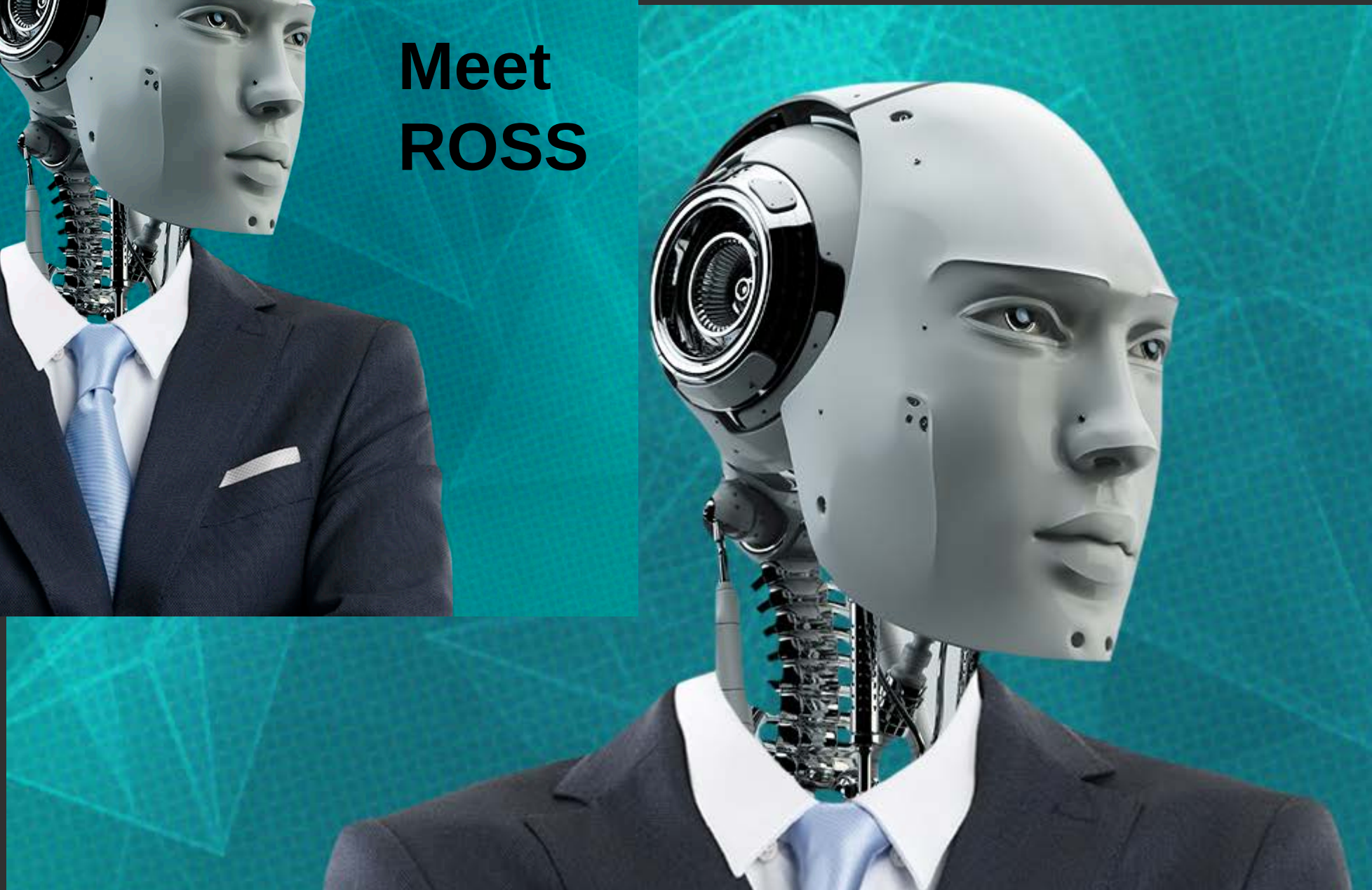
- OECD estimates that average restrictions **n**on business and consumers of key services such as computer services.
- SMEs and MSMEs are impacted the most.
- The costs of dealing with regulatory hurdles and complying with diverging regulations in different markets can amount to an **additional tariff of up to 14% on SME exports compared** to larger competitors with bigger resources to absorb trade costs.
- Divergent standards impacting on interoperability are overwhelming for MSMEs.

Business Messages

- The inter-governmental e commerce agenda is 2 decades old: from a business perspective, not enough is being done and not quickly enough and with insufficient focus on services
- APEC has an opportunity to make a real difference
- ASEAN has an opportunity to make a real difference
- The WTO at last has an opportunity to get on with it.
- The Global Services Coalition supports the commencement of plurilateral negotiations in the WTO on e commerce – including to ensure freedom of cross-border data flows, disciplines on data localisation and extended moratorium on customs duties on digital products and services.



Meet ROSS



What is Ross? How do we define it/classify it? A Good or a Service?

- Robot (Physical manifestation = Merchandise Good)
- Application of Artificial intelligence (Functionality = Services)
- Advanced Manufactured Product (very high embodied services value add/intensity in the manufacture) plus embedded after sales legal data processing and legal prediction and advisory services?
  - Computer hardware locked to specific legal services software and their updates?
- Ross is only just beginning
  - Physical Robot might become “unlocked” ie able to download additional and alternative software from an alternative legal services content provider – ie a good (becoming cheaper) and distinct from the high value added services?
  - Physical Robot might come to incorporate real time human intelligence (tele-presence)
  - Physical Robot might become obsolete (hologram)

How might “Ross” be traded?

- The Physical Robot will be shipped across a border; trade in merchandise goods (or Mode 5 trade in services)
  - In fact it will be shipped across many borders via a complex value chain of B2B trade in components
  - The legal services IP will no doubt be the highest value added component and as core business will not be outsourced by the legal services provider/owner/innovator
  - In due course, Ross will be 3D printed at the point of sales (via trade in services - CAD designs) and the legal services software will be downloaded (traded via e commerce) through the internet from the cloud or its next generation
- As the Physical Robot changes shape/manifestation and itself becomes obsolete due to technological change, the legal services, and the associated information and **data flows**, will increasingly become the critical focus for international trade governance.

How might we regulate Ross in our domestic jurisdictions?

- The Physical Robot will need to meet a multitude of standards?
- For consumer protection purposes, the embedded legal services will need to meet certified professional qualifications?
- How will current regimes for legal services regulation achieve this?
- To put it differently, how is digital transformation challenging existing professional services regulatory regimes? How do legal services regulators keep up?
- Given the digital platforms used not only by Ross, but by all kinds of emerging lower value-added on-line AI based legal services offerings, what other regulatory regimes might be involved?

Might we benefit from International Regulatory Cooperation?

- Need for regulatory best practice benchmarking? For efficiency/least burdensome industry compliance costs?
- Need to identify and address international regulatory disconnects, fragmenting the international market for legal services, now and in the future
- When legal services are not “like” in the eye of the regulator and regulatory discretion leads to discriminatory barriers to international trade
- Regulatory cooperation needs to begin at the most fundamental level in the process of international standards development.
- **Standards can show the way……..**

Towards governance of cross-border e commerce in the WTO

- E-commerce was carved out of the Doha Agenda because not everyone was ready for it;
  - we had a temporary moratorium on customs duties on electronic sales of goods (ongoing extension of which is now questioned)
  - And a work programme launched in 1998 which has now been running for 2 decades
- The rule making on e commerce/digital trade including on cross-border data flows has been experimented with in smaller groups eg FTAs .....
- At last, post WTO MC11, **plurilateral negotiations on e commerce are beginning to get underway**
  - Horizontal approach
  - 70 WTO members

Many issues raised

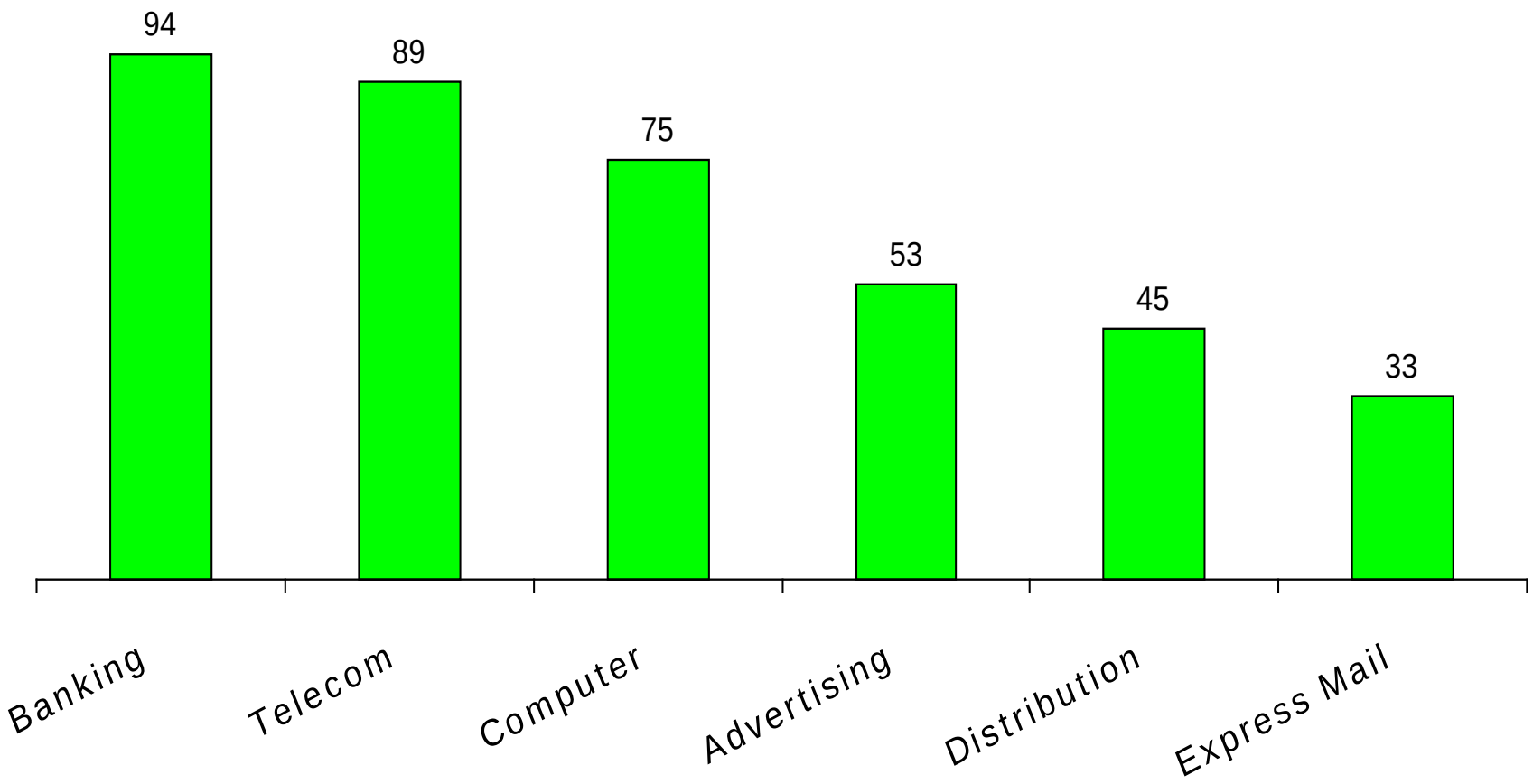
Definition
Customs duties/ moratorium
Transparency (general)
Non-discrimination
Data flows
Open Internet/ networks
Localization restrictions
Technology transfers
Source code
Choice of Technology
E-signatures/ Authentication
Network competition
Encryption
Future proofing frameworks
Standards/ interoperability
Customs procedures
Trade Facilitation
Transparency/ prior publication and comment
Conformity assessment

More issues

Cooperation with other I0s
Legitimate policy objectives,
DR & exceptions
Privacy/ personal data
Consumer protection/
confidence
- cybersecurity
- spam
Regulatory cooperation
Network neutrality
IPR protection

Market access commitments/
negotiations
Improve metrics and data
Trade monitoring
Classification
infrastructure gaps
Licensing/
authorization
Electronic payments
e-procurement
Paperless trading
Legal frameworks

GATS Commitments on E Commerce "infrastructure"



Thinking about ROSS, what regulatory regimes are relevant to digitalization of services and cross-border e-legal services?

Standardisation as well as domestic regulatory regimes such as **qualifications and licensing regimes** for professional services providers will affect the take up and use of professional services automation software – and cross-border trade in professional services?

To what extent and how might regulation affect how legal services automation software applications are used?

To what extent is cross-border trade in legal services complementary to other modes of supply (e.g. movement of people)?

What other regulatory regimes are also relevant to cross-border e-legal services?

- **Domestic regulatory regimes impacting on the electronic retail eco-system for both goods and services**/ie the entire e-tail value chain B2C, B2B, C2C (eg consumer protection and privacy, electronic payments systems, transport, logistics, delivery services, IP protection, access to telecoms, competition policy affecting horizontal and vertical monopolies eg between between ISPs and e-commerce platforms etc, intermediary liability, internet laws including censorship)
- **Domestic regulatory regimes impacting on e-commerce-enabling infrastructure services** (computer & related services, communication services, distribution services, financial services, transport and logistics)
- **Domestic regulatory regimes impacting on services whose classification is outstanding** (call centre services, cloud services, search engine services, software services including mobile apps, information services, machine-to-machine services, internet access services etc)

What space do services business need to watch?

- **O**f this complex emerging digital agenda, what might be the specific **trade governance aspects** ie **regulatory interface with trade liberalisation** (**freedom of cross-border data flows/absence of data localisation**)?
  - Cybersecurity and Cybercrime
  - Online Consumer protection
  - Protection of personal information/Privacy
  - Anti-spam
  - Protection of Source code
  - Intermediary liability
  - Authentication and E signatures
  - Infrastructure development
  - Digital divide
- **Trade in legal services could be affected by new governance arrangements in any of these areas?**
- **It's a big space to watch going forward.**

Pursuit of e commerce in FTAs

- Of the 267 FTAs notified to WTO, 63 (25%) have provisions on e commerce
- Of those 63, 84% have provisions on customs duties (with the focus on e commerce in goods)
- We also see:
  - expanded telecom regulatory principles (eg from a business point of view, these days, the internet seems pretty “basic”)
  - emerging e commerce principles (e.g. no customs duties on digital products, freedom of cross-border data flow provisions, e-commerce regulatory frameworks)
  - expanded market access commitments on telecoms and computer services (and on postal/express delivery)

CPTPP Article 14.11: Cross-Border Transfer of Information by Electronic Means

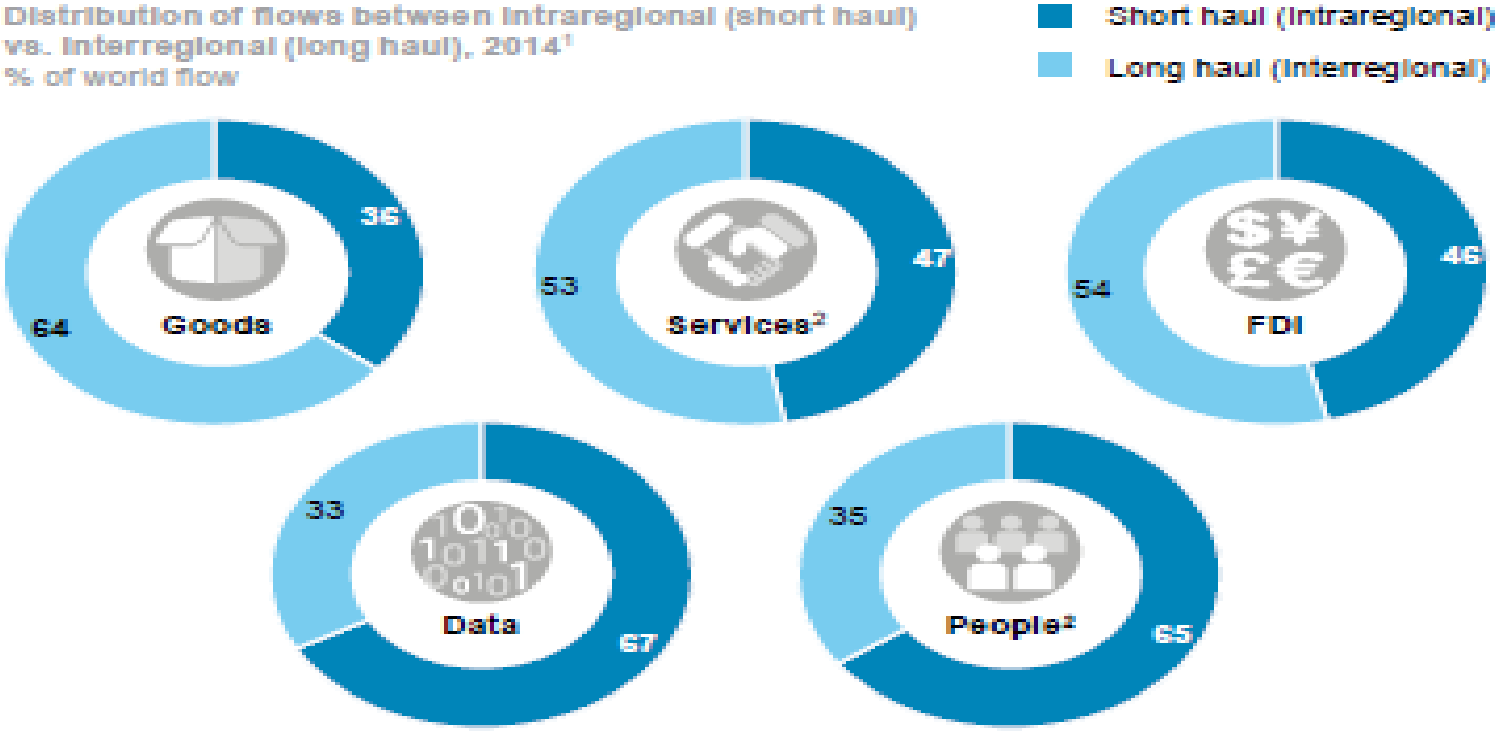
- 1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.
- 2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.
- 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures 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**.

Digital Trade and regional integration

Exhibit E8

While much of the world's trade in goods is long distance, roughly half or more of other global flows move within the same region

Distribution of flows between intraregional (short haul) vs. interregional (long haul), 2014[1]
% of world flow



1 For goods, services, FDI, and travelers we have divided the world into 10 regions; for data flows we have used TeleGeography's six regions.
2 Distribution of services flows for 2014 estimated based on 2011 data; 2013 bilateral traveler data used for people flows.
NOTE: Numbers may not sum due to rounding.

SOURCE: UNCTAD; UN World Tourism Organization; TeleGeography, Global Internet Geography; IMF; McKinsey Global Institute analysis

Morning Tea/Networking Session

Return at 10:30am

Thematic Session 4: Cybersecurity

Technical Expert: Mr New Soon Tee, Infocomm Media Development Authority

Country Presentation: Mr Heng Mara – Cambodia

Country Presentation: Mr Joseph Gan – Singapore

Country Presentation: Mr Aisharuddin Nuruddin – Malaysia

Trade Trust, Facilitating Trust and Interoperability in Cross Border Trade

Mr New Soon Tee

Infocomm Media Development Authority

TradeTrust

Facilitating Trust & Interoperability in Cross Border Trade

Sharing by IMDA Singapore

SG:D
EMPOWERING POSSIBILITIES

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

INFOCOMM MEDIA DEVELOPMENT AUTHORITY (IMDA)

DIGITAL CHAMPION

Drive digitalisation across industries

Supporting a digitally enabled workforce

INDUSTRY DEVELOPER

Develop the digital tech and media industries as an engine of growth for Singapore

Foster a data ecosystem for the digital economy

ENABLER

Master-planner for connectivity, digital infrastructure & standards

Prepare tech & media manpower, and segments of society to be digitally-ready

REGULATOR & PROTECTOR

Ensure resilient telecom & broadcast networks

Govern market conduct and protect consumer interest through infocomm, media, postal and data protection regulation

SG:D EMPOWERING POSSIBILITIES

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

TradeTrust is a set of Governance & Legal Frameworks, Standards and future-ready Digital Infrastructure, all of which facilitates the interoperability of electronic trade documents exchanged between different digital ecosystems.

It uses Distributed Ledger Technology to provide proof of authenticity and provenance for these documents, addressing the inefficiencies of cross-border trade that are caused by manual handling and verification processes.

EXISTING NON-TARIFF RELATED TRADE BARRIERS

Manual Processes

Heavy use of paper documentation

Susceptibility to fraud

Slow movement of paper documents

Risk of documents lost

Complexity

Many parties

Complex interactions

Many documents

Fragmented Systems

Lack of systems' interoperability

Lack of legal recognition for documents outside proprietary systems

Lack of standardisation for documents across trade ecosystem

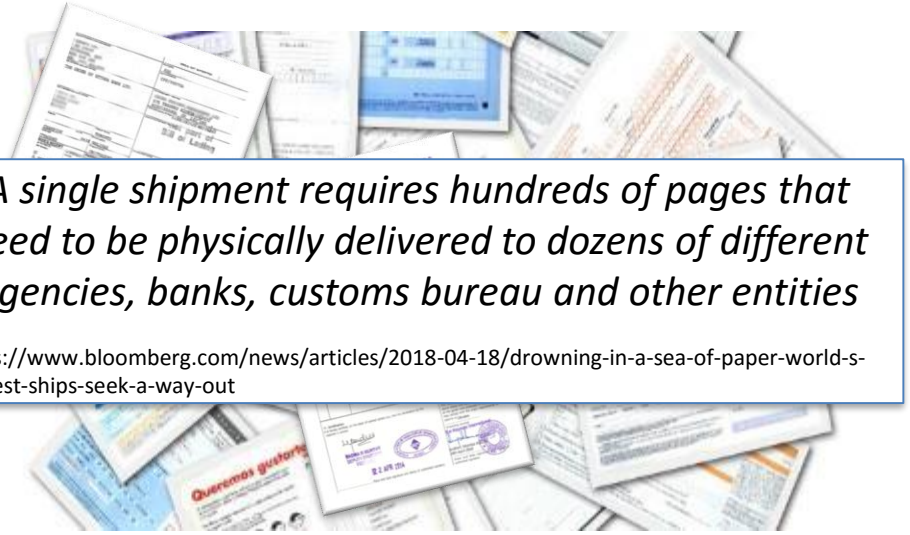
Paperless Trade originated from one country often gets "translated" into paper when crossing borders into another country

THESE TRADE BARRIERS RESULT IN INEFFICIENCIES

Lack Of Trust Is A Major Contributing Factor To The Non-Tariff Related Trade Barriers

- There is an **inherent lack of trust** between buyers, sellers, supply chain participants, agencies and governments
- Trust, or the lack of it **underlies almost every action and data exchange** in international trade
- The layer of trust has **traditionally seen little support from technology** and is still heavily reliant on the use of papers

Source:
1. Blockchain: Mapping New Trade Routes To Trust by Accenture
2. White Paper on Technical Application of Blockchain to UN/CEFACT deliverables by UN/CEFACT



A single shipment requires hundreds of pages that need to be physically delivered to dozens of different agencies, banks, customs bureau and other entities

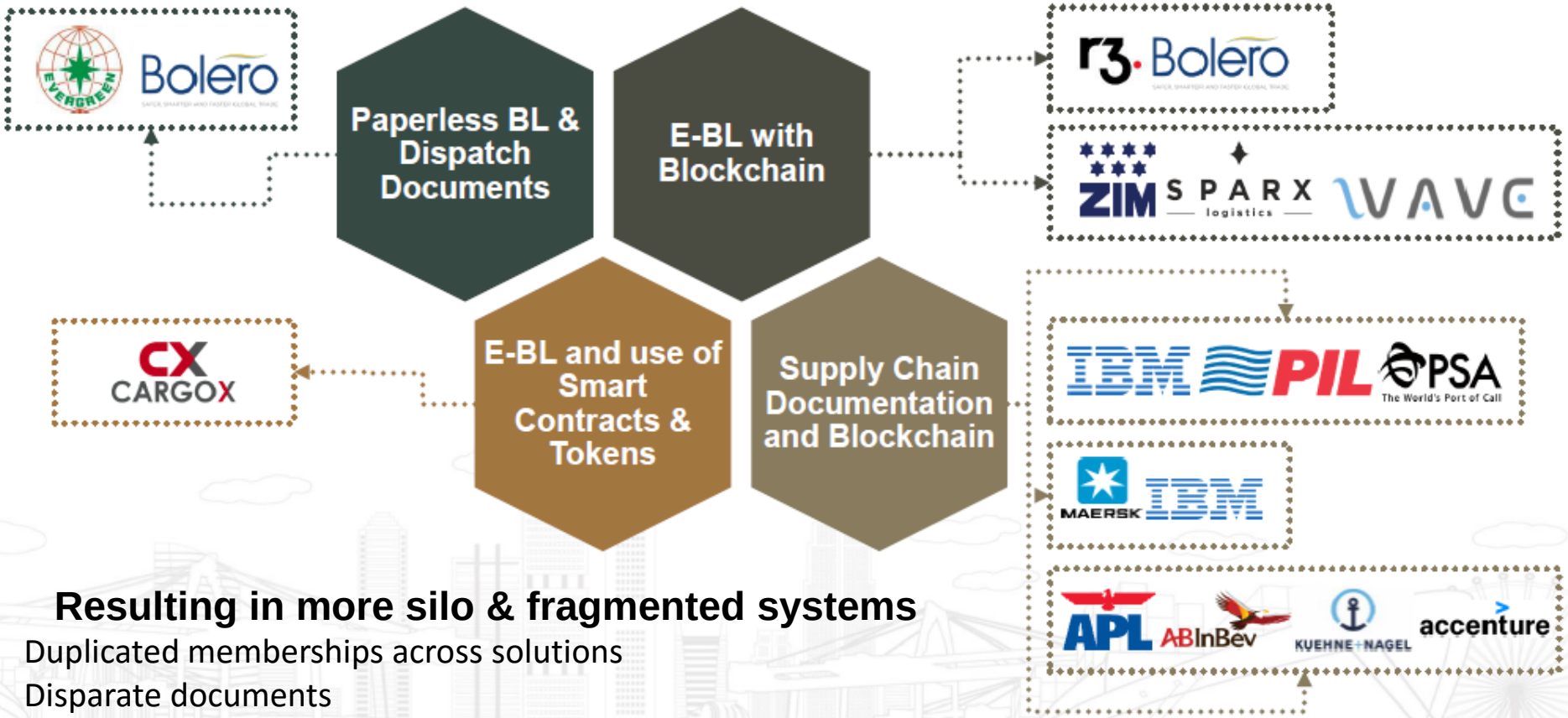
https://www.bloomberg.com/news/articles/2018-04-18/drowning-in-a-sea-of-paper-world-s-biggest-ships-seek-a-way-out

According to the World Economic Forum, the **costs of processing trade documents** are as much as **20%** of those of shifting goods.

The shipment took about **34 days** from farm to retailers, including **10 days** waiting for documents to be processed.

Maersk Paper Trail Research 2014

NEW TECHNOLOGY DEVELOPMENTS EMERGING



Resulting in more silo & fragmented systems

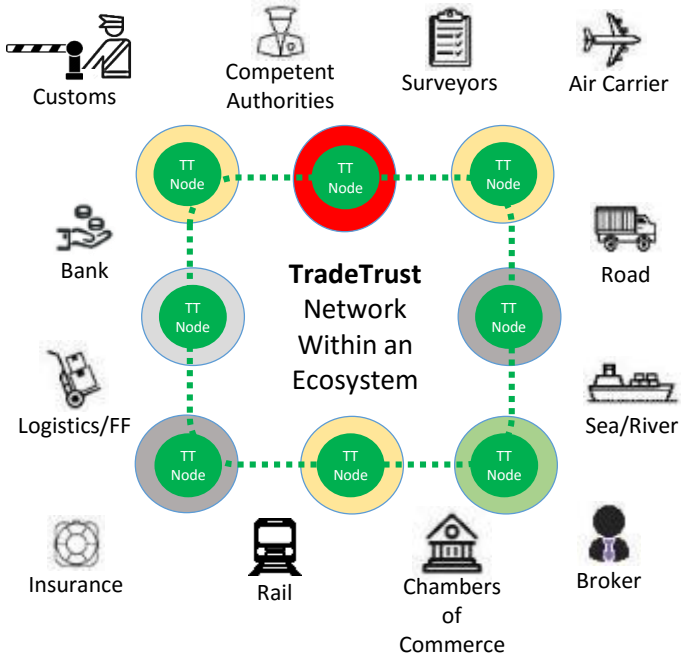
- Duplicated memberships across solutions
- Disparate documents
- Validity, Authenticity and Provenance not portable across solutions

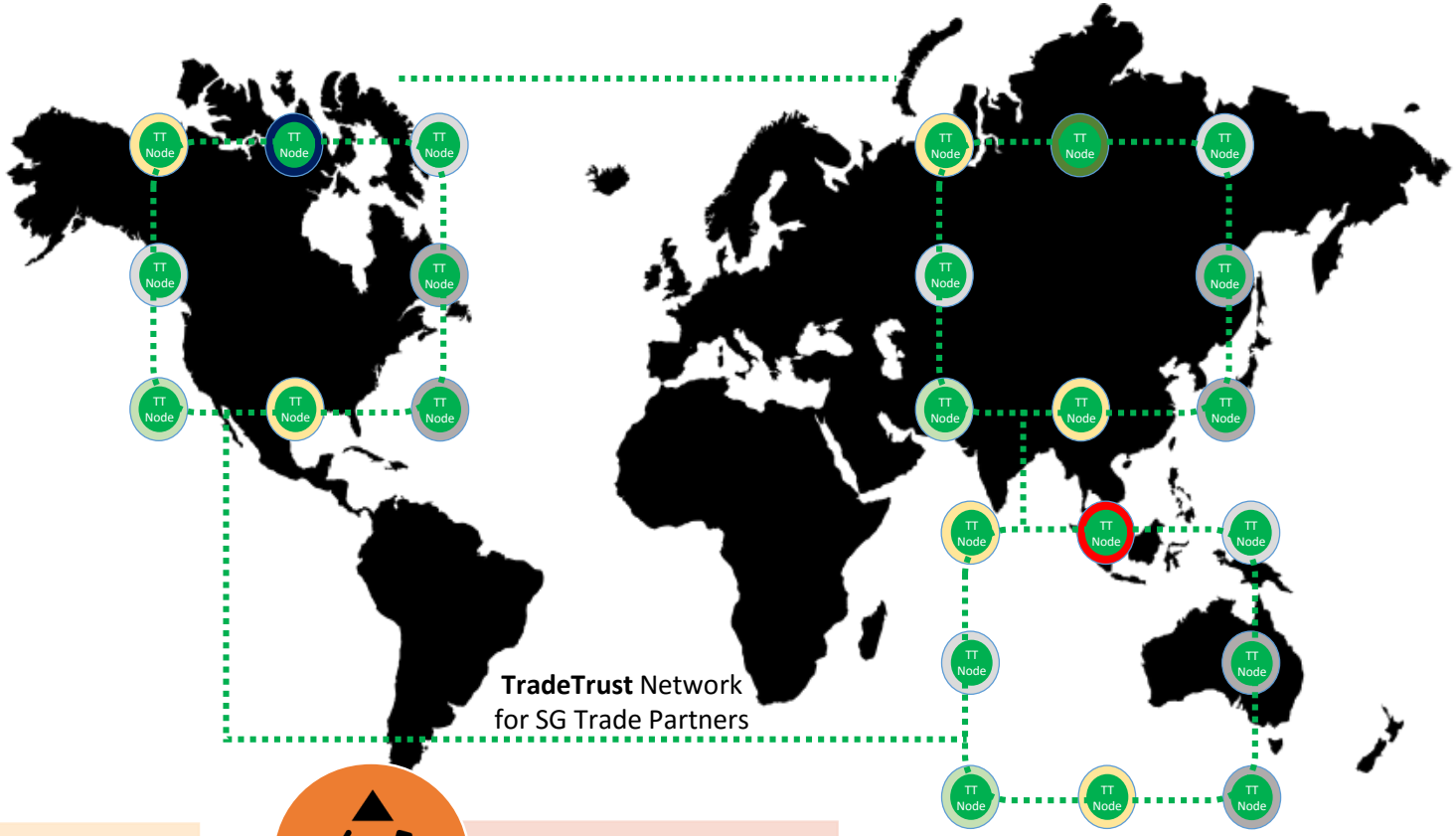
Interoperability is Vital To Integrate Different Digital Platforms in The Trade Ecosystem

SG:D EMPOWERING POSSIBILITIES

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

A NEUTRAL, TRUSTED & INTEROPERABLE NETWORK NEEDED





Neutral Network That Enforces Trade Secrecy Because Information Is Exchanged But Not Stored

DLT assures Provenance To **Create Trust**

Interoperability To Integrate Digital Platforms Based On Internationally Accepted Standards

SG:D EMPOWERING POSSIBILITIES

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

KEY COMPONENTS OF TRADETRUST TO DIGITALISE CROSS BORDER TRADE

Legal Recognition

- Incorporate UNCITRAL model law on electronic transferable records into Electronic Transactions Act by 2020
- Bilateral G2G recognition of electronic trade documents

Standards Development

- Technical standards to enable inter-system interoperability (ISO TC/307)
- Process standards to exchange electronic trade documents (UN/CEFACT)

Accreditation Structure

- Government-appointed accreditation service providers
- Service providers use the governance framework to perform accreditation

Distributed Ledger Technology Infrastructure (Part of Enhanced NTP)

Distributed Authority
Increase attractiveness to participate as only certain information will be captured

Synchronised
Activity on the DLT is automatically reflected across the network

Secure
Data cannot be changed once committed to the system

Smart transactions
Code can be added to transactions that allows autonomous execution of functions once predefined conditions are met

Improve operational efficiency across the supply chain

Facilitate trade & trade finance

Grow new value-added services
(e.g. automation of payment based on real-time shipment status)

SG:D EMPOWERING POSSIBILITIES

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

BACKGROUND OF UNCITRAL MODEL LAW ON ELECTRONIC TRANSFERABLE RECORDS (ETRS)

UN Convention on the Use of Electronic Communications in International Contracts (2005) (Electronic Communications Convention)

The Electronic Communications Convention aims at facilitating the use of electronic communications in international trade by assuring that contracts concluded and other communications exchanged electronically are as valid and enforceable as their traditional paper-based counterparts.

ETRs were **excluded** from the scope of the Electronic Communications Convention as time was needed to develop **legal and technical solutions.**

Electronic Communications Convention is cited in the Singapore Australia FTA (e-Commerce chapter)

United Nations Commission on International Trade Law (UNCITRAL) Working Group (2012 – 2017)

Harmonisation of rules on the legal recognition of ETRs on a technologically neutral basis and functional equivalent approach

UNCITRAL Model Law on Electronic Transferable Records (MLETR) (2017)

UNCITRAL adopts MLETR in Jul 2017 followed by adoption by the UN General Assembly in Dec 2017

BENEFITS OF MUTUAL RECOGNITION AND INTEROPERABILITY OF ETRS

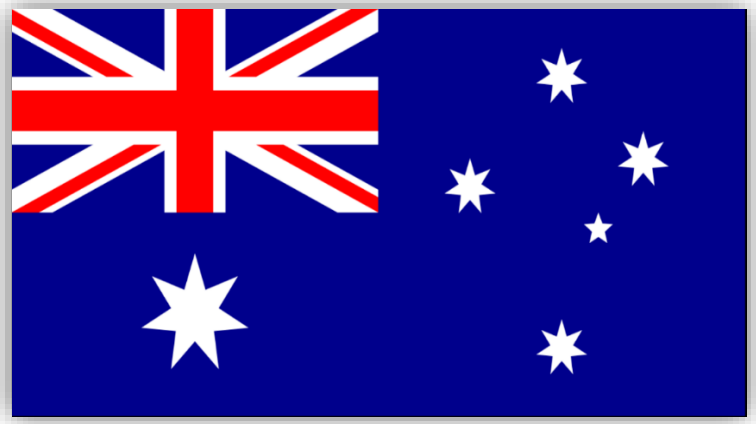
Opportunities for Singapore, Australia and ASEAN members to explore interoperability of ETRs

Many countries still in early stages of assessing the MLETR, Singapore included.

MLETR provides the best chance to date for cross border use of ETRs

Mutual recognition and interoperability of ETRs will being numerous benefits to the shipping and logistics industry, including:

- Lowering cost of financing
- Reducing risk of mis-delivery
- Enhancing security



SG:D EMPOWERING POSSIBILITIES

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

TRADETRUST FRAMEWORK & INFRASTRUCTURE TO ENHANCE TRADE CONNECTIVITY

Digital Ecosystems Co-Development, SME Adoption & Digitalisation

GeTS · CCNhub · PSA CALISTA

Commercial Applications/Platforms/Ecosystems

Trade Trust Framework (Standards, Semantics, Legal)
e.g. Standards & Semantics - e-Bill of Lading, e-Certificate of Origin, e-Invoice, Legal – ETA and MLETR

Domain Specific Standards Development
- Commercial Measures
- Trade Finance & Settlement
- Transport & Logistics
- Regulatory Compliance

Cross-domain Interoperable Framework
- Inter-ledger Interoperability
- Resource Discovery
- e-Notary Services
- Legal (ETA/ETR Model Law)

Technical Infrastructure
- Trade Event Registry
- Smart Contracts
- Master Chain

National Single Window

Interoperability to integrate digital platforms based on internationally accepted standards

Neutral Network that enforces trade secrecy because information is exchanged but not stored

A set of Governance & Legal Frameworks, Protocol Standards, and Infrastructure to facilitate exchange of trusted digital documents

Business-led
- Business Innovation

Govt-led
- Standards Devt
- UN/CEFACT
- Cross-border Recognition
- United Nations UNCITRAL
- UNITED NATIONS ESCAP
- Technical Implementation

SG:D EMPOWERING POSSIBILITIES · INFOCOMM MEDIA DEVELOPMENT AUTHORITY

CALL TO ACTION

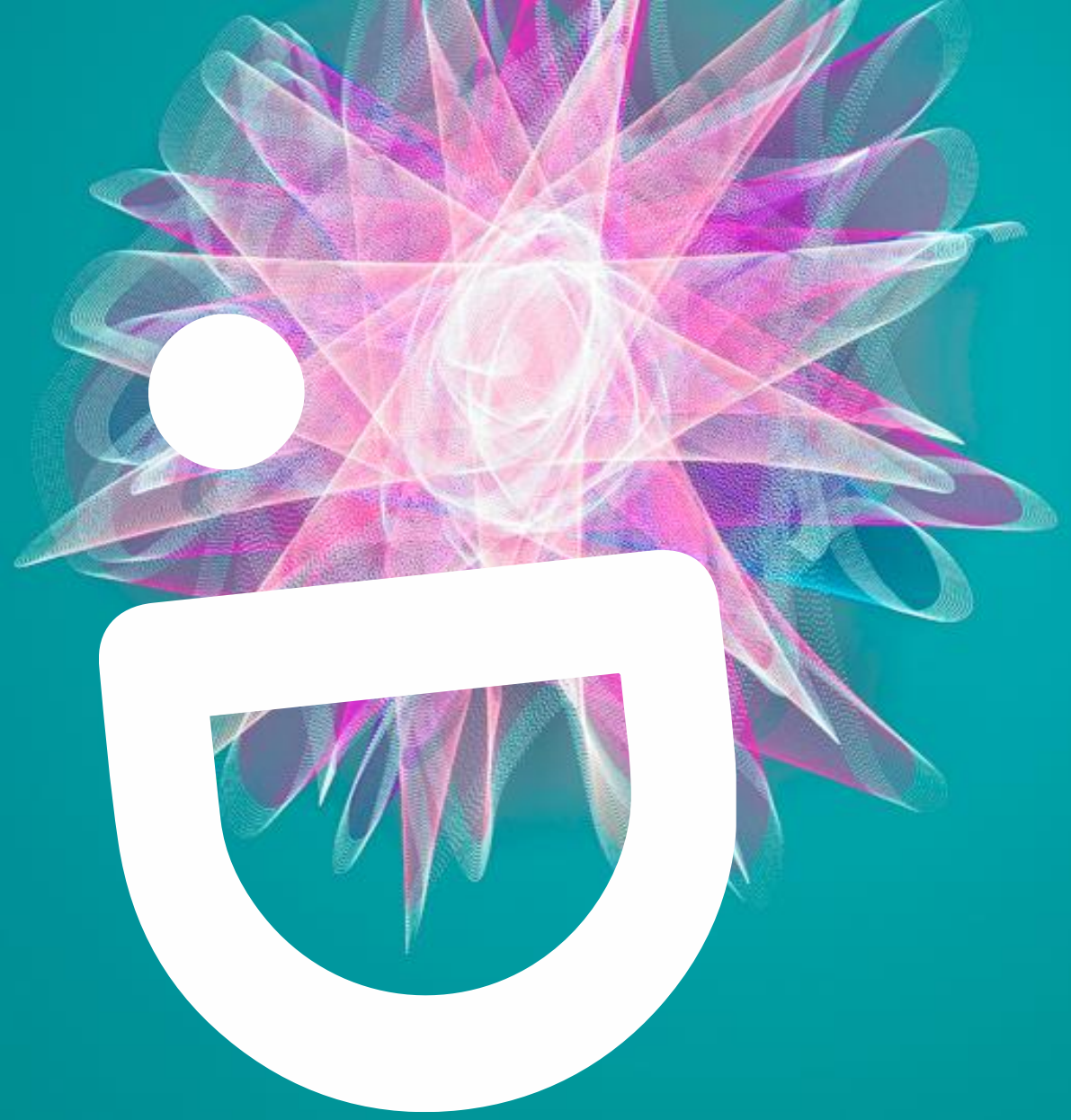
Participate In **Future Pilots**
To **Demonstrate Value** Of Trade Documents Digitalisation

- Identify potential industry partners
  (Shippers, Carriers, Consignees, Banks, Insurers)

- Select a specific trade route for technical trials and demonstrations

- Interested partners can register their interest with IMDA

MPA SINGAPORE
INFOCOMM MEDIA DEVELOPMENT AUTHORITY



Thank You

new_soon_tee@imda.gov.sg

SG:D
EMPOWERING POSSIBILITIES

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

Country Presentation 1: Cambodia

Mr Heng Mara

Ministry of Posts and Telecommunications

WORKSHOP ON ASEAN-Australia Digital Trade

16-17 Oct 2018 | Sydney

Cybersecurity in Cambodia

Heng Mara
Deputy Director of ICT Security Department
Ministry of posts and telecommunications
Email : mara-heng@mptc.gov.kh
Fingerprint : D96D B67D EDD1 F189 447E 534F 4328 4EF7 8795 FCB3

Content

1. Digital Statistic in Cambodia
2. Organization Structure
3. Cambodia ICT Policy 2020
4. Challenge

Cambodia digital Statistic

DIGITAL CAMBODIA STATISTIC

18.2 million

Mobile Subscriber by Apr 2018
Cover around 100% urban

121.5 %

Mobile
Penetration rate by 2017

10.9 million

Internet Subscription
Penetration rate around 72%
By Apri 2018

25 Capitals and Provinces

Almost 57.5% of Population
by Jan-2018

DIGITAL CAMBODIA STATISTIC

36,631 km

CFOCN=13,031km
Viettel(Cambodia)= 22,000 km
TC = 1,600km

2 Submarines cable infra. in 2017

MCT by Telco-Tech
AAE-1 by Heyroute

100 %

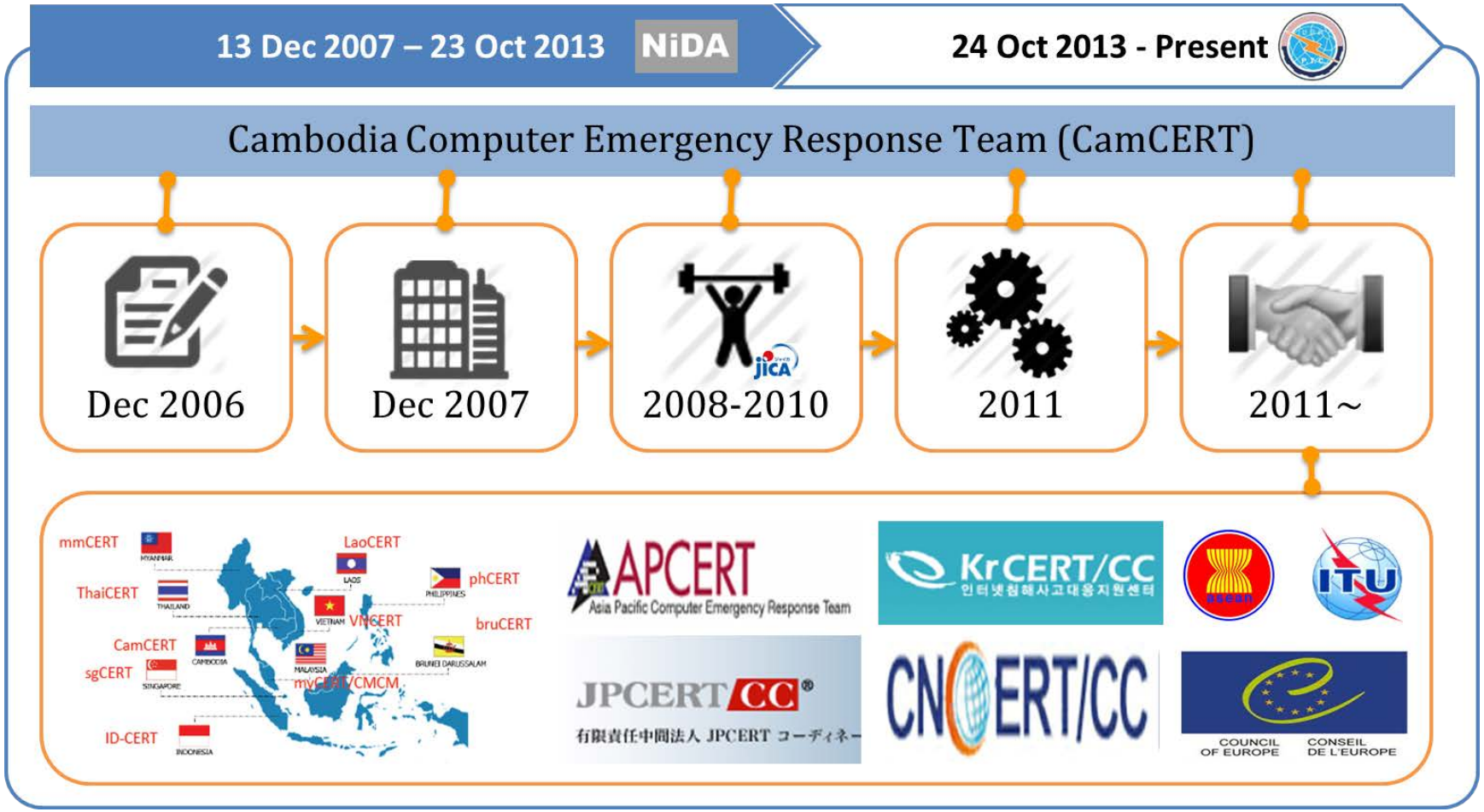
Broadband coverage by 2020
In urban and **70%** in rural

10 %

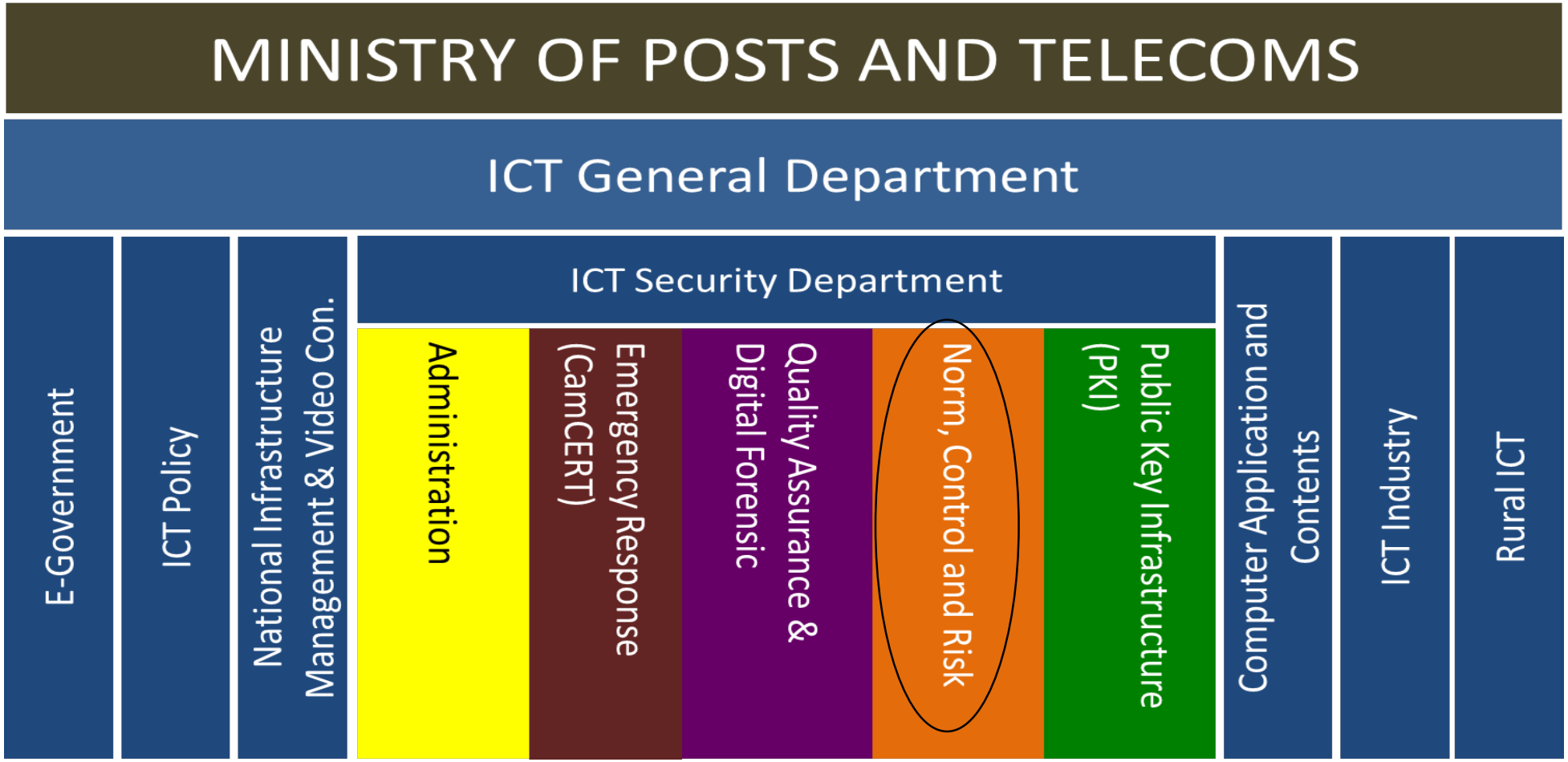
Internet of Things (IoT) by 2020

Organization Structure

Organization Structure Change



Organization Change(ICT Security Dep.)



T-ICT Related Framework

ICT Master Plan: Finished in 2014
Detail: http://www.mptc.gov.kh/site/detail/241

Telecom Law: Adopted by The Royal Degree in Dec 2015

T-ICT Policy 2020: Has been endorsed by the royal government of Cambodia on April 2016

Cambodia E-government Strategic Plan (2018-2023): is being drafted

E-Commerce Laws: On Going (MOC), Digital Signature sub degree Adopted

Cyber Crime Law: On Going (MOI)

Cambodia ICT Policy 2020

Vision:

"Toward ICT Connectedness and Readiness"

Goals:

To provide vision, policy framework, coordination framework and institutional arrangment for Telecommunication and ICT development in Cambodia .

To address structural challenges and enhance business and investment enviroment in Telecommunication and ICT sectors.

To provide interlock measures and specific interventions as needed between 2015 to 2020.

Cambodia ICT Policy 2020

1. Strengthening the Foundation of Telecom/ICT Development

- Policy and Legal Framework
- Telecom/ICT infrastructure Development
- Bridging Digital Divide
- Human Resource Development and R&D

2. Strengthening ICT Security and Developing Industry

- Strenthening ICT Security
- Developing ICT Industry

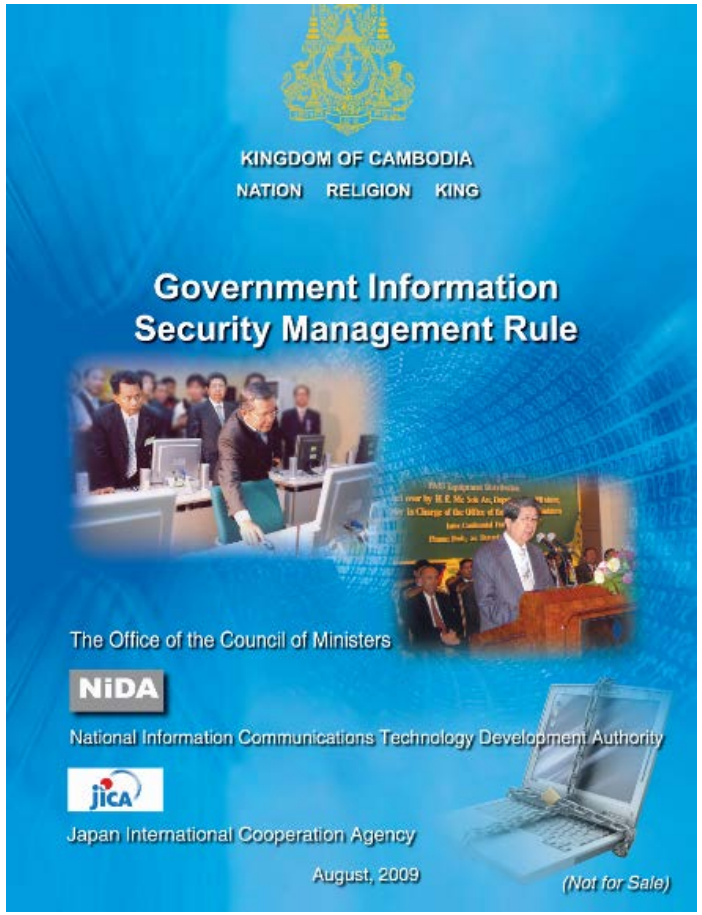
3. Promoting ICT Usage

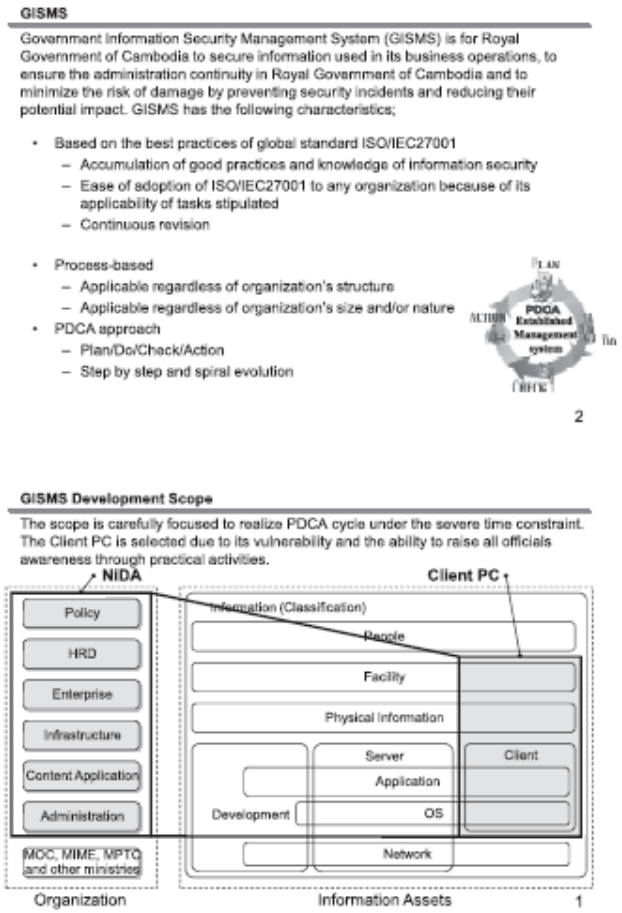
- Developing and Promoting the use of e-Government application
- Promoting e-Commerce
- Promoting the use of ICT for disaster relief and environmental protection

Enhance ICT security and develop ICT

- ✓ Raise public awareness on ICT security.
- ✓ Develop and implement ICT security technical guidelines, standards, and best practices.
- ✓ Develop national technical framework on ICT security.
- ✓ Enhance the capacity of CamCERT and the security of government websites.
- ✓ Establish digital forensic laboratory and national public key infrastructure.
- ✓ Identify and establish mechanism to protect critical information infrastructure.
- ✓ Enhance national and international collaboration and cooperation on ICT security

Experince- GISMS based on ISO 27001





GISMS

Government Information Security Management System (GISMS) is for Royal Government of Cambodia to secure information used in its business operations, to ensure the administration continuity in Royal Government of Cambodia and to minimize the risk of damage by preventing security incidents and reducing their potential impact. GISMS has the following characteristics;

- Based on the best practices of global standard ISO/IEC27001
  - Accumulation of good practices and knowledge of information security
  - Ease of adoption of ISO/IEC27001 to any organization because of its applicability of tasks stipulated
  - Continuous revision
- Process-based
  - Applicable regardless of organization's structure
  - Applicable regardless of organization's size and/or nature
- PDCA approach
  - Plan/Do/Check/Action
  - Step by step and spiral evolution

2

GISMS Development Scope

The scope is carefully focused to realize PDCA cycle under the severe time constraint. The Client PC is selected due to its vulnerability and the ability to raise all officials awareness through practical activities.

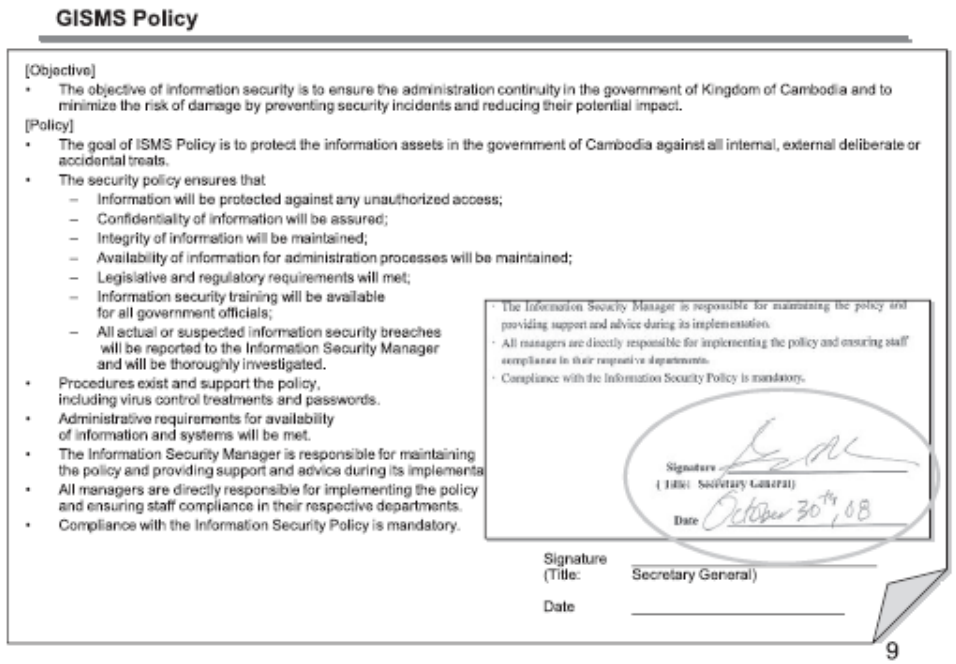
NiDA — Client PC

Policy
HRD
Enterprise
Infrastructure
Content Application
Administration
MOC, MIME, MPTC and other ministries

Information (Classification)
People
Facility
Physical Information
Server
Client
Application
Development
OS
Network

Organization — Information Assets

1



GISMS Policy

[Objective]

- The objective of information security is to ensure the administration continuity in the government of Kingdom of Cambodia and to minimize the risk of damage by preventing security incidents and reducing their potential impact.

[Policy]

- The goal of ISMS Policy is to protect the information assets in the government of Cambodia against all internal, external deliberate or accidental treats.
- The security policy ensures that
  - Information will be protected against any unauthorized access;
  - Confidentiality of information will be assured;
  - Integrity of information will be maintained;
  - Availability of information for administration processes will be maintained;
  - Legislative and regulatory requirements will met;
  - Information security training will be available for all government officials;
  - All actual or suspected information security breaches will be reported to the Information Security Manager and will be thoroughly investigated.
- Procedures exist and support the policy, including virus control treatments and passwords.
- Administrative requirements for availability of information and systems will be met.
- The Information Security Manager is responsible for maintaining the policy and providing support and advice during its implementa
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.
- Compliance with the Information Security Policy is mandatory.

- The Information Security Manager is responsible for maintaining the policy and providing support and advice during its implementation.
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.
- Compliance with the Information Security Policy is mandatory.

Signature
(Title: Secretary General)
Date October 30th, 08

Signature
(Title: Secretary General)
Date

9

Awareness

Outreach campaign on Cybersecurity awareness

Gov't

students

Public

ICT Security Department

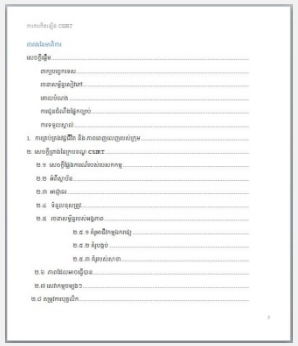
New Initiatives

- Training
  - Information Security Basic and information Security Management System(ISMS).
  - DNSSEC , IPv6…etc.
- Cyber exercise
  - Cambodia Cyber Sea Game 2015 (CTF)
  - Cyber Angkor 2017 (TTX)
  - Cambodia Cyber Contest 2018 (CTF)



New Initiatives

- Workshop
  - Digital Signature, Fintech
  - Strengthening Security in the Use of Telecommunication Networks - Information and Communication Technology,
  - E-Government Security [Targeted Government official]
- Translate Establishing a CSIRT Book



Challenge

- Leak of Human resource (Leak of Expert in Cybersecurity)
- Stakeholders engagement
- Leak of Law and regulation relate cybersecurity

THANKS YOU

Country Presentation 2: Singapore

Mr Joseph Gan

V-Key

Establishing Trust for Digital Trade

Joseph Gan

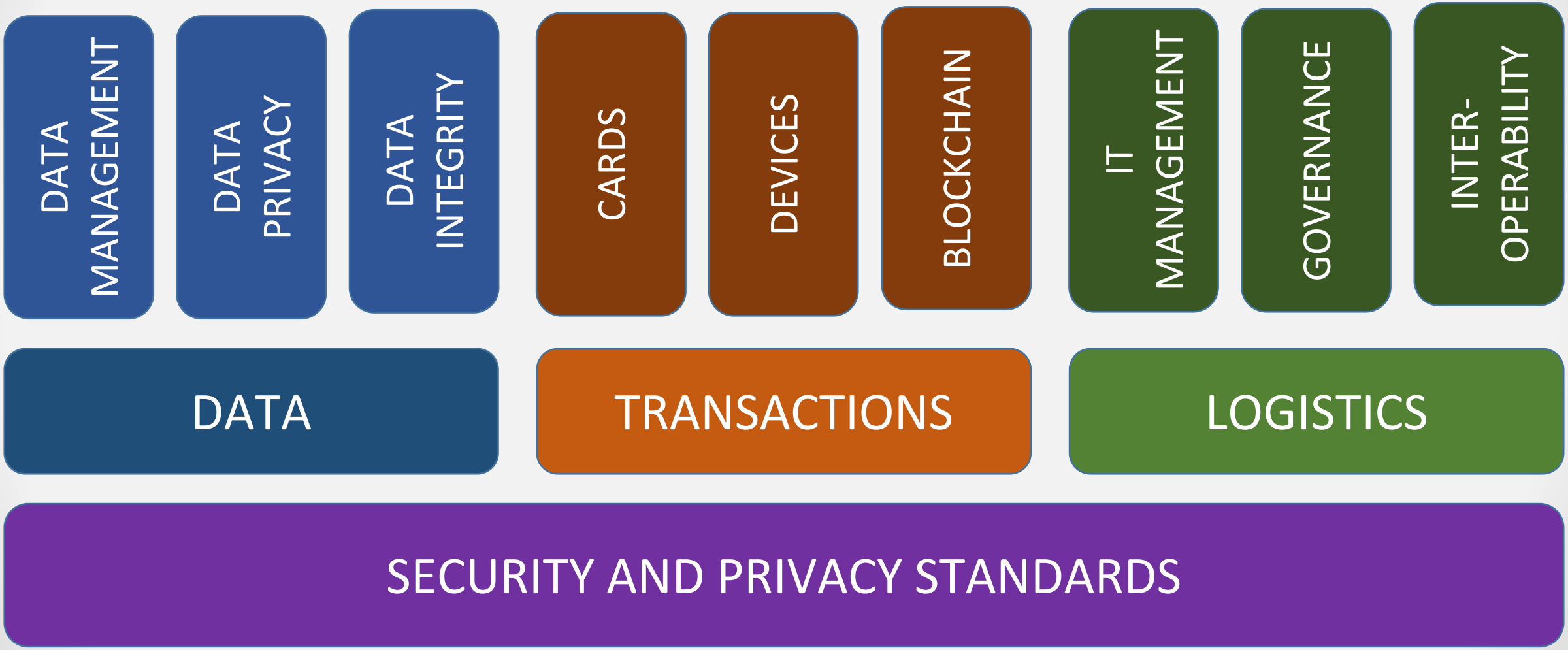
Chairperson, Security & Privacy Standards Technical Committee, Singapore

Standards and Singapore's National Digital Identity

A Cornerstone of Singapore's Smart Nation Vision

TRUST UNDERPINNING DIGITAL TRADE INITIATIVES

Establishing baseline security standards



iTSC Information Technology Standards Committee

GOVTECH SINGAPORE

SECURITY AND PRIVACY STANDARDS

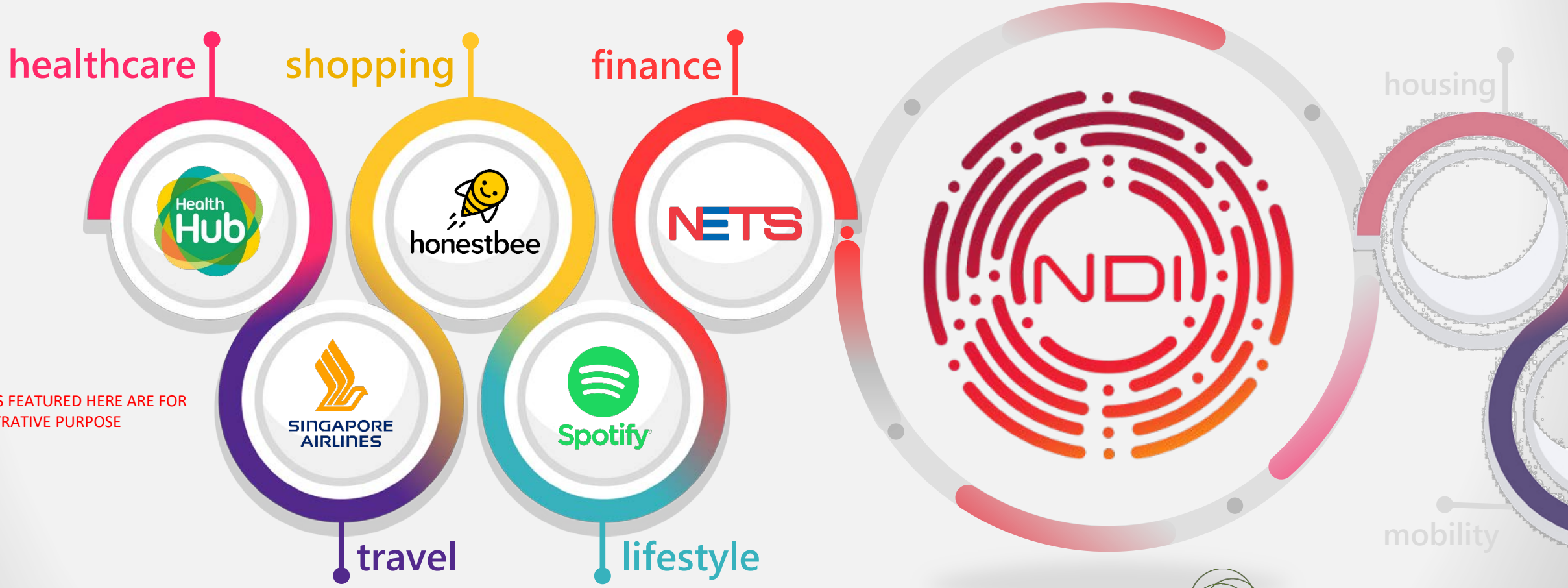
National Digital Identity

A unique digital identity for every Singaporean

iTSC Information Technology Standards Committee

GOVTECH SINGAPORE

Enabling private and public sectors in-country to build more digital services on a **common and universal trust framework**



LOGOS FEATURED HERE ARE FOR ILLUSTRATIVE PURPOSE

iTSC Information Technology Standards Committee

GOVTECH SINGAPORE

Trusted framework for facilitating cross-border **business-to-business** and **business-to-government** digital trade transactions

LOGOS FEATURED HERE ARE FOR ILLUSTRATIVE PURPOSE

iTSC Information Technology Standards Committee

GOVTECH SINGAPORE

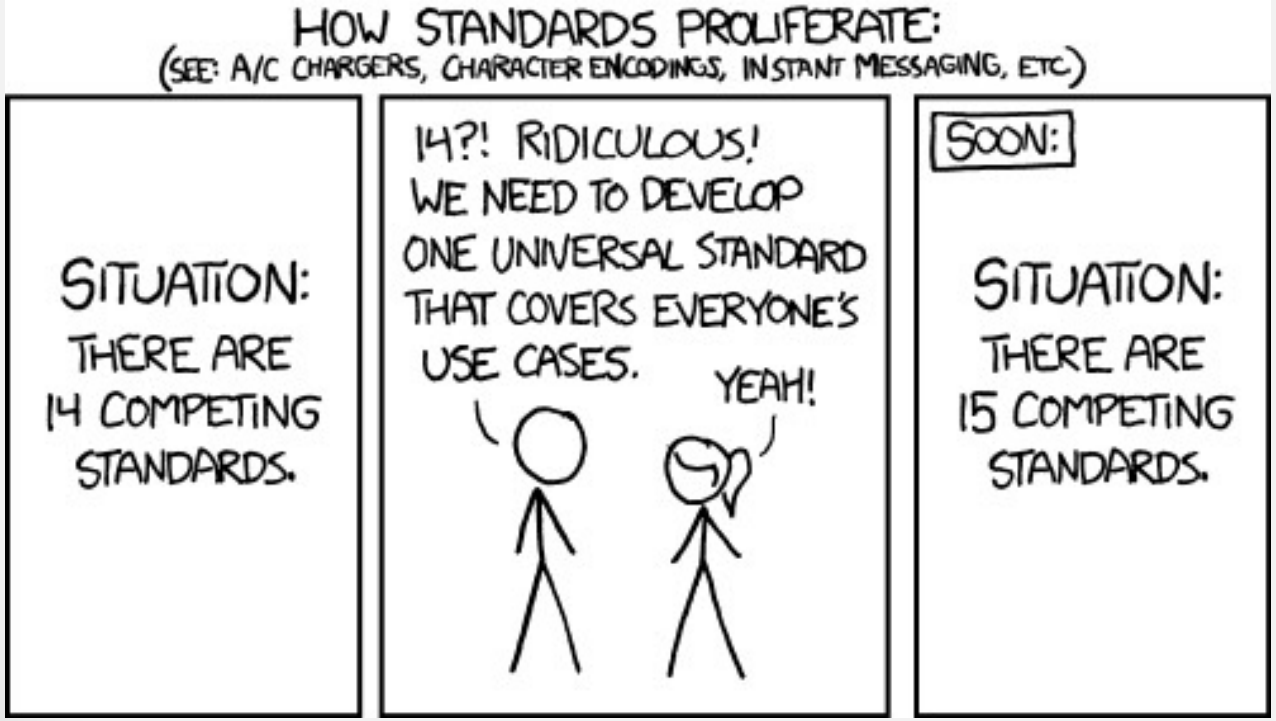
DIGITALISATION

primarily, is about facilitating the movement of data across boundaries

iTSC Information Technology Standards Committee

GOVTECH SINGAPORE

NDI NATIONAL DIGITAL IDENTITY



NDI is an open ecosystem that enables interoperability through open standards

iTSC Information Technology Standards Committee

GOVTECH SINGAPORE

Digital Enablers for the Digital Age

IDENTITY

Who are you?

AUTHORISATION

Do you have authority to access the data or services?

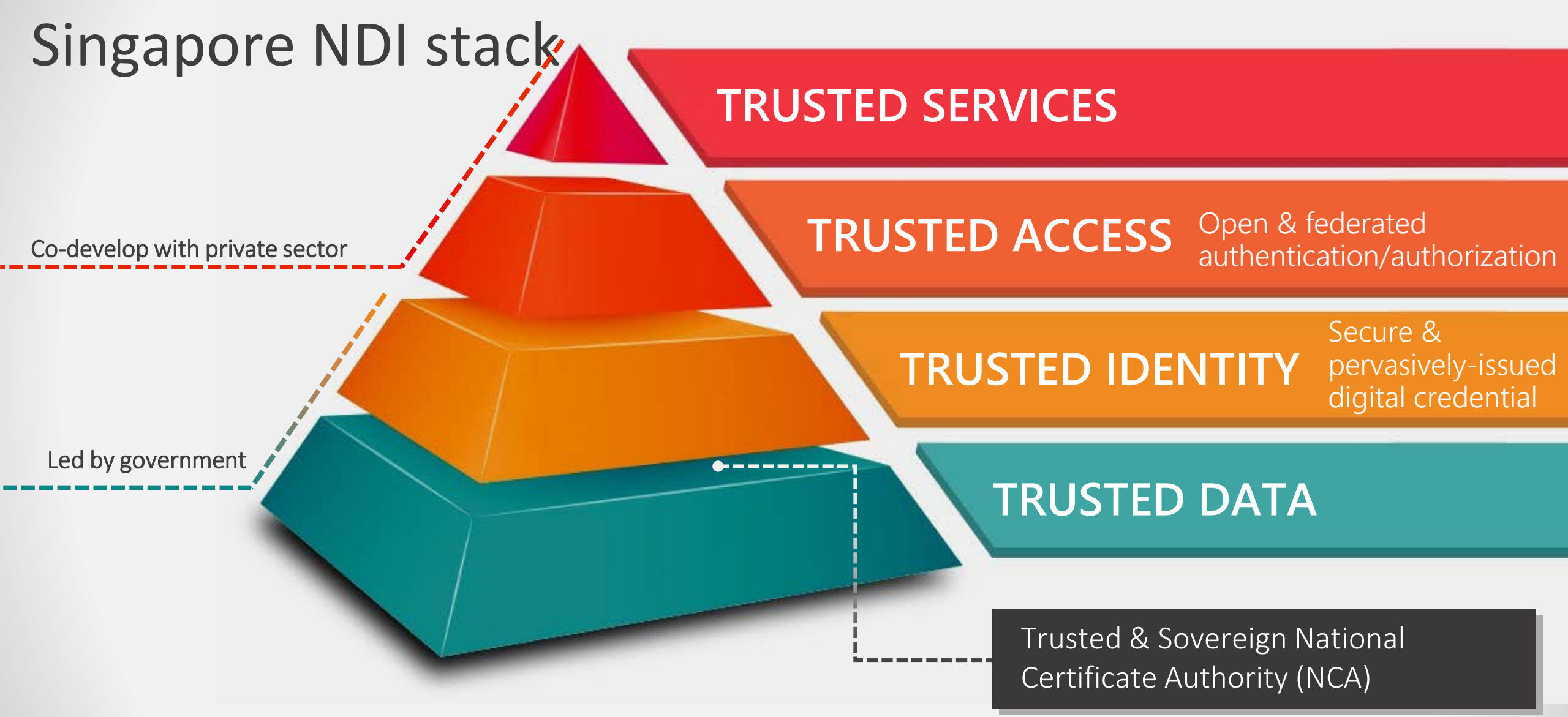
CONSENT

Do you allow me to pass on your data to another party?

iTSC Information Technology Standards Committee

GOVTECH SINGAPORE

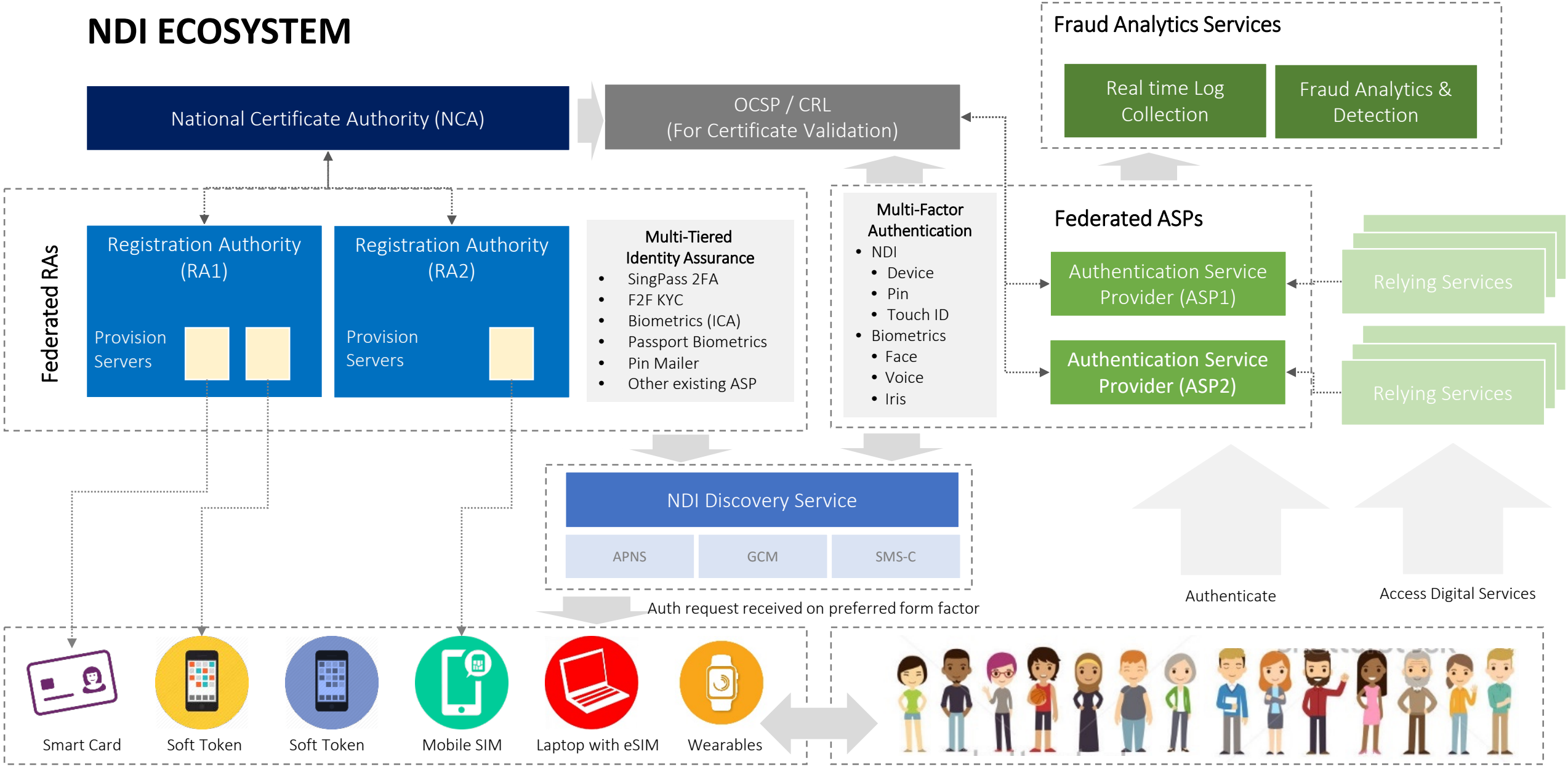
Singapore NDI stack



iTSC Information Technology Standards Committee

GOVTECH SINGAPORE

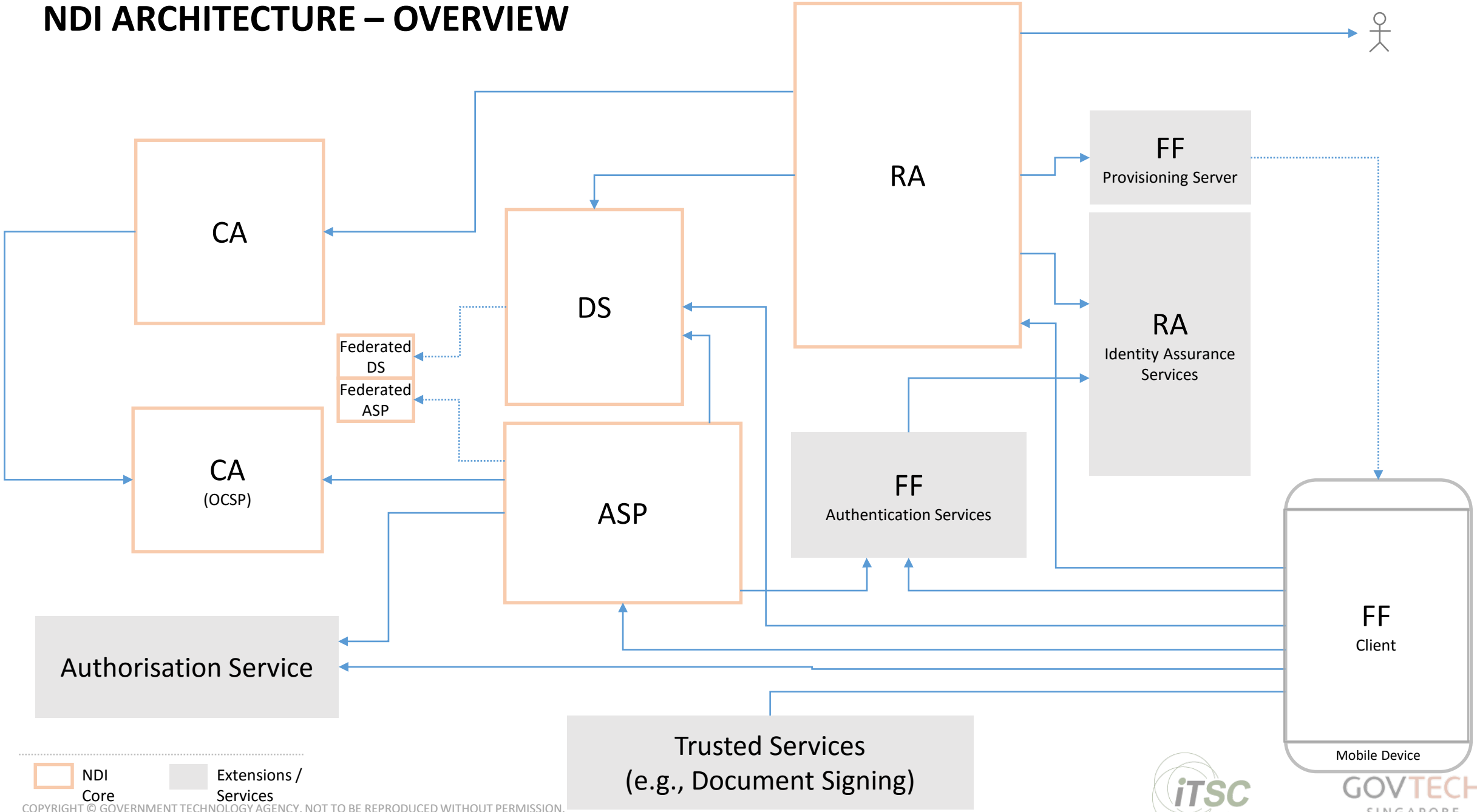
NDI ECOSYSTEM



iTSC Information Technology Standards Committee

GOVTECH SINGAPORE

NDI ARCHITECTURE – OVERVIEW



KEY DESIGN PRINCIPLES

OPEN

- Use of **open standards**
- Build **portable**, **reusable** components
- **Diversity** through support for multi-form-factors

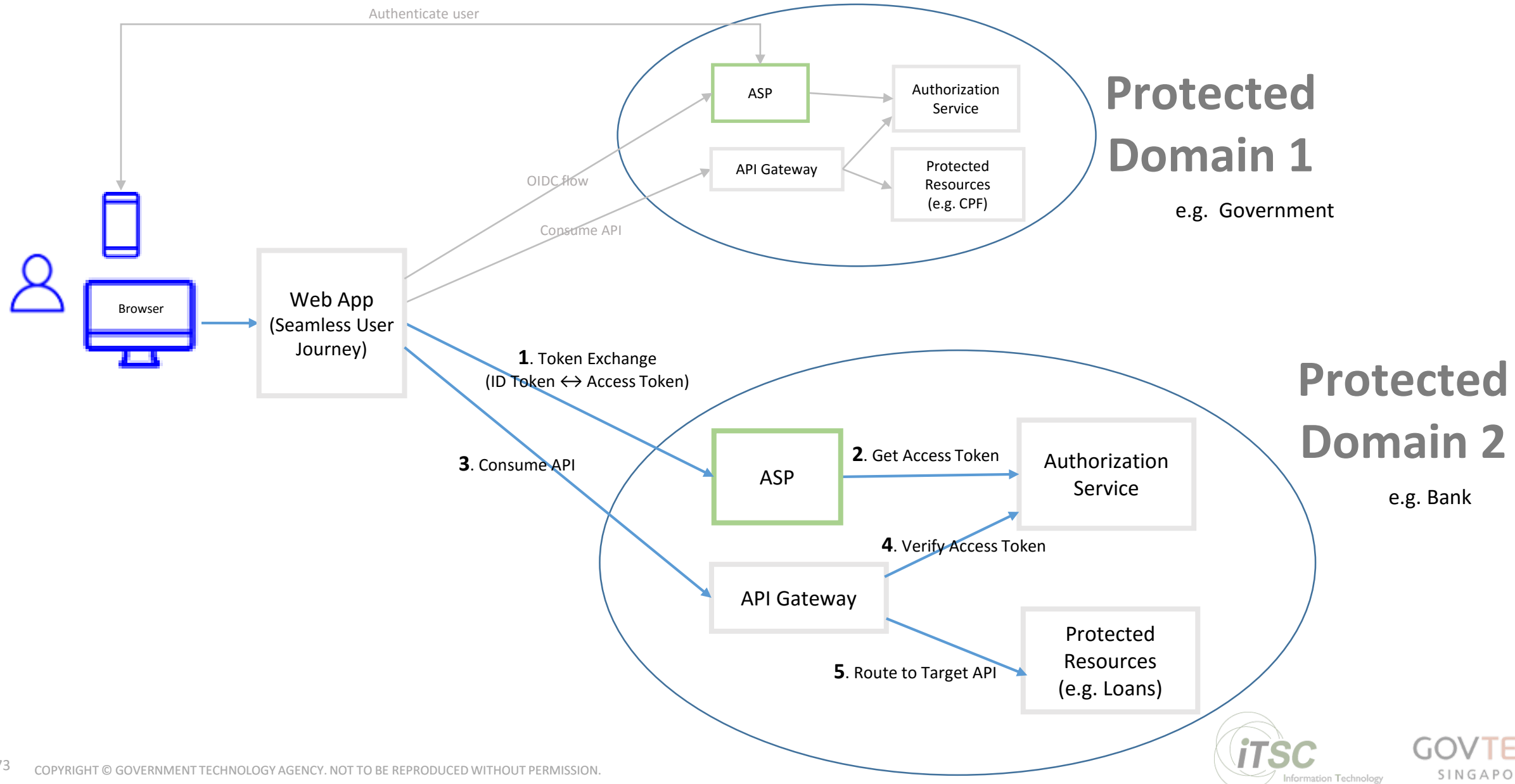
RESILIENT

- **Design for failure** – through use of loose coupling, distributed architecture, circuit-breakers
- Design for **zero downtime**
- Cloud-ready

SECURE

- **Security by design**
- **Borderless security model**
- Secure implementation of open standards

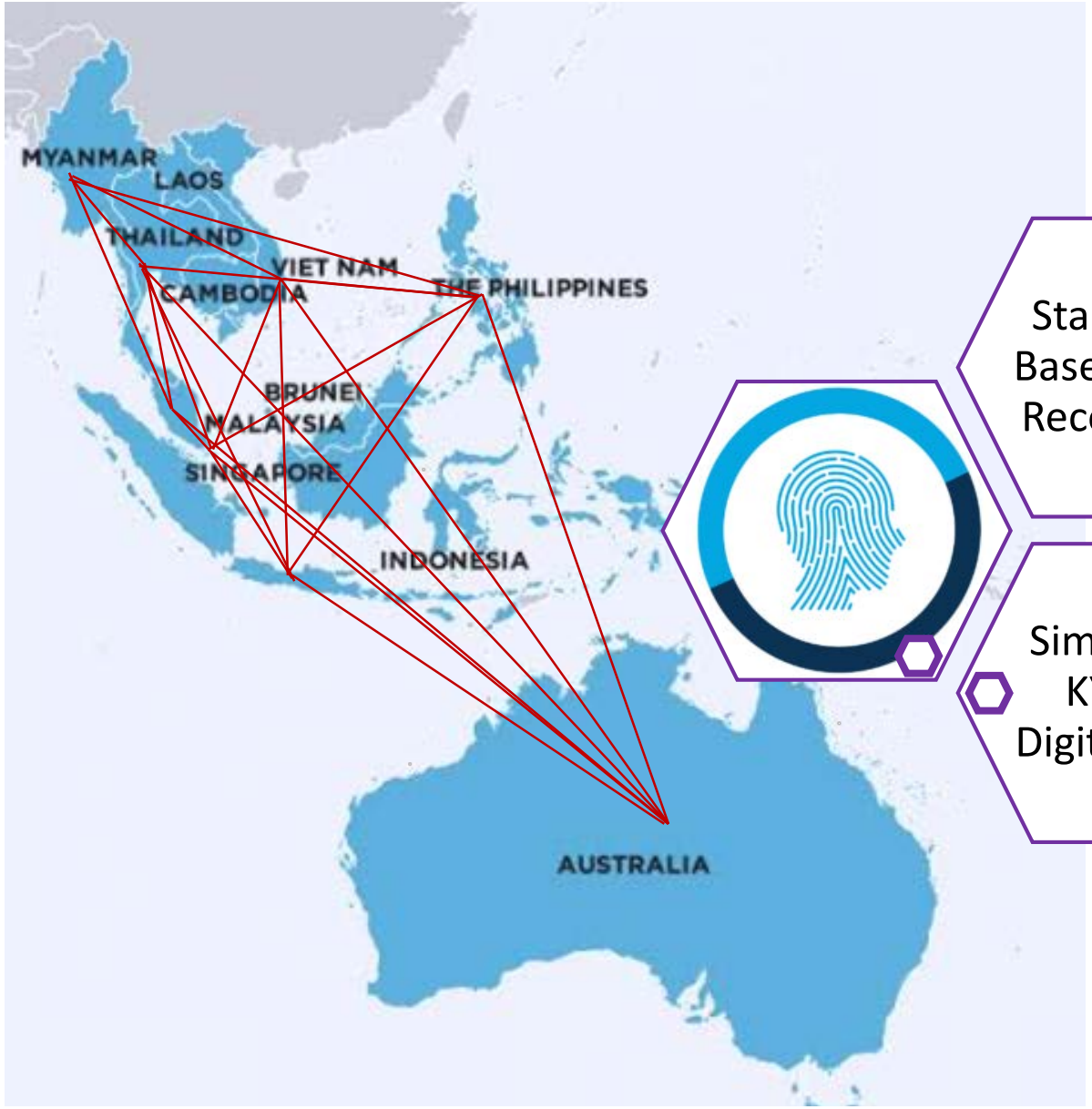
BEHIND THE SCENES – CROSS DOMAIN / CROSS BORDER AUTHORISATION



iTSC Information Technology Standards Committee

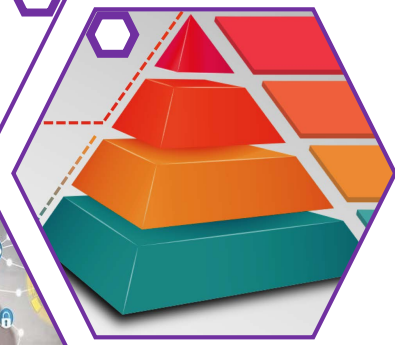
GOVTECH SINGAPORE

TRUSTED DIGITAL IDENTITIES FOR SUPPORTING TRADE



Standards-Based Cross-Recognition

Flexible Trust Framework



Federated Digital Transactions

Simplifying KYC for Digital Trade

iTSC Information Technology Standards Committee

GOVTECH SINGAPORE

DEVELOPING THE DIGITAL IDENTITY STANDARDS

Developing Technical Reference

Oct 2018 – June 2019
Singapore

Designed initially for internal Singapore usage

Discussions on relevant trade standards

July 2019 – Dec 2019
ASEAN-Australia engagement

Standards for collaborative digital trade platform

Possible new ISO/IEC standardization process

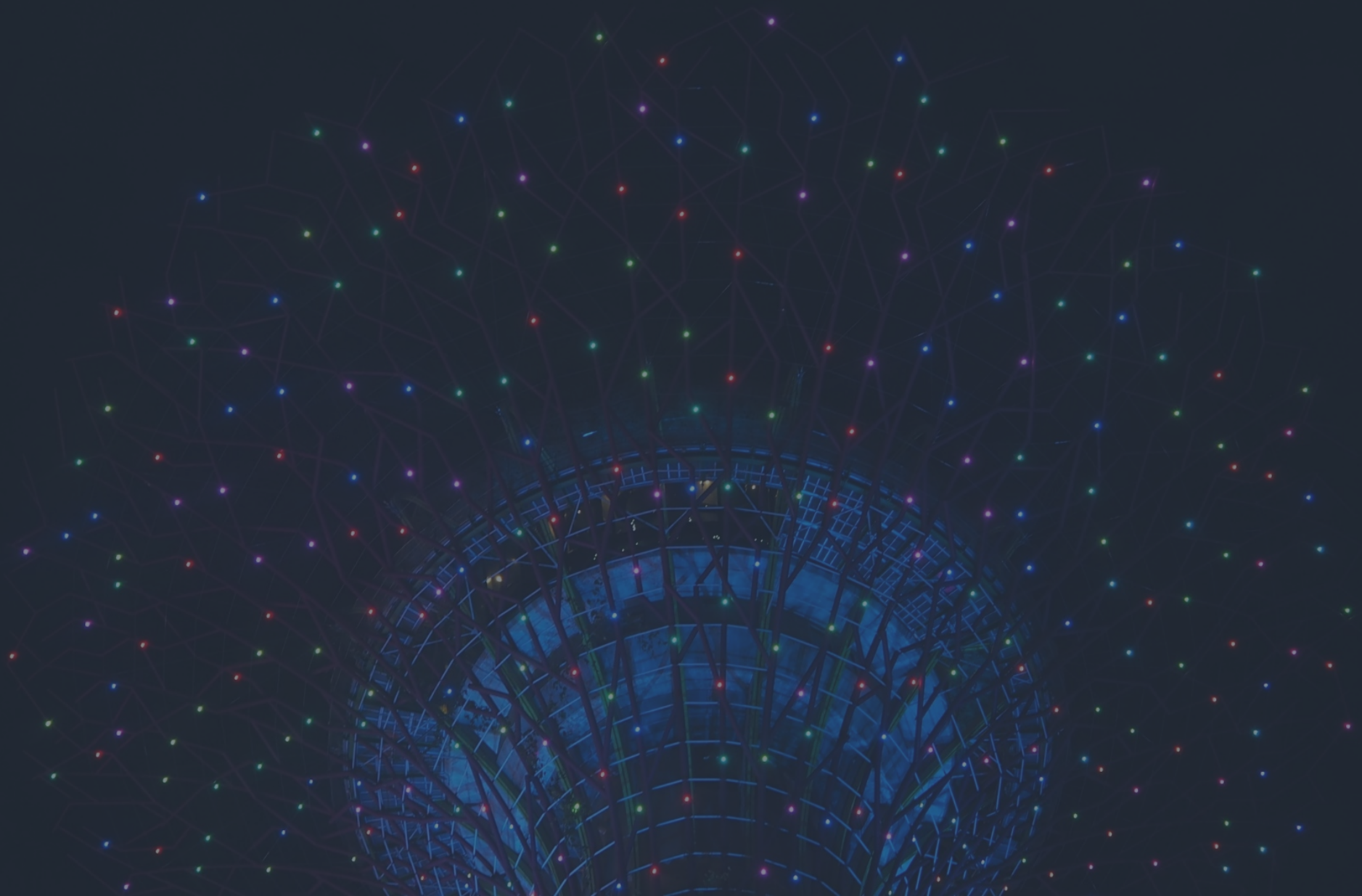
Jan 2020 onwards
Global engagement

Focus on cross-recognition with other regions, e.g. EU

iTSC Information Technology Standards Committee

GOVTECH SINGAPORE

THANK YOU



Country Presentation 3: Malaysia

Mr Aisharuddin Nuruddin

Malaysian Communications and Multimedia Commission

INFORMATION AND NETWORK SECURITY STANDARDS IN MALAYSIA

Digital Trade Standards Workshop

Sydney, Australia

Malaysian Communications and Multimedia Commission (MCMC)

MCMC is a regulatory agency that regulates based on

- Communications and Multimedia Act 1998 (CMA)
- Postal Services Act 2012 (PSA)
- Digital Signature Act 1997 (DSA)
- Strategic Trade Act 2010 (STA)

Other roles include, but not limited to the following

- to implement and promote the Government's national policy objectives for the communications and multimedia sector
- overseeing regulatory framework for the converging telecommunications and broadcasting industries and on-line activities

The 10 National Policy Objectives for Communications & Multimedia Industry in Malaysia	
1. Creating a Global Hub	6. Promote Access and Equity
2. Building a Civil Society	7. Creating Robust Application Environment
3. Nurturing Local Content and Culture	8. Facilitating Efficient Allocation of Resources
4. Ensuring Long Term Benefits for the End Users	9. Developing Industry Capabilities
5. Nurturing User Confidence	10. Promoting Secure and Safe Networking

Malaysian Technical Standards Forum Berhad (MTSFB)

Key role: **Development of Technical Codes / Voluntary Industry Codes (VIC)**

Technical codes may be prepared by the MTSFB either:-

- **on its own initiative; or**
- **upon request by the Commission**

Compliance is voluntary

Shall not be effective until registered by the Commission

Malaysian Technical Standards Forum Bhd

The company

- A company limited by guarantee incorporated on 8 June 2004
- Designated as Technical Standards Forum by the Commission on October 2004 pursuant to Section 94 and Section 184 of the CMA
- Develop and recommend codes or standards to the Commission

Membership

- Ordinary or Associate Membership
- Open to operators, manufacturers, vendors, universities, R&D organizations, government agencies or non-government agencies and other interested parties

Standardization

- 22 Working Groups
- Standardization on areas of network facility, network equipment/terminal and network technology

MTSFB's Working Groups

Working Groups

Network Facility

- Broadcasting Network Facility (BNF WG)
- Fixed Network Facility (FNF WG)
- Green Information & Communication Technology (GICT WG)
- Installation of Network Facility-Regulatory (INF-R WG)
- Occupational Safety & Health (OSH WG)
- Radiocommunications Network Facility (External) [RNI (Ex) WG]
- Radiocommunications Network Facility (Internal) [RNI (In) WG]
- Wireless Industry Emission (WIE WG)

Network Equipment / Terminal

- Fixed Terminal (FT WG)
- Multimedia Terminal (MMT WG)
- Satellite Broadcast Terminal (SBT WG)
- Wireless Terminal (WT WG)

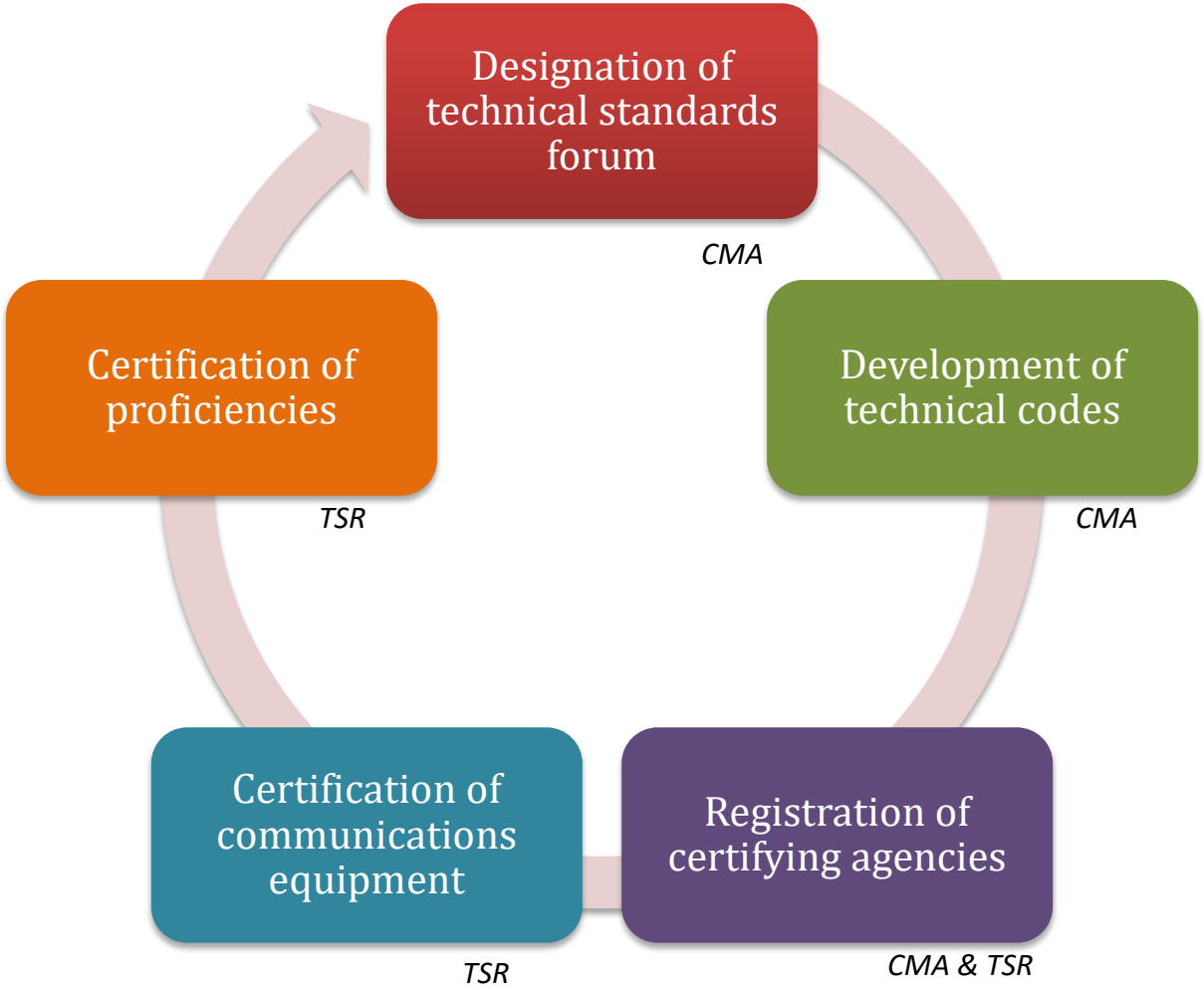
Network Technology

- Digital Radio Broadcast (DRB WG)
- Digital Terrestrial Television (DTT WG)
- Future Networks (FN WG)
- International Mobile Telecommunications (IMT WG)
- Internet of Things (IoT WG)
- Internet Protocol Television (IPTV WG)
- Internet Protocol Version 6 (IPv6 WG)
- Powerline Communications (PLC WG)
- Security, Trust & Privacy (STP WG)
- TV White Space (WS WG)

Framework for Technical Standards

CMA 98
General framework for technical standards regulation

TSR 2000
Detailed procedural requirements, offences & penalties

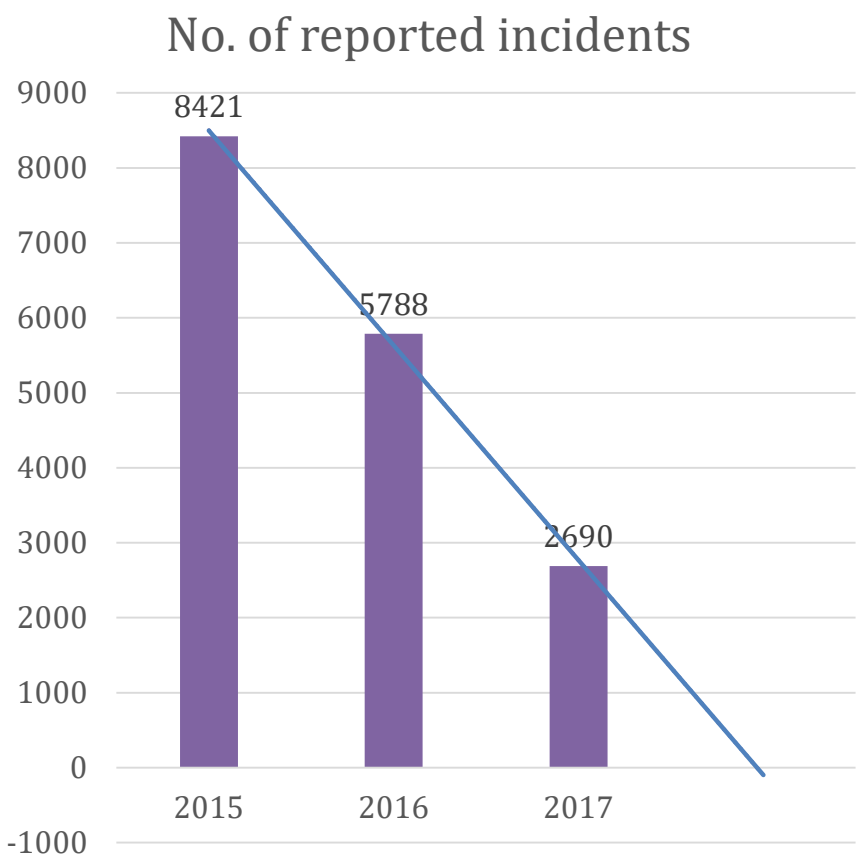


- TSR 2000 – Communications and Multimedia (Technical Standards) 2000
- CMA 98 – Communications and Multimedia Act 1998

Reported Security Incidents 2015-2017

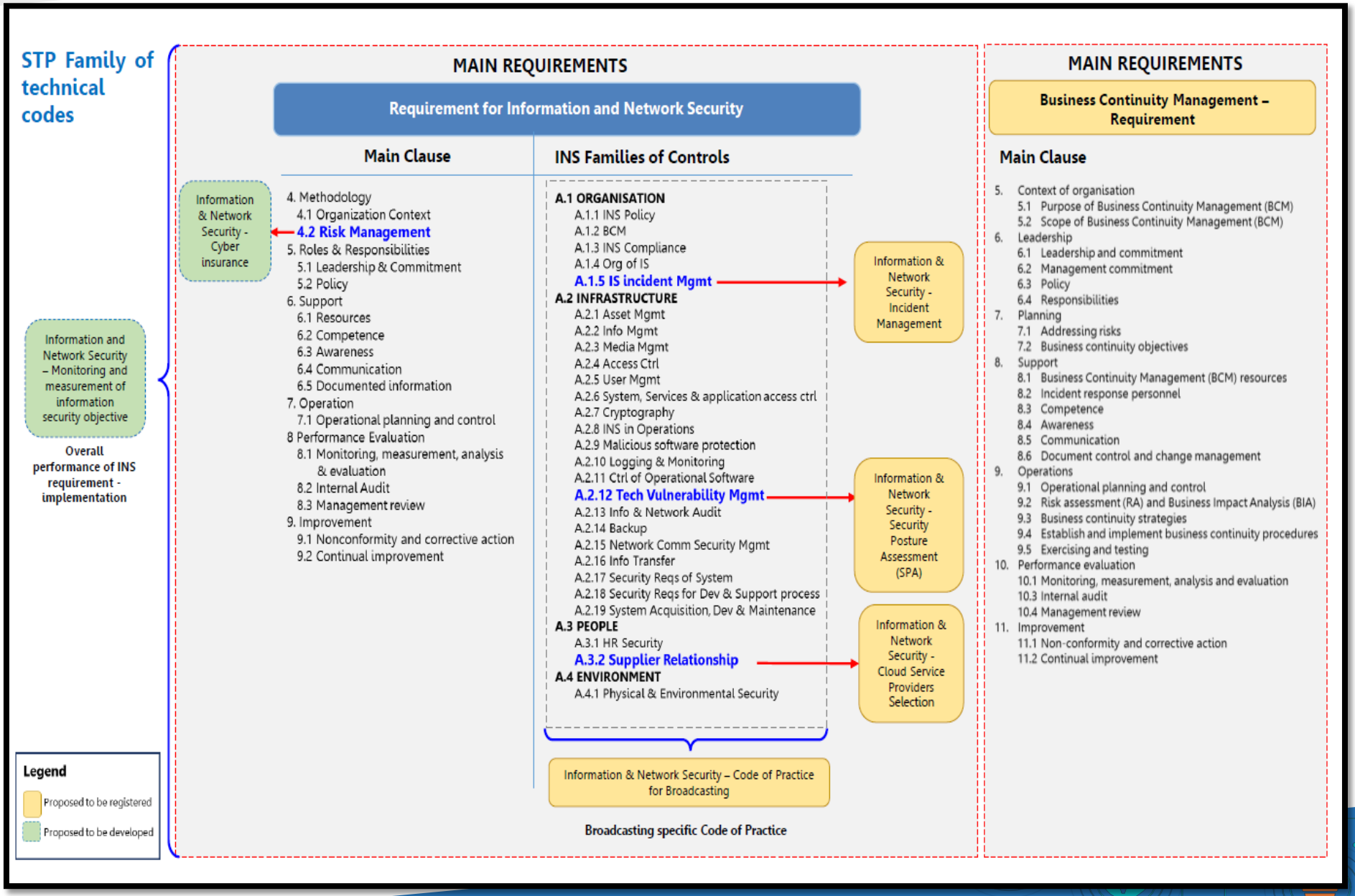
Categories	2017	2016	2015
Defacement	1,183	1,222	2,214
Fraud/Phishing	602	687	987
Malware	517	1,416	4,929
Network Security Attempts	338	2,451	191
Vulnerability	43	8	69
Intrusion	7	3	28
Denial of Service	0	1	3
Total	2,690	5,788	8,421

Reported security incidents based on categories from 2015-2017



Source: MCMC Network Security Centre

Security, Trust and Privacy (STP) Family of Technical Codes



Information and Network Security Technical Codes

1. **Requirements for Information and Network Security**
   - 2. Information and Network Security – Incident Management
   - 3. Information and Network Security – Security Posture Assessment (SPA)
   - 4. Information and Network Security – Cloud Service Providers Selection
   - 5. Information and Network Security – Code of Practice for Broadcasting
   - 6. Information and Network Security – Cyber Insurance (In Progress)
   - 7. Information and Network Security – Monitoring and measurement of information security objective (In Progress)

8. **Business Continuity Management - Requirements**

9. **Internet of Things (IoT) – Security Management**

Information and Network Security Technical Codes

1	Requirements for Information and Network Security	Requirements for Information and Network Security Management System (ISMS) implementation
2	Information and Network Security – Incident Management	Requirements in managing information security incidents to minimize the impact of security incidents through a proper incident management process
3	Information and Network Security – Security Posture Assessment (SPA)	evaluation criteria and the process to employ an external security assessor for an effective SPA programme
4	Information and Network Security – Cloud Service Providers Selection	Requirements for selecting cloud service provider for organizations in ensuring all security requirements are taken into account
5	Information and Network Security – Code of Practice for Broadcasting	Additional details of controls specific to broadcasting industry for the implementation of ISMS
6	Information and Network Security – Cyber Insurance (In Progress)	Requirements for the sharing of information between an insurer and insured party to prepare a cyber-insurance policy
7	Information and Network Security – Monitoring and measurement of information security objective (In Progress)	Requirements for measuring the effectiveness of system and controls or groups of information security controls

Information and Network Security Technical Codes

8	Business Continuity Management - Requirements	Requirements that support the implementation of the Business Continuity Management in an organisation
9	Internet of Things (IoT) – Security Management	General requirements for security and privacy protection in the IoT ecosystem

Technical Codes vs International/Industry Standards (1/2)

Technical Codes	International or Industry Standards	Remarks
Requirements for Information and Network Security	▪ ISO/IEC 27001 Information technology – Security techniques – Information security management systems - Requirements	Adapted from ISO/IEC 27001 by focusing on selected security domains.
Information and Network Security – Incident Management	▪ ISO/IEC 27035 Information technology – Security techniques – Information security incident management	Adapted from ISO/IEC 27035 and take into account category of incidents and implementation at the national practice.
Information and Network Security – Security Posture Assessment (SPA)	▪ ISO/IEC 27005 Information technology - Security techniques - Information security risk management ▪ ISO/IEC 27017 Information technologies – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services ▪ Open Source Security Testing Methodology Manual (OSSTMM) ▪ Open Web Application Security Project (OWASP)	Indigenous
Information and Network Security – Cloud Service Providers Selection	▪ ISO/IEC 27017 Information technologies – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services ▪ ISO/IEC 27036-4 Information technologies – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services ▪ ITU-T X.1601 Security framework for cloud computing ▪ ITU-T X.1641 Guidelines for cloud service customer data security ▪ ITU-T X.1642 Guidelines of operational security for cloud computing	Indigenous

Technical Codes vs International/Industry Standards (2/2)

Technical Codes	International or Industry Standards	Remarks
Information and Network Security – Code of Practice for Broadcasting	▪ ITU-T X.1051 & ISO/IEC 27011 Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations	Adapted from ISO/IEC 27002 and take into account implementation at the national practice.
Business Continuity Management - Requirements	▪ ISO 22301 Societal security -- Business continuity management systems -- Requirements	Adapted from ISO 22301 and take into account implementation at the national practice.
Internet of Things – Security Management	▪ ITU-T Y.4001 Common requirements of the Internet of Things	Adapted from ITU-T Y.4001 to focus on security management aspects.
Information and Network Security – Cyber Insurance	▪ ISO/IEC CD27102 Information technology - Security techniques - Information security management guidelines for cyber insurance	Adapted from ISO/IEC CD27102 to provide minimum requirements to suit the national practice.
Information and Network Security – Monitoring and measurement of information security objective	▪ ISO/IEC 27004 Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation	Adapted from ISO/IEC 27004 and take into account implementation at the national practice.

Next steps

The Technical Codes will be used by MCMC:

as a tool for assessment to gauge the implementation of relevant information and network security principles

To support the mandate by the Malaysian cabinet ("Critical National Information Infrastructure (CNII) entities of Malaysia to be certified under MS ISO/IEC 27001:2007 Information Security Management System (ISMS)")

- to ensure all CNII are ISMS certified.

Conclusion

Governments and businesses increasingly mandate their implementation

Standards help establish common security requirements and the capabilities needed for secure solutions

Standards are based on consensus and generally incorporate best practices and conformance requirements, their use typically results in improvements in quality

To support the 10 National Policy Objectives for Communications & Multimedia Industry in Malaysia

Thank You!

Question and Answer

Group Discussion

Standards Australia

Questions:

1. Do you agree/disagree with these issues raised?
2. What are we missing?
3. What do you want to hear more about?
4. Were there additional questions you didn’t get to ask?
5. Do you want to know more about how standards work or how to engage in them?
6. Are there partnership/relationships you already have that are helping tackle some of these core issues?

ISO/IEC JTC 1 Sub-committees and participation

Committee Designation	Committee Title	Australia (SA)	Brunei Darussalam (ABCI)	Cambodia (ISC)	Indonesia (BSN)	Lao PDR (DOSM)	Malaysia (DSM)	Myanmar (DRI)	Philippines (BPS)	Singapore (ESG)	Thailand (TISI)	Viet Nam (STAMEQ)
ISO/IEC JTC 1	**Information Technology**											
ISO/IEC JTC 1/SC 2	Coded character sets											
ISO/IEC JTC 1/SC 6	Telecommunications and information exchange between systems											
ISO/IEC JTC 1/SC 7	Software and systems engineering											
ISO/IEC JTC 1/SC 17	Cards and security devices for personal identification											
ISO/IEC JTC 1/SC 22	Programming languages, their environments and system software interfaces											
ISO/IEC JTC 1/SC 23	Digitally Recorded Media for Information Interchange and Storage											
ISO/IEC JTC 1/SC 24	Computer graphics, image processing and environmental data representation											
ISO/IEC JTC 1/SC 25	Interconnection of information technology equipment											
ISO/IEC JTC 1/SC 27	IT Security techniques											
ISO/IEC JTC 1/SC 28	Office equipment											
ISO/IEC JTC 1/SC 29	Coding of audio, picture, multimedia and hypermedia information											
ISO/IEC JTC 1/SC 31	Automatic identification and data capture techniques											
ISO/IEC JTC 1/SC 32	Data management and interchange											
ISO/IEC JTC 1/SC 34	Document description and processing languages											
ISO/IEC JTC 1/SC 35	User interfaces											
ISO/IEC JTC 1/SC 36	Information technology for learning, education and training											
ISO/IEC JTC 1/SC 37	Biometrics											
ISO/IEC JTC 1/SC 38	Cloud Computing and Distributed Platforms											
ISO/IEC JTC 1/SC 39	Sustainability for and by Information Technology											
ISO/IEC JTC 1/SC 40	IT Service Management and IT Governance											
ISO/IEC JTC 1/SC 41	Internet of Things and related technologies											
ISO/IEC JTC 1/SC 42	Artificial intelligence											

Lunch

Return at 1:15pm

Breakout Discussion Sessions

Breakout Group Questions:

‘What are the barriers preventing greater awareness of, participation in, adoption and use of international standards to support digital trade in ASEAN and Australia?’

‘How can ASEAN and Australia work together to address these barriers in a longer-term work program?’

Additional Questions

1. What are your top five priority actions that could be taken to address the leading issues in your country?

2. Which of the aspects identified of international standards (awareness, engagement, adoption or use) is the greatest challenge in your country? Why?

3. Are there any partners you are already working with to address some of these issues in your country?

Afternoon Tea/Networking Session

Return at 3:15pm

Report on Findings of Breakouts

Recommendations Discussion

Standards Australia

Workshop Summary

Standards Australia

Closing

Standards Australia