IoT Alliance Australia

Industry Briefing
Security Labelling Scheme for Smart Devices

26 August 2025

www.iot.org.au

IoT Alliance Australia

Agenda

Time	Topic
10:00 - 10:05	Opening remarks: Georgina Papoutsi, Department of Home Affairs
10:05 - 10:15	IoTAA introduction and program overview
10:15 – 10:40	Key design aspects
10:40 - 10:45	How to participate in co-design
10:45 - 10:55	Questions and feedback

Opening remarks

Georgina Papoutsi
Director, Secure Technology Section, Cyber Policy and Programs Branch, Department of Home Affairs

IoTAA overview

IoT Alliance Australia (IoTAA) the peak Australian industry body for IoT and AIoT

- Formed in 2016
- **Our vision:** a data smart Australia
- **Our mission:** to advance society through trusted, accessible, automated technology and data
- Our membership comprises suppliers, designers, manufacturers, communications service providers, hardware and software developers, IoT service providers, consultants, research, utilities, councils and government observers
- Collaborations and working relationships across industries and government:
  - Water, energy, manufacturing, cities, agriculture, skills
  - OAIC, ACCC, ACMA
  - Tech industry – AiiA, TCA, ACS
  - Standards – nominating entity and active participant across IoT (SC41), AI (SC42), Digital Twin (SC41), Security (SC27), smart manufacturing and sustainability

Objectives and outcomes

The **objectives** of the program are to:

- Co-design and implement an industry-led and internationally aligned voluntary labelling scheme for consumer-grade smart devices in Australia.
- Increase consumer awareness of the Government's proposed mandatory minimum standard for consumer-grade smart devices in Australia.

The **intended outcomes** of the program are:

- Increased consumer understanding and awareness of the security of products available in the Australian market
- Enable consumers to make informed decisions about the level of security when purchasing smart devices
- Align the Australian smart device market more closely with international best practice
- Greater adoption of security and privacy protections (secure-by-design features) by manufacturers of smart devices.

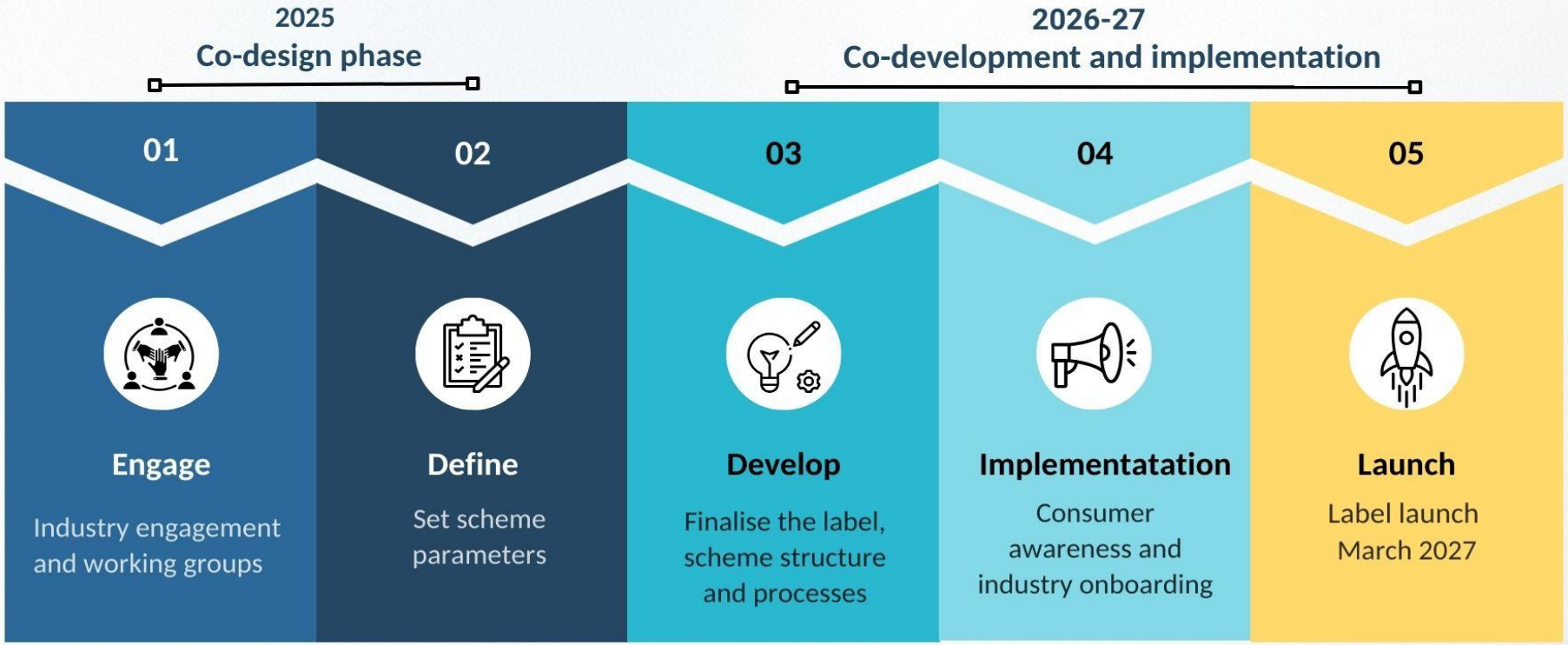
What does success look like?

- Increased consumer confidence and understanding of smart device security leaps
- High adoption from launch, low friction adoption by suppliers
- Launch with some Australian smart devices
- Alignment with key jurisdictions to accelerate labelled smart device international bi-directional flow
- Scheme is flexible to accommodate new security features
- Financially sustainable scheme post March 2027

Security Labelling Scheme for Smart Devices

IoT Alliance Australia

Timeline



Milestones and key dates

July to December 2025: Discovery and Co-design (first six months)

- Define scope, assumptions, options for each work package

Jan 2026 to October 2026: Co-develop

- Label physical and digital design
- Documenting and implementing processes
- Selecting scheme participating entities
- Developing systems to support
- Developing awareness and training collateral
- Recruitment and first manufacturing and retail adopters work through process for launch in March 2027

November 2026 to March 2027: Launch and Learn

- Training
- Awareness campaigns
- Public launch

Industry Involvement

Organisation Types

Manufacturer

Retailer/Distributor

Government

Standards

Research

Services

Consumer representatives

Industry association

Program Advisory Group

- Provides strategic perspective and advice
- Provide advice on members, project structure etc.
- Help identify other stakeholders

Co Design Working Group

- Participate in design activities
- Interactive discussions
- Ad-hoc breakout activities
- Document review
- May include Program Advisory Group members

PAG members

Organisation	Type	Representative
ACCAN	Industry Association	Carol Bennett
ACCC	Government	Luke McMahon
ACMA	Government	Dominic Byrne
AMTA	Industry Association	Louise Hyland
Australian Retailers Association	Industry Association	Ryan Swenson
British Standards Institute (BSI)	Services	Dushyant Sanathara
Consumer Electronics Supplier Association	Industry Association	Evelyn Soud
COSBOA	Industry Association	Catherine Donnan
CSIRO	Research	Marthie Grobler
Deakin University	Research	Robin Doss
Dept of Home Affairs	Government	Ashley Bell
Edith Cowan University	Research	Helge Janicke
Engineers Australia	Industry Association	David Manfield
Genysys Electronics Design	Manufacturer	Damien Landais
Google	Manufacturer	Srinjoy De
GS1	Standards	Peter Carter
ioXT (Internet of Secure Things)	Services	Lloyd Lindner
Rheem	Manufacturer	Richard Horton
Samsung	Manufacturer	Marc Dunn
Standards Australia	Standards	Kyle McCurdy
Tech Council of Australia	Industry Association	Adam Robens
Telstra	Retailer/Distributor	Anuskha Ranasinghe

Key design and implementation challenges

- Keeping it simple for consumers
  - Binary or multi-level label and what it means
  - Label design and use
  - Getting the message out
- Trusted low friction process for suppliers
  - Clear product scope
  - Security and testing standards
  - International alignment
  - Transparent and trusted certification and testing
  - Cost effective Australian process
- Scheme governance and financial model
  - Self-sustaining scheme
  - Empowered and trusted
- Making it attractive for suppliers to adopt the label
  - Market value vs ease and cost of adoption
  - Recruitment and onboarding of first suppliers for launch

Security Labelling Scheme for Smart Devices

IoT Alliance Australia

Trusted low friction process for suppliers

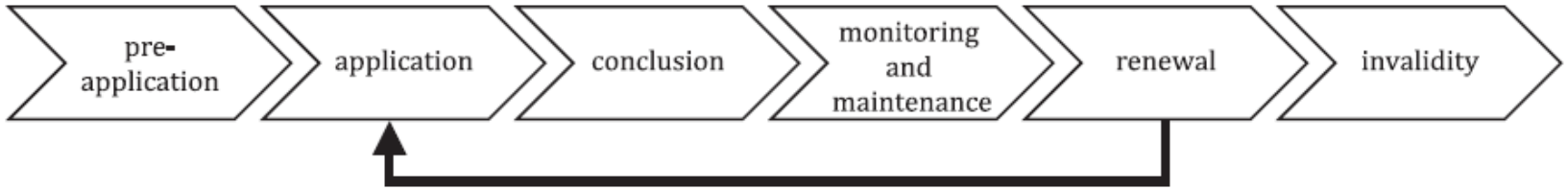


Figure 2 — Process of a consumer IoT labelling scheme

- Australian process to be designed and developed
  - Learn for similar Australian labelling schemes
- Aligned internationally to lower cost of entry and facilitate bi-directional flow
- Trusted processes based on standards and suitable monitoring
- Lowest cost

International context and alignment

The objectives of the program include *"co-design and implement an industry-led and internationally aligned voluntary labelling scheme for consumer-grade smart devices in Australia"*.

Why internationally aligned?

A range of schemes have already been introduced in countries such as Singapore, Germany and Japan, with further initiatives under development in jurisdictions including the United States. Aligning the Australian scheme levels with those of established international schemes (e.g., CLS, Cyber Trust Mark) could facilitate

- **Leveraging mutual recognition**. Reduce duplication by recognising equivalent international smart device security labels.
- **Simplify supplier compliance**. Allow manufacturers to reuse existing certifications when they already meet equivalent security levels.
- **Enable reciprocal agreements**. Position Australia to negotiate and enter into Mutual Recognition Agreements where equivalence is established.

Together, these measures should contribute to a low-friction pathway for industry participation and accelerate the roll-out of smart device security labels in Australia.

Product scope

An important initial tasks for the **Co-design Working Group** will be to define the scope of products covered by the security labelling scheme.

- **Eligible product classes:** define which consumer device classes are in scope and set the criteria for those decisions (e.g. market prevalence, consumer risk, security threat profile). Identify explicit exclusions such as PCs, tablets, phones, medical devices, and vehicles (as per Australian mandatory security standards for smart devices).
- **Functional coverage:** establish the functional boundaries of what certification covers – for example, the device hardware, firmware and software, plus its companion apps, communications links, cloud services, and supporting data systems.
- **Compliance envelope:** specify the product characteristics within which certification remains valid (form factor, hardware, firmware, software versions and so on). Define allowable updates and variations and set the triggers for re-evaluation or retesting when changes fall outside those limits.

The aim is to agree on a clear product scope that helps ensure the scheme is practical, targeted and enforceable.

Security requirements for products

As it relates to defining what it means for a product to be secure, a core task for the Co-design Working Group will be to set the baseline security requirements for smart devices to be granted a label. This could include consideration of Australia's security standards and international standards such as ETSI EN 303 645, and additional attributes that could support higher levels of assurance.

The aim is to establish clear, internationally aligned security labelling requirements that build trust in labelled products and ensure the scheme reflects global best practice.

ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements			Examples of additional security requirements
No universal default passwords	Attack surface exposure	Ease of personal data deletion	Secure development lifecycle and design assurance
Vulnerability management process	Software integrity	Easy installation and maintenance	Software binary analysis
Software updates	Security of personal data	Validation of input data	Black-box penetration testing
Sensitive security parameter storage	Outage resiliency		Vulnerability management & supply chain transparency
Secure communications	Monitoring of telemetry data		User and privacy-centric enhancements

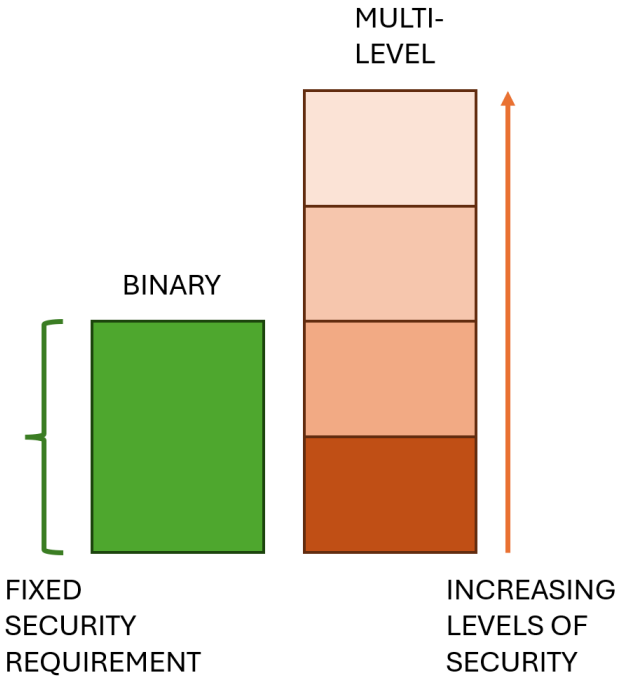
Security Labelling Scheme for Smart Devices

IoT Alliance Australia

Security grading levels

As part of the co-design process, the working group must determine how security will be graded for labelling purposes. The choice lies between a binary model, which sets a single compliance benchmark, and a multi-level model, which establishes progressively stricter tiers of security.

Examples of “binary” labelling schemes - Germany and United States



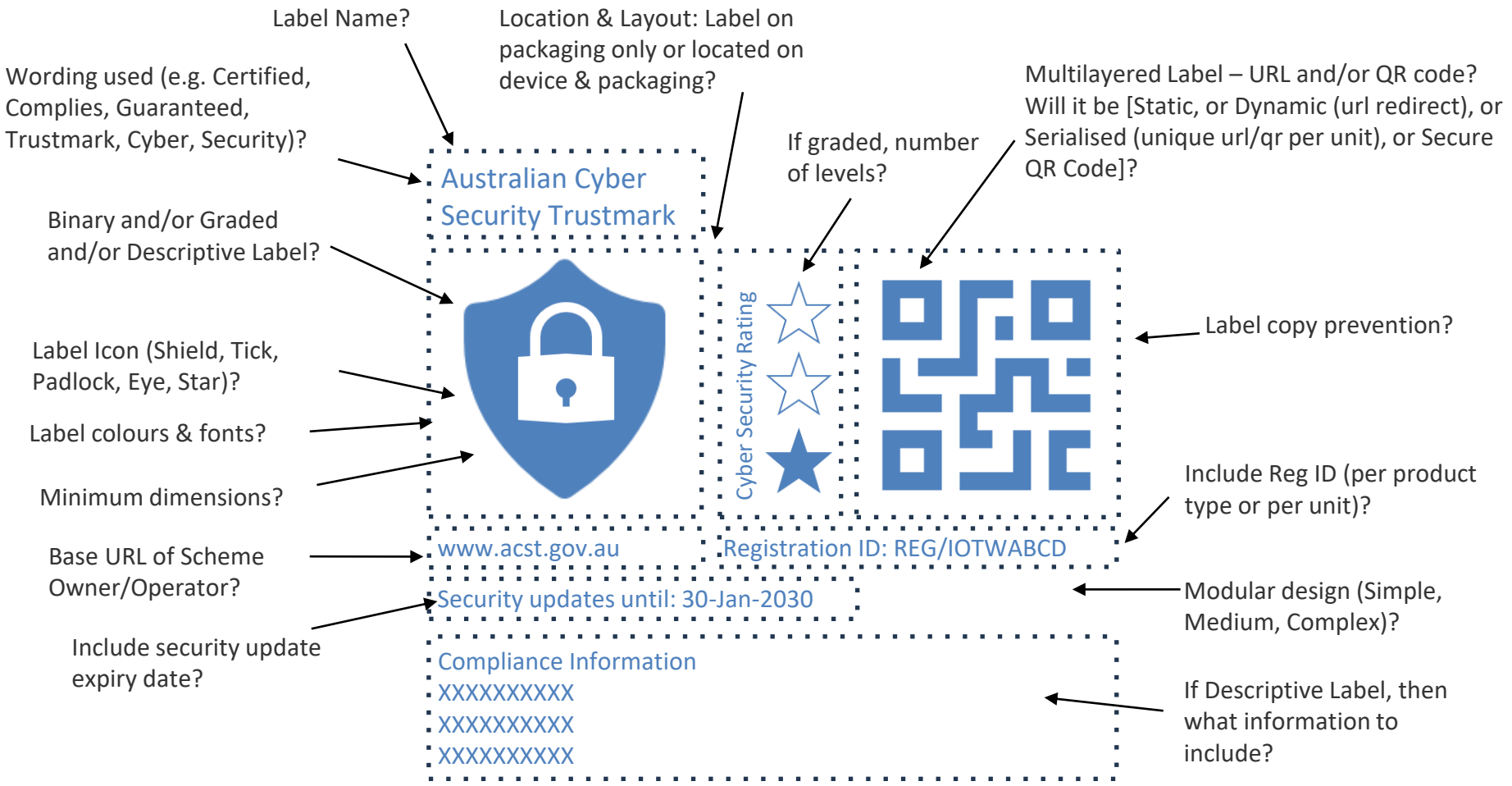
Examples of “multi-level” labelling schemes – Singapore and Japan

Security Labelling Scheme for Smart Devices

IoT Alliance Australia

Label design and usage

Example Design Only



Design an effective trust mark label with attention to both physical and digital elements to ensure recognisability, security, utility and future flexibility.

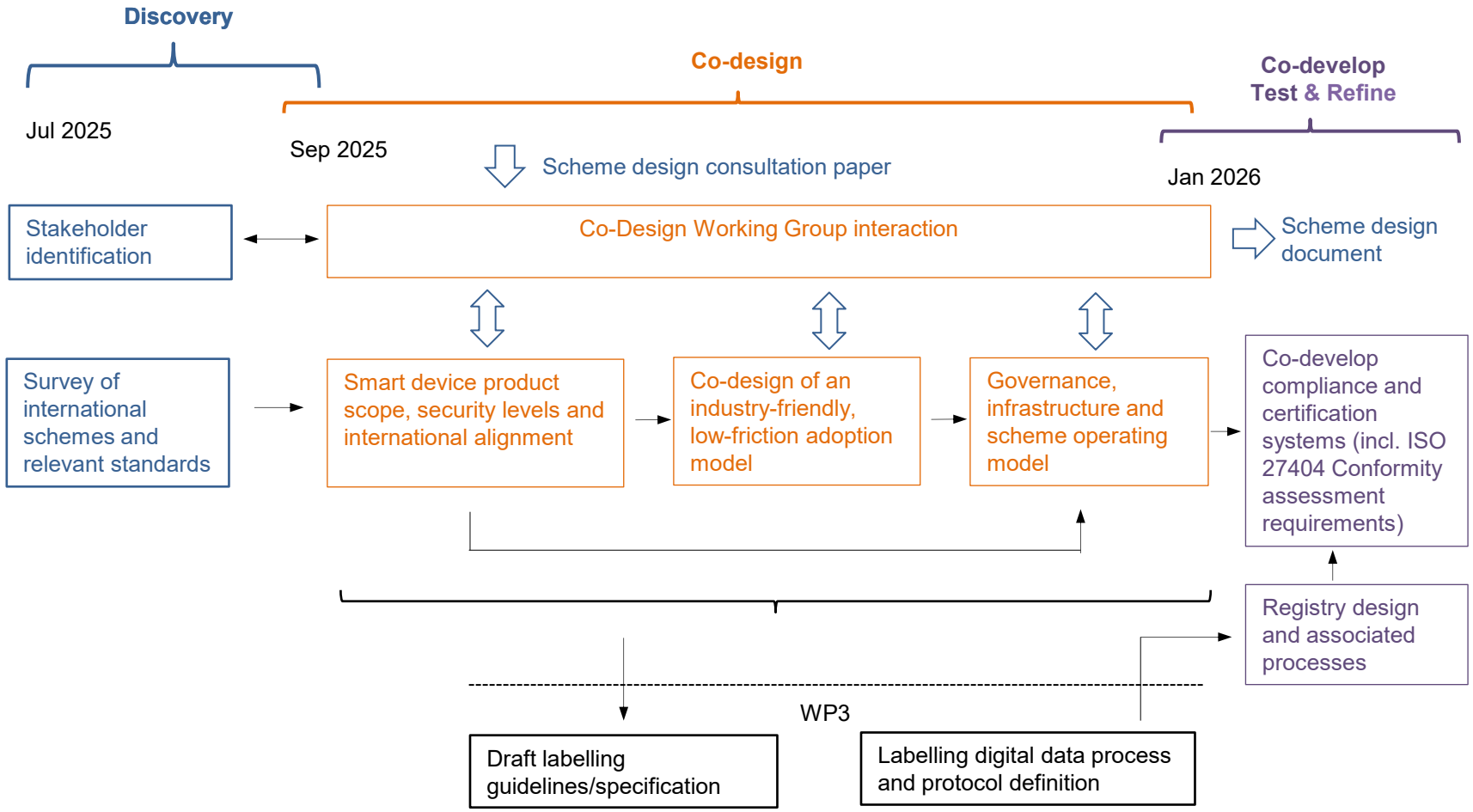
Market and consumer engagement

- Progressive awareness raising and education for suppliers
  - How to apply and get the label
- Collateral for consumers and other stakeholders
  - What the security label means, what products have it and where to find them
- Making it attractive for suppliers to adopt the label
  - Market value vs ease and cost of adoption
  - Recruitment campaign
- Security Label for Smart Devices launch March 2027

Security Labelling Scheme for Smart Devices

IoT Alliance Australia

Co-design working group



Co-design working group

- Join the Co-Design Working Group to have your say in the co-design phase of the program or become an early adopter
- Provide input into consultation papers and targeted discussions around 6 key topic areas:

Scheme security grading / levels
Product scope
Label design and usage
Scheme operating model and procedures
Compliance and certification systems
Market and consumer engagement

- Click here to register your interest and indicate which key topic areas you are most interested to participate in.


Security Labelling Scheme for Smart Devices
IoTA
IoT Alliance Australia

Questions

Contacts

Frank Zeichner, Program Director, IoTAA
Email: LabellingScheme@iot.org.au
Ph: 0408 233 762 (Frank Zeichner)

www.iot.org.au