IoT Security Device Labeling

ISOC IoT Security WG, Ottawa, Canada **Nov. 20th, 2018**

Objective

• Identify the requirements of an IoT device label, aiming to:

- Provide consumers with information to help them make informed decisions at time of purchase on the security compliance and privacy measures of IoT devices

- Provide manufacturers* with a clear and concise way to display security features and related standards compliance of IoT products or devices

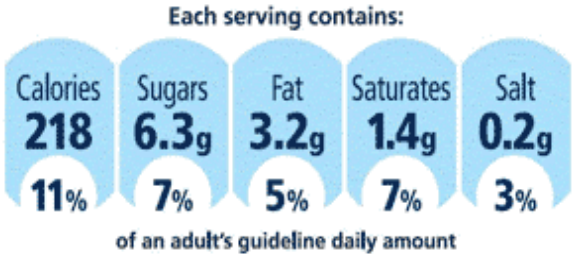
- Allow market oversight authorities to assess compliance to IoT security in a consistent and transparent approach.

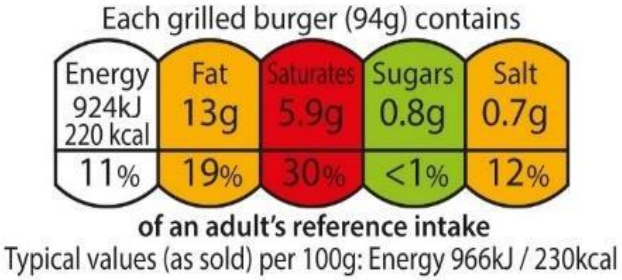
Key Considerations

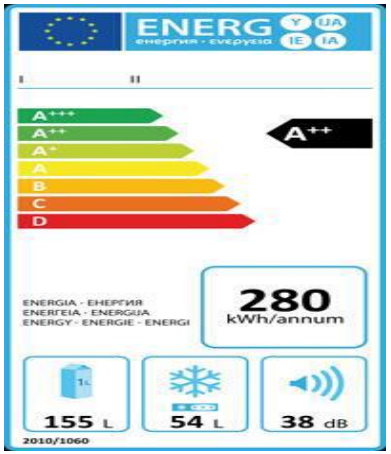
- Label formats
- Standards
- Certification
- Enforcement
- Example label requirements and structure

Label Formats

- Graded Scheme







Refrigerating appliances, as EEI									
A+++	A++	A+	A	B	C	D	E	F	G
<22	<33	<42/44	<55	<75	<95	<110	<125	<150	>150

Label Formats - 2

- Binary or “Seal of Approval” Scheme

- Descriptive Information Scheme
  - Details security related information

10 Principles for IoT Device Security

- No default passwords
- Implement a vulnerability disclosure policy
- Keep software updated
- Securely store credentials and security sensitive data
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure personal data is protected
- Make systems resilient to outages
- Monitor system telemetry data
- Make it easy for customers to delete personal data
- Make installation and maintenance of IoT devices easy
- Validate input data

  - From: UK DCMS, “Code of Practice for Consumer IoT Security”.

Possible IoT Device Security Labels

- Colored graded scheme would attract attention for consumers
  - Need to be mandatory to be effective

- Binary “seal of approval” format is typically preferred by consumers
  - Could lead to false sense of security or that no further action from consumer is needed

- Descriptive information label format highlights critical information to consumers
  - Limit to most relevant information only
  - Good for voluntary label introduction

- Mandatory vs voluntary labels
  - Voluntary initially to become mandatory after a grace period

Certifications - UK

- BSI Kitemark for IoT devices
  - Rigorous independent assessment
  - Three types of BSI Kitemarks for IoT devices
    - Residential
    - Commercial
    - Enhanced, for high value or high risk applications
  - Manufacturer assessed against ISO 9001
  - Product assessed on functionality and interoperability, and
  - Penetration testing scanning for vulnerabilities and security flaws
  - Regular monitoring and audit post award

Certification - Australia

- IoT Product Testing
  - Trust framework based on
    - IoT Security Foundation,
    - Open Web App Security Project (OWASP), and
    - Online Trust Alliance (OTA)
  - Testing to be done by labs accredited by National Association of Testing Authority (NATA)
  - Award of test certificate
  - Currently not mandatory
  - IoTAA will release security test procedures based on OTA Framework
  - Recommend to issue an IoTAA Security and Privacy Trustmark

Certification - EU

• European Cybersecurity Certification framework Act (CSA)

• Certification covers availability, authenticity, integrity, and reliability of data or of functionality and services offered.

• Aim to start mandatory on specific high-risk products and services.

• Long term, mandatory certification with CE marking for all products with internet connectivity.

CSA Cyber Verification Program (CVP)

• CVP is a program and standard for *product* and *organization* security aspects.

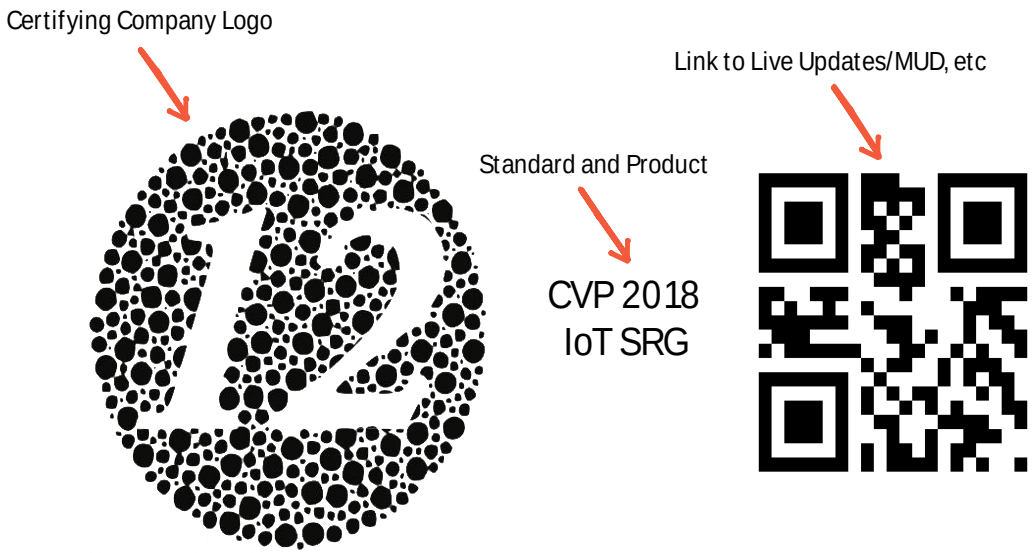
• CVP consists of:
  - Self assessment questionnaire: 198 binary questions covering 6 domains and 18 practices
  - An audit
  - Answers and audit will provide a maturity raring for the organization

• Program has been field tested

• Notice of Intent (NOI) for a Canadian standard is being filed.

Example IoT Device Label

- Label needs to identify
  - Organization who performed formal testing and assessment
  - Standard and product being tested
  - Means to prevent counterfeiting (e.g. holographic, embedded RFID, etc.)
  - Machine readable code to provide up-to-date/live product information (e.g. QR code)



THANK YOU !!