# Trust by Design and The Internet of Things

Internet Society

Robin Wilton

Senior Advisor - Internet Trust

wilton@isoc.org

TIIME 2019

14th February

Vienna

# The Internet Society

Vision: an Internet that is open, globally-connected, secure, and trustworthy

Mission: to ensure that the benefits of the Internet reach everyone

Key themes: access, and trust

Topics:

- Cautionary Tales
- Stakeholders to Influence
- Consumers and choices
- Certification
- IoT Trust Framework

# What does IoT Bring?

# New devices, new vulnerabilities…

… plus some we really ought to have learned about by now.

- Device Cost/Size/Functionality
- Volume of identical devices (homogeneity)
- Long service life (often extending far beyond supported lifetime)
- No or limited upgradability or patching
- Physical security vulnerabilities
- Access

- Limited user interfaces (UI)
- Limited visibility into, or control over, internal workings
- Embedded devices
- BYOIoT into the enterprise (!)

… and, above all, erosion of context.

# The Internet Society's Dual Perspective

## "Inward" Security

Focus on potential harms to the health, safety, and security of device users and their property stemming from compromised IoT devices and systems.

## "Outward" Security

Focus on potential harms that compromised devices and systems can inflict on the Internet and other users.

# Cautionary Tales From the Connected World

Two “case studies” and their consequences…

- Context and Risk
- Personal Impact

# 1 - Context and Risk: an example from 2016-17

- Pay for the toy,
- Pay again with your data,
- Pay again when the data is ransomed!
- No need to worry about security, just enable Bluetooth on your phone!

- One retail product, aimed at young children
- Over 800,000 accounts/profile photos compromised
- Over 2 million voice recordings exposed

# Lessons from the connected toy

- Security of the device was not designed in
- Security of the back end was not designed in
- What value set does this approach indicate?

- Securing IoT devices increases their cost
- There’s a cost to insecurity, too
- But it generally falls on someone else

- Values-based design is a viable option: plenty of guidance is available

# 2 - Personal Impact: an example from 2017-18

- ☆ Dr Marie Moe, SINTEF (Norwegian University of Science and Technology - NTNU)
- ☆ Depends on her pacemaker to keep her heart beating
- ☆ Discovered - the hard way - that this supposedly “smart” connected device had some flawed design assumptions.

# Lessons from the connected pacemaker

- Failure modes for the device were… unfriendly
- Communications were not secure
- Different manufacturers' devices weren't interoperable

Exactly when would you like your heart to go offline for a firmware update?

A connected world offers the promise of convenience, efficiency and insight, but also creates a platform for shared risk.

Many of today’s IoT devices are rushed to market to satisfy commercial imperatives, with little consideration for basic security and consumer safety protections.

# Internet Society's Approach for IoT Trust by Design

1

Work with manufacturers and suppliers to adopt and implement the OTA IoT Trust Framework

2

Mobilize consumers to drive demand for security and privacy capabilities as a market differentiator

3

Encourage policy and regulations to push for better security and privacy features in IoT

# Industry/Service Providers/Retail

- Commit to Framework principles
- Push back through supply chain
- Curate offerings – only carry products that ”clear the bar”

# Policymakers

- Strengthen accountability
- Promote use of “trustability” signals
- Motivate stakeholders to practice “trust by design”
- Foster technology & vendor neutral solutions
- Use full range of regulatory tools (consumer, competition, market, insurance…)

# Consumer Organizations

- Highlight security and privacy in reviews/ratings
- Help reach and educate consumers
- Build recognition of certification/trust mark

2018: Internet Society and Consumers International partnership announced

How do we encourage consumers to make better trust decisions?

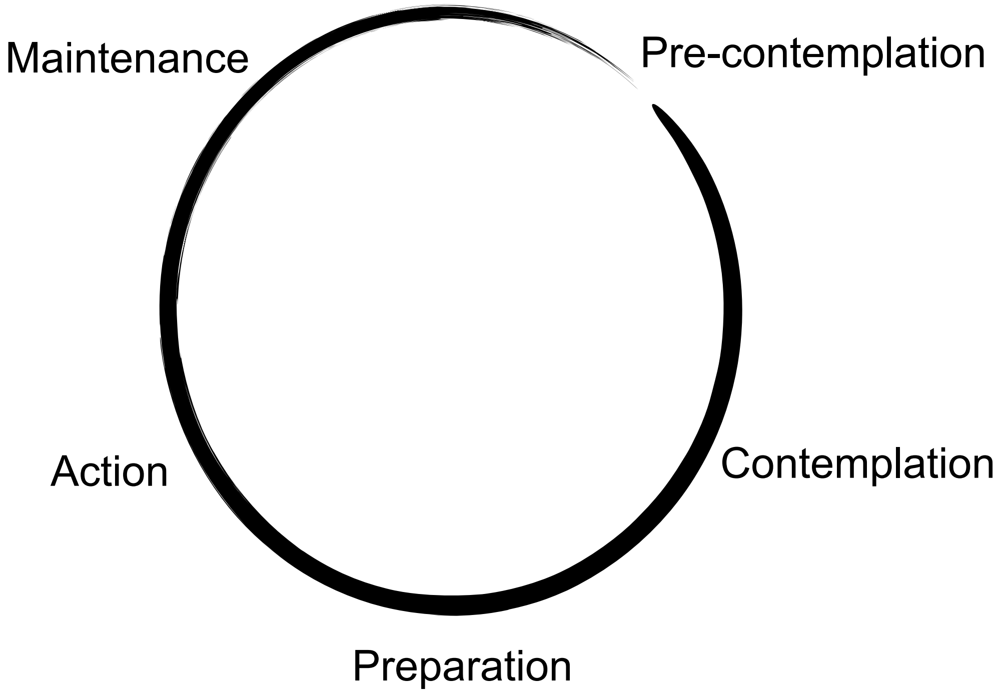
After all… what is trust?

A candidate definition:

“Trust is a belief that someone else will act in your interest, even if they have the opportunity and the motivation to do otherwise.”

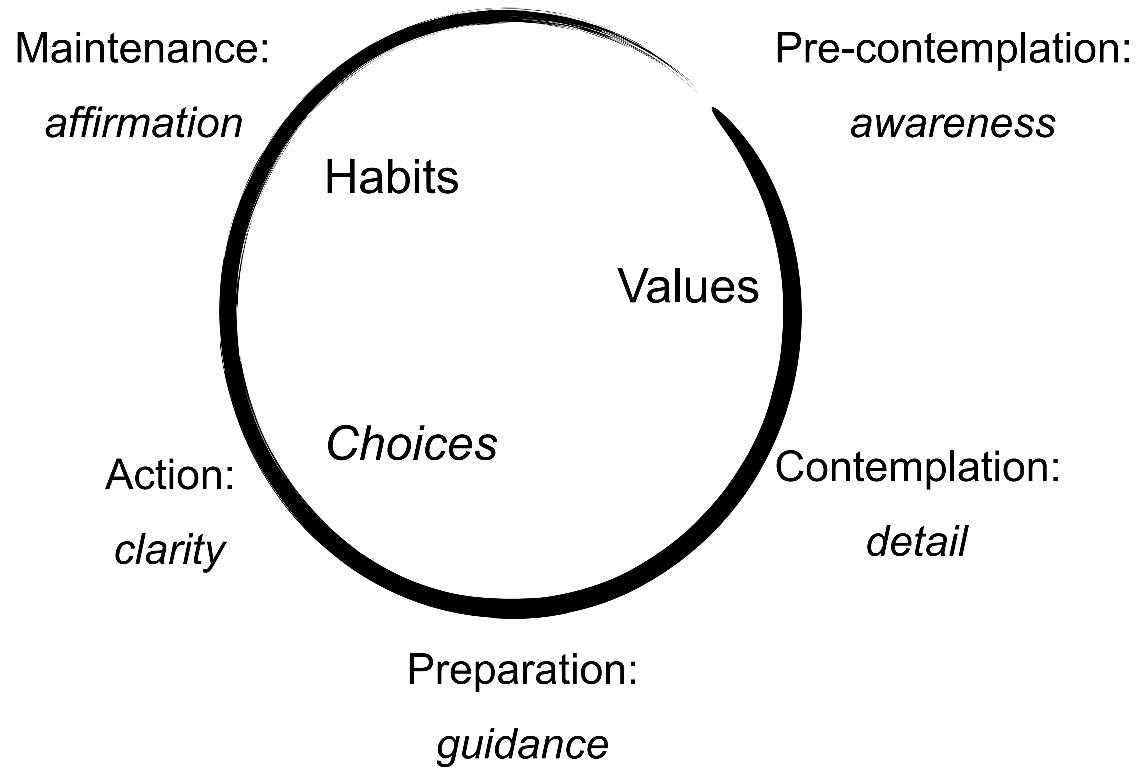
Like any belief, it can be well- or ill-founded - so what can we do to improve the foundations?

# Stages in behavioural change



- This is one model for *sustained* behavioural change (Prochaska and Di Clemente, 2005)
- A one-off “nudge” doesn’t work
- The real goal is to change values, not just one decision
- Privacy protection differs from e.g. weight loss; how do you know when you’ve succeeded?

# Intervention: clear information at the point of choice



Maintenance:

*affirmation*

Pre-contemplation:

*awareness*

Habits

Values

*Choices*

Action:

*clarity*

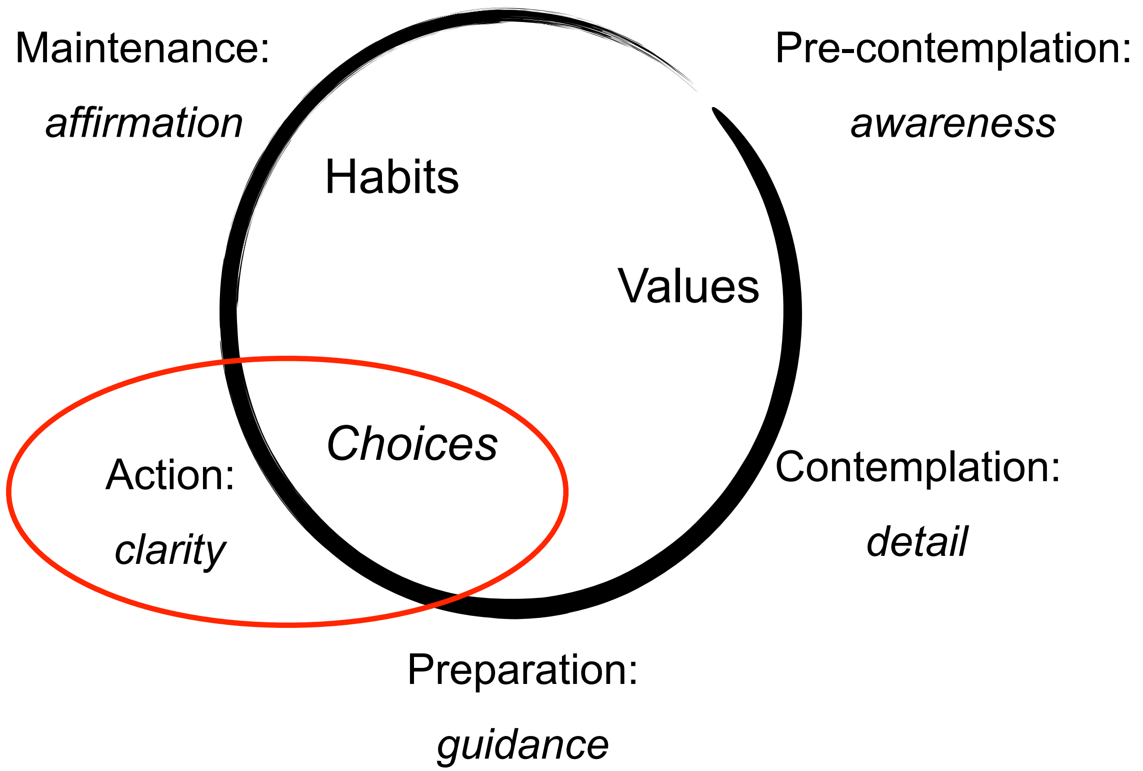
Contemplation:

*detail*

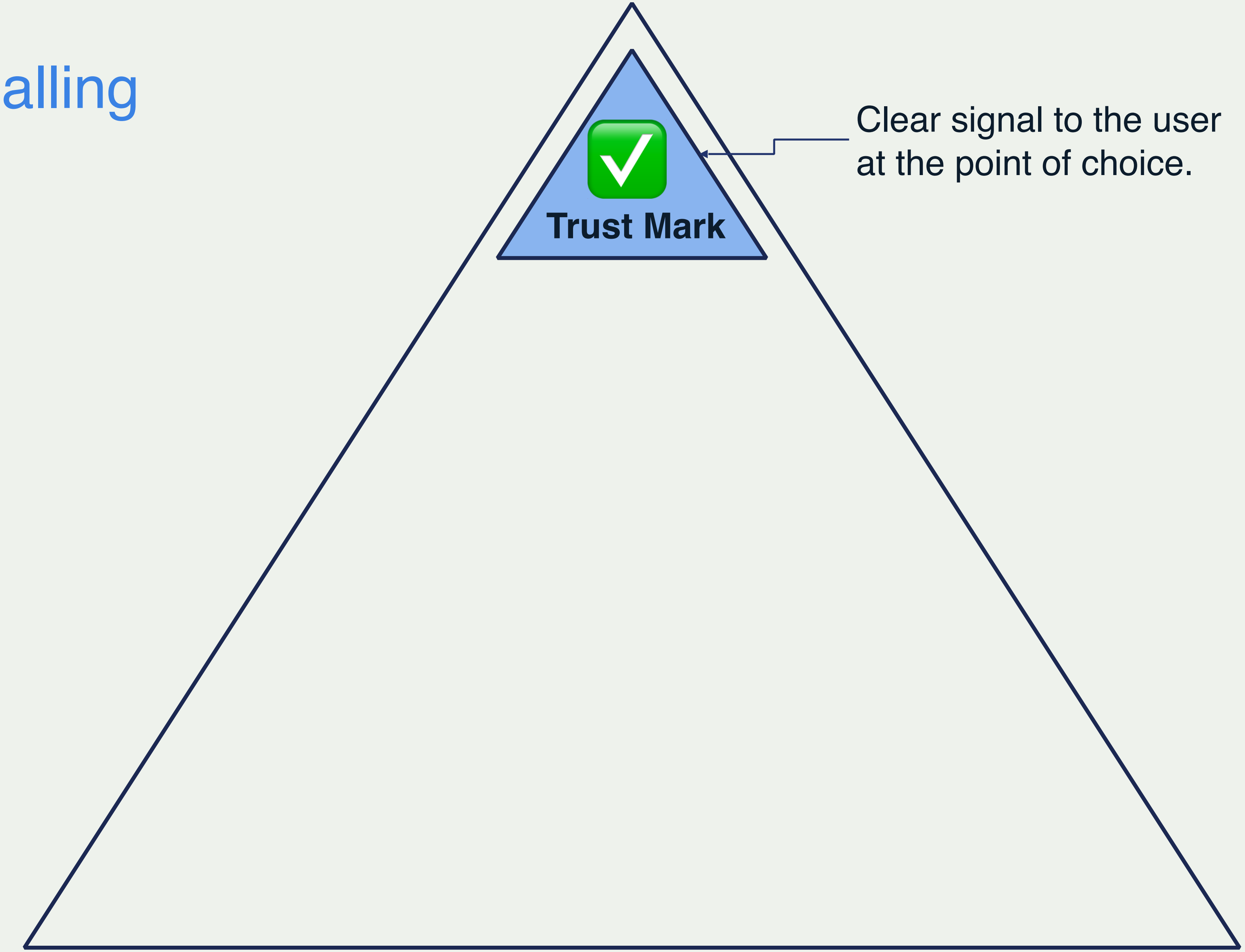
Preparation:

*guidance*

# Intervention: clear information at the point of choice

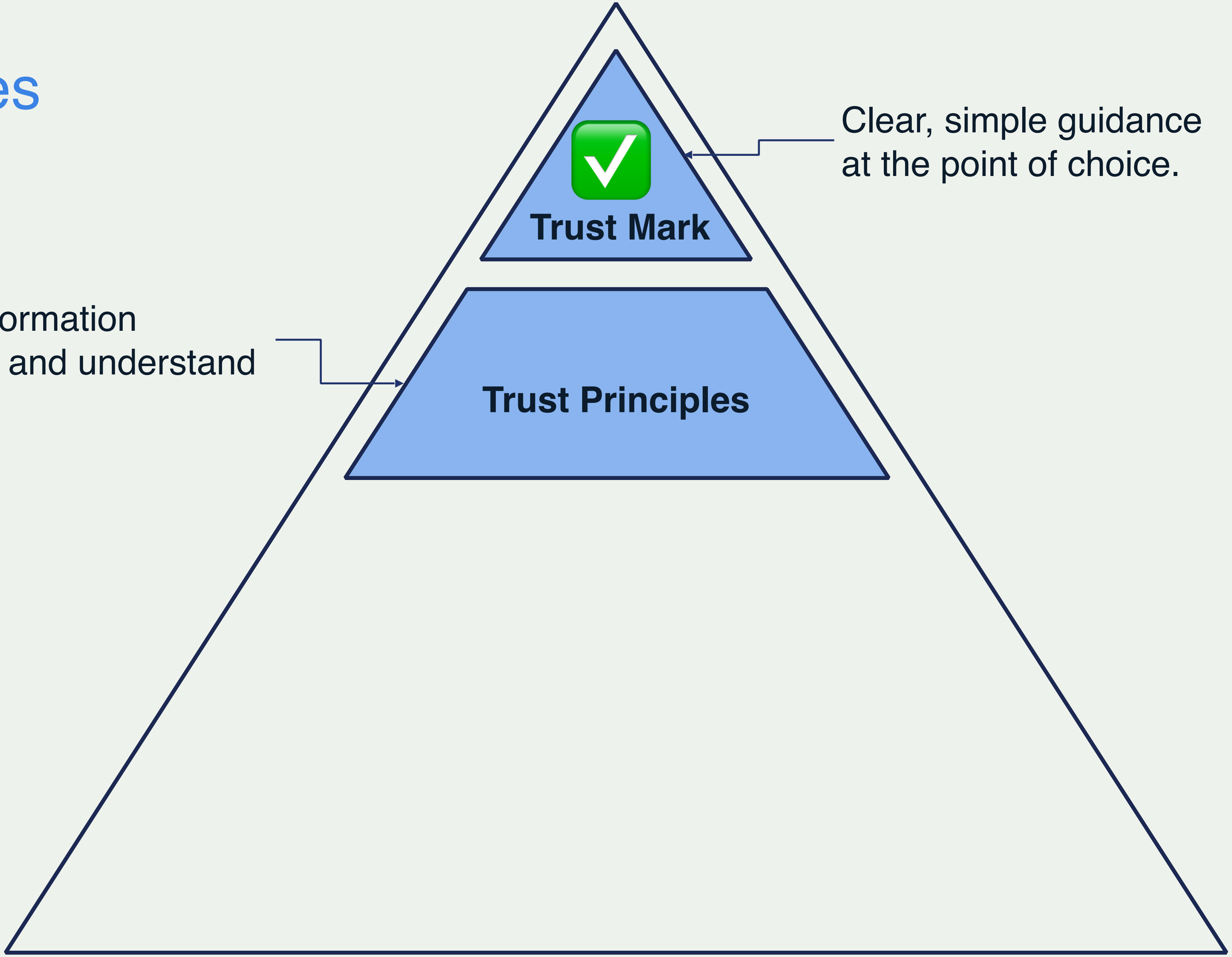


# Clear Signalling



Clear signal to the user at the point of choice.

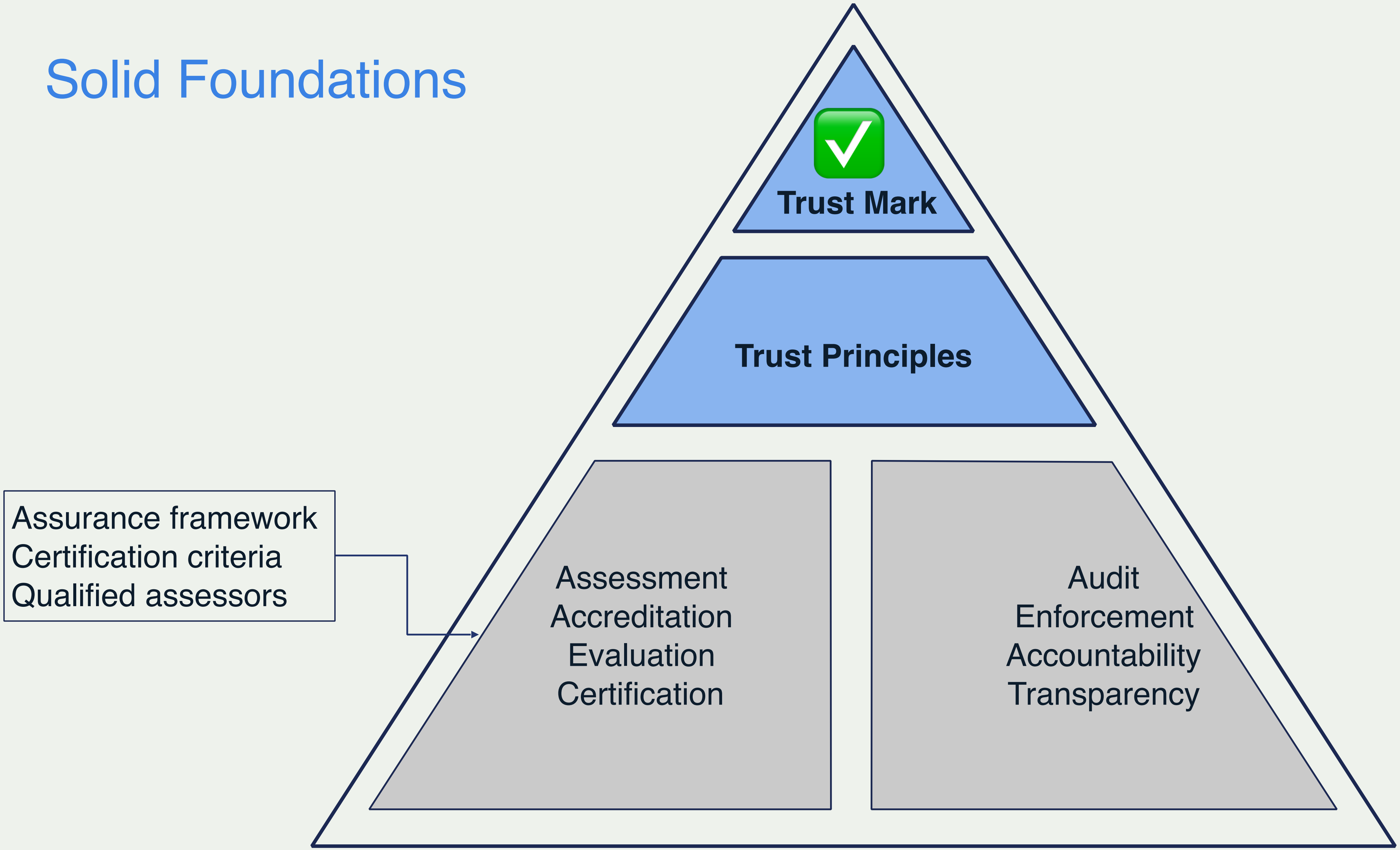
# Clear Values



Clear, simple guidance at the point of choice.

Supplementary information that is easy to find and understand

# Solid Foundations



✅

Trust Mark

Trust Principles

Assessment
Accreditation
Evaluation
Certification

Audit
Enforcement
Accountability
Transparency

Assurance framework
Certification criteria
Qualified assessors

The Internet Society's

Online Trust Alliance is here to help!

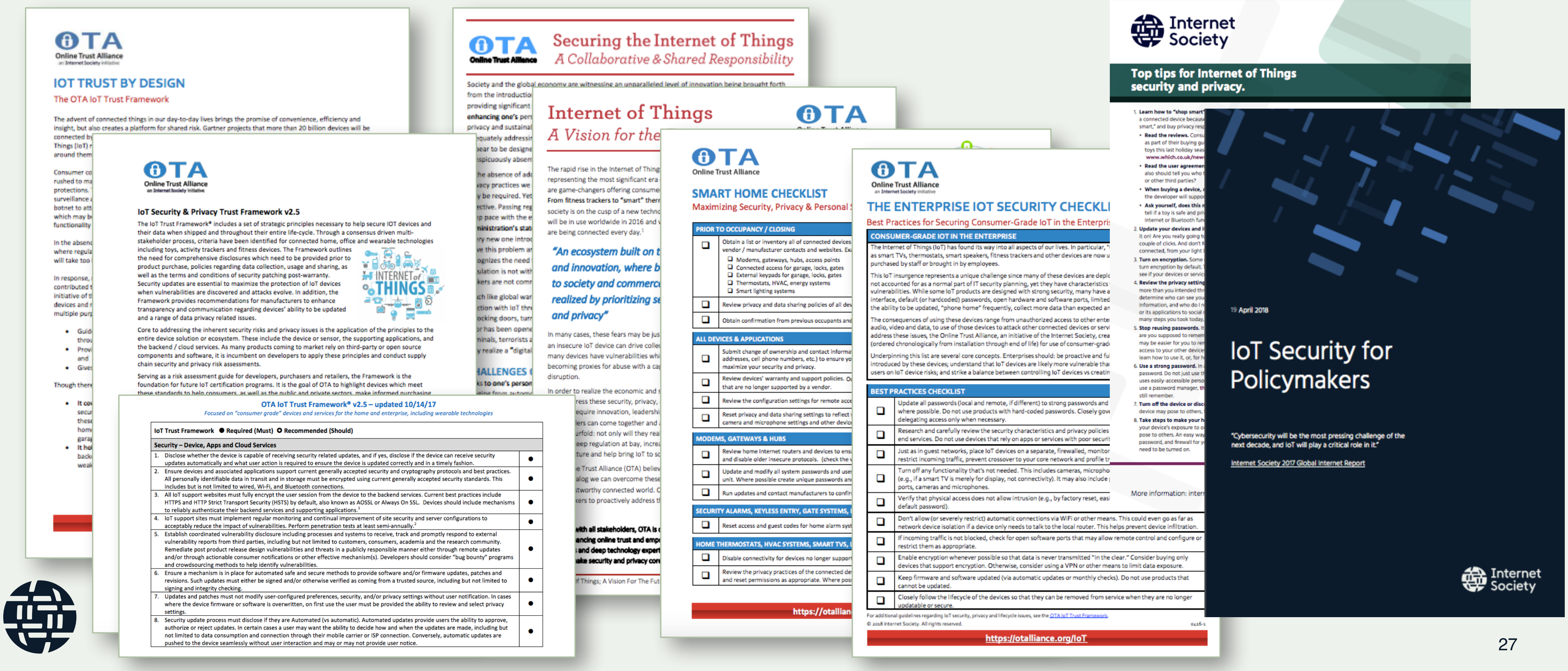
# Online Trust Alliance's IoT Trust Framework:

40 clear criteria addressing 8 topic areas:

| | | | |
|---|---|---|---|
| Authentication | Encryption | Security | Updates |
| Privacy | Disclosures | Control | Communications |

# Resources to Help

- Latest checklist posted at https://otalliance.org/IoT



## IOT TRUST BY DESIGN

The OTA IoT Trust Framework

## Securing the Internet of Things

*A Collaborative & Shared Responsibility*

## Internet of Things

*A Vision for the*

## SMART HOME CHECKLIST

Maximizing Security, Privacy & Personal

## THE ENTERPRISE IOT SECURITY CHECKLI

Best Practices for Securing Consumer-Grade IoT in the Enterpri

https://otalliance.org/IoT

## Top tips for Internet of Things security and privacy.

## IoT Security & Privacy Trust Framework v2.5

The IoT Trust Framework® includes a set of strategic principles necessary to help secure IOT devices and their data when shipped and throughout their entire life-cycle. Through a consensus driven multi-stakeholder process, criteria have been identified for connected home, office and wearable technologies including toys, activity trackers and fitness devices. The Framework outlines the need for comprehensive disclosures which need to be provided prior to product purchase, policies regarding data collection, usage and sharing, as well as the terms and conditions of security patching post-warranty. Security updates are essential to maximize the protection of IoT devices when vulnerabilities are discovered and attacks evolve. In addition, the Framework provides recommendations for manufacturers to enhance transparency and communication regarding devices' ability to be updated and a range of data privacy related issues.

Core to addressing the inherent security risks and privacy issues is the application of the principles to the entire device solution or ecosystem. These include the device or sensor, the supporting applications, and the backend / cloud services. As many products coming to market rely on third-party or open source components and software, it is incumbent on developers to apply these principles and conduct supply chain security and privacy risk assessments.

Serving as a risk assessment guide for developers, purchasers and retailers, the Framework is the foundation for future IoT certification programs. It is the goal of OTA to highlight devices which meet these standards to help consumers, as well as the public and private sectors, make informed purchasing

### OTA IoT Trust Framework® v2.5 – updated 10/14/17

*Focused on "consumer grade" devices and services for the home and enterprise, including wearable technologies*

| IoT Trust Framework ● Required (Must) ○ Recommended (Should) | |
|---|---|
| **Security – Device, Apps and Cloud Services** | |
| 1. Disclose whether the device is capable of receiving security related updates, and if yes, disclose if the device can receive security updates automatically and what user action is required to ensure the device is updated correctly and in a timely fashion. | ● |
| 2. Ensure devices and associated applications support current generally accepted security and cryptography protocols and best practices. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This includes but is not limited to wired, Wi-Fi, and Bluetooth connections. | ● |
| 3. All IoT support websites must fully encrypt the user session from the device to the backend services. Current best practices include HTTPS and HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL. Devices should include mechanisms to reliably authenticate their backend services and supporting applications.[1] | ● |
| 4. IoT support sites must implement regular monitoring and continual improvement of site security and server configurations to acceptably reduce the impact of vulnerabilities. Perform penetration tests at least semi-annually.[2] | ● |
| 5. Establish coordinated vulnerability disclosure including processes and systems to receive, track and promptly respond to external vulnerability reports from third parties, including but not limited to customers, consumers, academia and the research community. Remediate post product release design vulnerabilities and threats in a publicly responsible manner either through remote updates and/or through actionable consumer notifications or other effective mechanism(s). Developers should consider "bug bounty" programs and crowdsourcing methods to help identify vulnerabilities. | ● |
| 6. Ensure a mechanism is in place for automated safe and secure methods to provide software and/or firmware updates, patches and revisions. Such updates must either be signed and/or otherwise verified as coming from a trusted source, including but not limited to signing and integrity checking. | ● |
| 7. Updates and patches must not modify user-configured preferences, security, and/or privacy settings without user notification. In cases where the device firmware or software is overwritten, on first use the user must be provided the ability to review and select privacy settings. | ● |
| 8. Security update process must disclose if they are Automated (vs automatic). Automated updates provide users the ability to approve, authorize or reject updates. In certain cases a user may want the ability to decide how and when the updates are made, including but not limited to data consumption and connection through their mobile carrier or ISP connection. Conversely, automatic updates are pushed to the device seamlessly without user interaction and may or may not provide user notice. | ● |

19 April 2018

## IoT Security for Policymakers

"Cybersecurity will be the most pressing challenge of the next decade, and IoT will play a critical role in it."

Internet Society 2017 Global Internet Report

# All The Frameworks…

OTA
Online Trust Alliance
an Internet Society initiative

**IoT Security & Privacy Trust Framework v2.5**

The IoT Trust Framework® includes a set of strategic principles necessary to help secure IOT devices and their data when shipped and throughout their entire life-cycle. Through a consensus driven multi-stakeholder process, criteria have been identified for connected home, office and wearable technologies including toys, activity trackers and fitness devices. The Framework outlines the need for comprehensive disclosures which need to be provided prior to
product purch
well as the ter
Security upda
when vulnera
Framework pr
transparency
and a range o

Core to addre
entire device
the backend /
components a
chain security

Serving as a ri
foundation fo
these standar
decisions. The

The Framewo

- **Security P** cloud serv process to supply cha principles
- **User Acce** shipment processes
- **Privacy, D** privacy pr capability applicable addresses
- **Notificati** mechanis include re communi accessibil

© 2017 Online

NISC
内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity
（首相官邸Webサイトの検索システム

General Framework for Secure IoT Systems

National center of Incident readiness and Strategy for Cybersecu
Governmen
Augus

1. General Framework Objective

Internet of Things (IoT) systems consist of connected things and networks and th
be regarded as an integrated system of IT with physical components. It is importan
physical safety in addition to existing information security measures. It is essenti
systems are designed, developed and operated under the principle of "Security b
while looking ahead to the future where many individual systems are interconn
new vulnerabilities possibly introduced. To rationally accomplish this, a two-step
is appropriate: instituting general requirements on design, development, and op
all IoT systems, in addition, sector-specific requirements for development and
based on characteristics of respective sectors.

Based on this concept, this framework aims to clarify the fundamental and essenti
requirements for secure IoT systems.

It is expected that this framework will contribute to promoting the industr
involvement in the development of secure IoT systems and will create an environment in which IoT systems users can utilize the systems with a condition that security and safety is assured, by promoting the interoperability of IoT systems and the implementation of security requirements.

enisa

Baseline Securit
Recommendatio
in the context of Critical Informatio

NOVEMBER 2017

www.enisa.europa.eu
European Union Agency For N

Secure by Design Report

Department for
Digital, Culture
Media & Sport

Secure by Design: Improvi
security of consumer Intern
Report

Singapore
Standards
Council

TR 64 : 2018
(ICS 35.030)

TECHNICAL REFERENCE
**Guidelines for IoT security for smart nation**

Published by
Enterprise Singapore

IoTA
IoT Alliance Australia

INTERNET OF THINGS
SECURITY GUIDELINE

*IoT SECURITY GUIDELINE V1.2*
November 2017

**Draft NISTIR 8200**

**Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)**

Prepared by the Interagency International Cybersecurity Standardization Working Group.

The Interagency International Cybersecurity Standardization Working Group (IICS WG) has developed this draft report based upon the information available to the participating agencies. Comments are being solicited in order to augment that information, especially on the information about the state of cybersecurity standardization for IoT that is found in Sections 8, 9, 10, and Annex D.

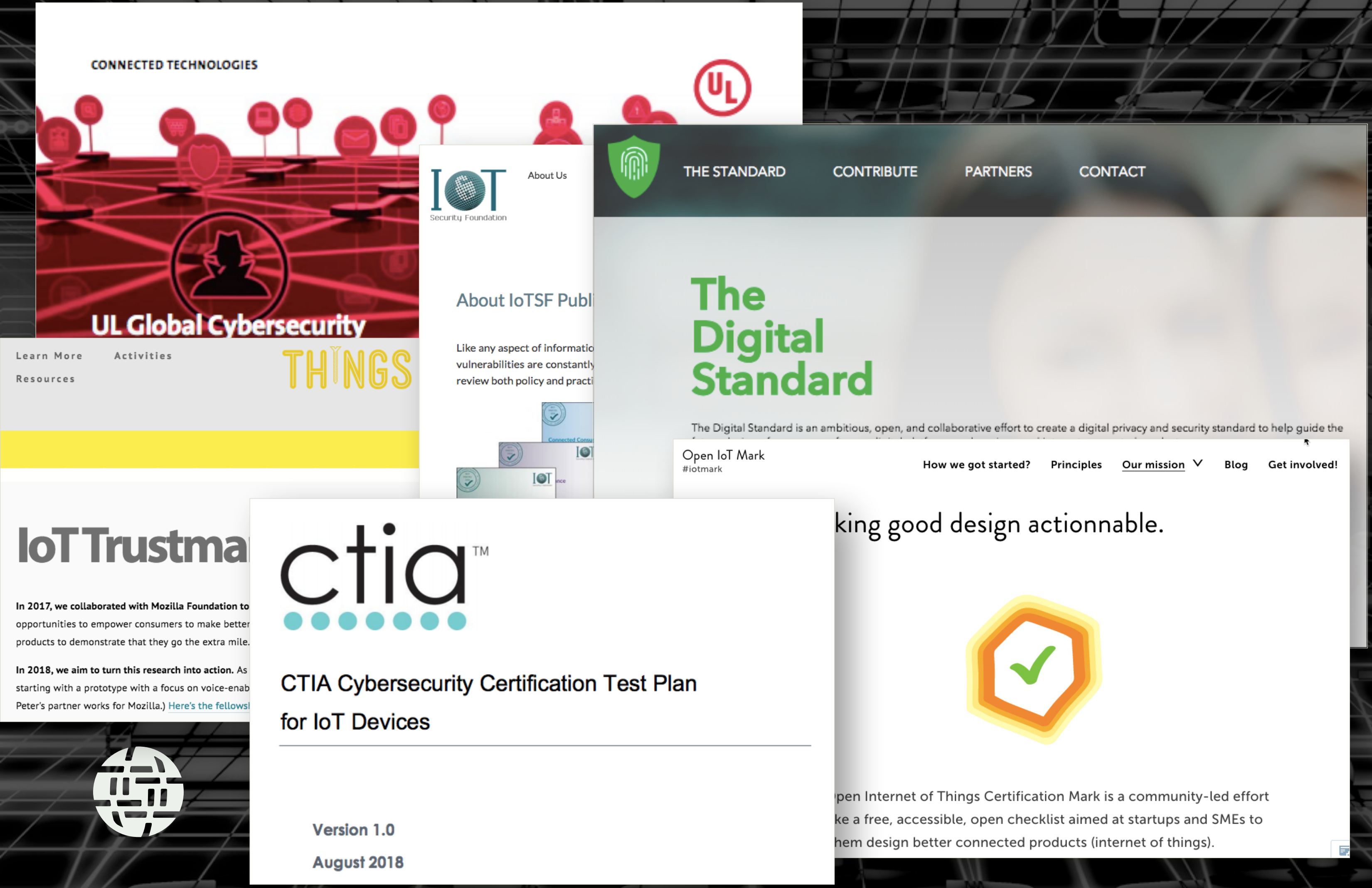
Reviewers are requested to submit comments to NISTIR-8200@nist.gov using the comment template at https://csrc.nist.gov/publications/detail/nistir/8200/draft. Comments will be posted at https://www.nist.gov/itl/comments-draft-nistir-8200 as they are received.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

We ended up commissioning a comparative analysis

# Next, with Consumers International's help:

# Testing/Certification/Trustmark Design



CONNECTED TECHNOLOGIES

UL Global Cybersecurity

Learn More Activities

Resources

THINGS

IoT Trustma

**In 2017, we collaborated with Mozilla Foundation to** opportunities to empower consumers to make better products to demonstrate that they go the extra mile.

**In 2018, we aim to turn this research into action.** As starting with a prototype with a focus on voice-enab Peter's partner works for Mozilla.) Here's the fellows

IOT Security Foundation

About Us

About IoTSF Publ

Like any aspect of informatio vulnerabilities are constantly review both policy and practi

THE STANDARD CONTRIBUTE PARTNERS CONTACT

The Digital Standard

The Digital Standard is an ambitious, open, and collaborative effort to create a digital privacy and security standard to help guide the

Open IoT Mark
#iotmark

How we got started? Principles Our mission Blog Get involved!

king good design actionnable.

pen Internet of Things Certification Mark is a community-led effort ke a free, accessible, open checklist aimed at startups and SMEs to hem design better connected products (internet of things).

ctia™

CTIA Cybersecurity Certification Test Plan for IoT Devices

Version 1.0

August 2018

- Who is the mark aimed at?
- What does it convey?
- What does it stand for?

# Standards Work, Through the IoT Lifecycle

- **EAT (Entity Attestation Token)** – prove provenance and characteristics about a device, node or service
- **MUD (Manufacturer Usage Description)** – things can signal the access and network functionality they require – approved as proposed standard
- **SUIT (Software Updates for the Internet of Things)** – securely update firmware
- **TEEP (Trusted Execution Environment Processing)** – standardizing protocols for provisioning applications into secure areas of computer processors
- **ACE (Authentication and Authorization for Constrained Environments)**
- **CBOR (Concise Binary Object Representation)** – efficient machine-to-machine formats

Reference: https://www.ietfjournal.org/rough-guide-to-ietf-102-internet-of-things/

# In Summary…

- Users need to make better trust decisions about IoT
  - Trust decisions must be well founded
- Trust marks have a role to play
  - They must be based on reliable certification
- Trust marks must be recognisable and understood at the point of choice

## In Summary…

- Users need to make better trust decisions about IoT
  - Trust decisions must be well founded
- Trust marks have a role to play
  - They must be based on reliable certification
- Trust marks must be recognisable and understood at the point of choice

After all …

# In Summary…

- Users need to make better trust decisions about IoT
  - Trust decisions must be well founded
- Trust marks have a role to play
  - They must be based on reliable certification
- Trust marks must be recognisable and understood at the point of choice

The Internet: it's a trust thing.
Mainly cat videos, but also trust.

# Thank you.

Robin Wilton

Senior Adviser - Internet Trust

wilton@isoc.org

Visit us at
www.internetsociety.org

Follow us
@internetsociety