CANADIAN IOT SECURITY INITIATIVE 2018

IoT Labelling

Webinar, 1 August 2018, 14:00 UTC

Labelling presumptions

The project aims at helping *Consumers making smarter choices* when buying IoT tools and services.

Labels can help, but:

1. Labels need to be meaningful and relevant;
2. Labels need to be easily understood by people, but also by machines;
3. Labels need to be backed by standardization/certification. What ways for testing and certification?

Your panel today

Moderator: Maarten Botterman

Speakers:

- Jonathan Cave
- Jacques Kruse Brandao
- Faud Kahn

Agenda

5:00’ Jonathan Cave – informing consumer choice through labelling: what to consider? Lessons learned from the EU ECO-labelling Directive.

13:00’ Jacques Kruse Brandao – certification of security of “Things”: what levels of assurance can be achieved? Two approaches: <1> the advise from EU industry to the European Commission on the Cyber Security Act; <2> bottom up development of norms and standards by AIOTI.

21:00’ Faud Kahn – types of labels, and a Canadian case study: “CSA Group Cyber Verification Program”

30:00’ Panel discussion, including contributions from other participants

60:00’ ends

Jonathan Cave – Warwick University

What are labels meant to do?

- Before purchase by informing consumer decisions:
  - Helping markets to give us the devices we need;
  - Ensuring that designs, prices, implementation, etc. reflect consumer preferences – including ethics, country of origin, tech compatibility etc.;
  - Encouraging and rewarding innovation
- After purchase to ensure realisation of anticipated benefits
  - Informing the way devices are used
  - Documenting an accountability trail
  - Informing purchases and connections of subsequent devices.
- At the end of device life by informing disposal.

Practical requirements

- Labels must ‘speak to’ users at or before key decisions
  - Direct information
  - Pointers to reliable detailed information
  - Certification ‘marks’ …
- For purchase decisions
  - Provide an assured complement to marketing
  - Be sufficiently standardised to enable product comparisons
  - Cover a defined set of attributes (some specified in law, some set by self-regulation)
  - Be available without impediments and kept up to date
  - Comply with legal and regulatory requirements
    - On the label itself
    - On the contents of the label
    - On the description of the item (Trades Description, COO certification, CE mark)
- For use decisions
  - Contact/traceback/compatibility details (?)

Online labelling

Most purchase decisions are made online

Ecolabelling Directive responsible for 50% of reduction in household energy use before 2010 recraft;

Effectiveness declined rapidly thereafter in line with online shopping.

Electronic provision allows proximity to decision, minimises cost to supplier (esp. updates), retailer (esp. for systems) and shopper (e.g. mouseover, links to further information)

Machine-readability

Allows third-party processing (search engines, mashups with energy tariffs or IoT system details)

Customiseability of and user-derived additional content

Facilitates market surveillance (a regulatory requirement)

Jacques Kruse Brandao - NXP

Mission & Objectives

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries.

The main objective of ECSO is to support all types of initiatives or projects that aim to develop, promote, encourage European cybersecurity,

https://ecs-org.eu/

The European Cybersecurity Act – a proposal by the European Commission

- Article 45 : Security objectives (data confidentiality, data integrity, data/services right management, data/services access/logs, incident response, patch management)

- Article 46 : assurance levels (basic : limited degree of confidence, substantial : certificate with a substantial decrease of the risk, high : certificate to prevent cybersecurity incidents)

- Article 47 : certification schemes defining evaluation criteria depending on security objectives

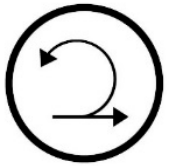
What industry expects (examples)

Fast and predictable

High level of flexibility

Full harmonization

Pragmatism

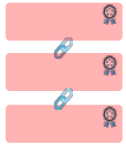


agility

Detecting cheaters in the supply chain

Patching and updates

Ethical hacking



Lean modular composite certifications

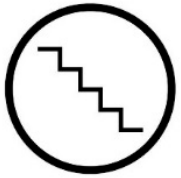
What industry worries about (examples)

Too slow and too unpredictable

Not flexible enough

Lack of harmonization

Too much formalisms

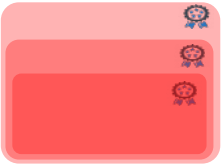


lack of agility

Undetected cheaters in the supply chain

Static certificates

Pure checklist evaluations



complex composite certifications

Meta-Scheme Idea

- Allows composition across **different** schemes via a meta-language
- Supports scaleable common structure and re-use across verticals through horizontals
- Different schemes can be defined „equivalent“ if needed

For Verticals

Sector A | Sector B | Sector C | Sector D | Sector E

Sector independent „generic“ schemes, e.g. Common Criteria, ISO 27001...

For Horizontals

Schemes specific for Sector A

Schemes specific for Sector B

Schemes specific for Sector C

Schemes specific for Sector D

Schemes specific for Sector E

Levels of assurance and assessment types

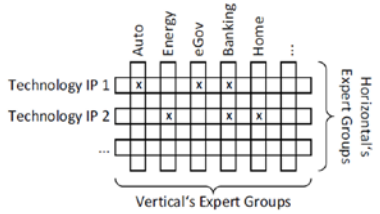
	Symbol (Example)	Assessment Type	Assurance Level	Scope of Security Functionality Level = min	Scope of Security Functionality > min	Schemes allowed
Advanced	A	Accredited Third Party	High	Sector/Use Case dependent	Sector / Use Case dependent	<mapping from SOTA>
	B	Accredited Third Party	Moderate			<mapping from SOTA>
	C	Accredited Third Party	Enhanced Basic			<mapping from SOTA>
Base	D	Accredited Third Party	Basic	Sector/Use Case agnostic		<mapping from SOTA>
	E	Self	Entry			

A sector can decide to not define certain levels → free to define if and which advanced levels to provide, whereas
the basic levels D and E must be supported in any case

Disclaimer: should be seen as a default case/template for sectors. Depending on the sector this might be refined or overridden in exceptional cases where e.g. assessment by a company-internal independent organisation is done for the advanced levels. Notice, however that this can never replace the level of independence and trust which an external party can give. Moreover, for such cases a very strict shadowing process by an accredited third party is required, which tightly audits the internal organisation on a regular basis. This also has an impact on liability.

Identify gaps in the mapped schemes and in the meta-level structure and close them!

Horizontal View: experts for a certain technology IP domain
Vertical View: experts for a certain use case doing also risk assessment



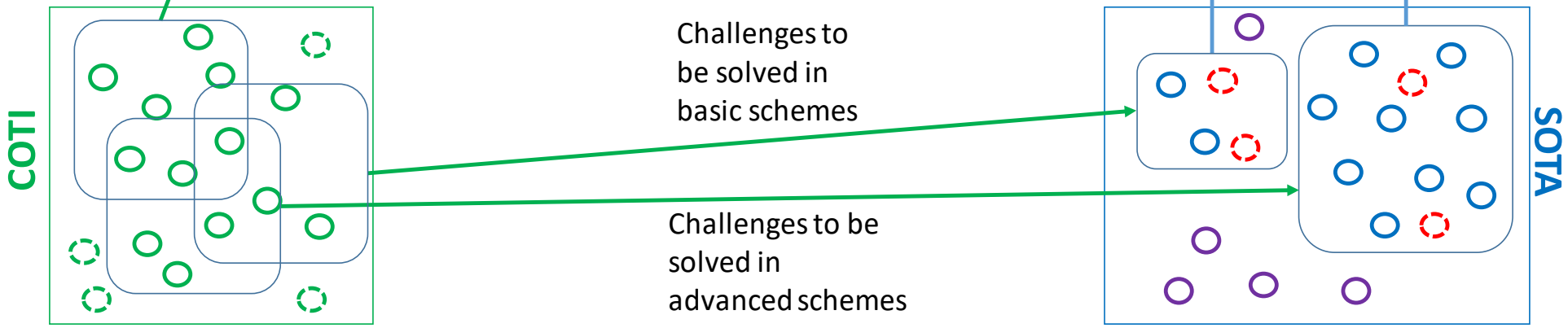
	Symbol (Example)	Assessment Type	Assurance Level	Scope of Security Functionality Level = min	Scope of Security Functionality > min	Schemes allowed
Advanced	A	Accredited Third Party	High	Sector/Use Case dependent	Sector / Use Case dependent	<mapping from SOTA>
	B	Accredited Third Party	Moderate			<mapping from SOTA>
	C	Accredited Third Party	Enhanced Basic			<mapping from SOTA>
Base	D	Accredited Third Party	Basic	Sector/Use Case agnostic		<mapping from SOTA>
	E	Self	Entry			

Not applicable
applicable
gap

Mapping Schemes appropriate for „advanced“

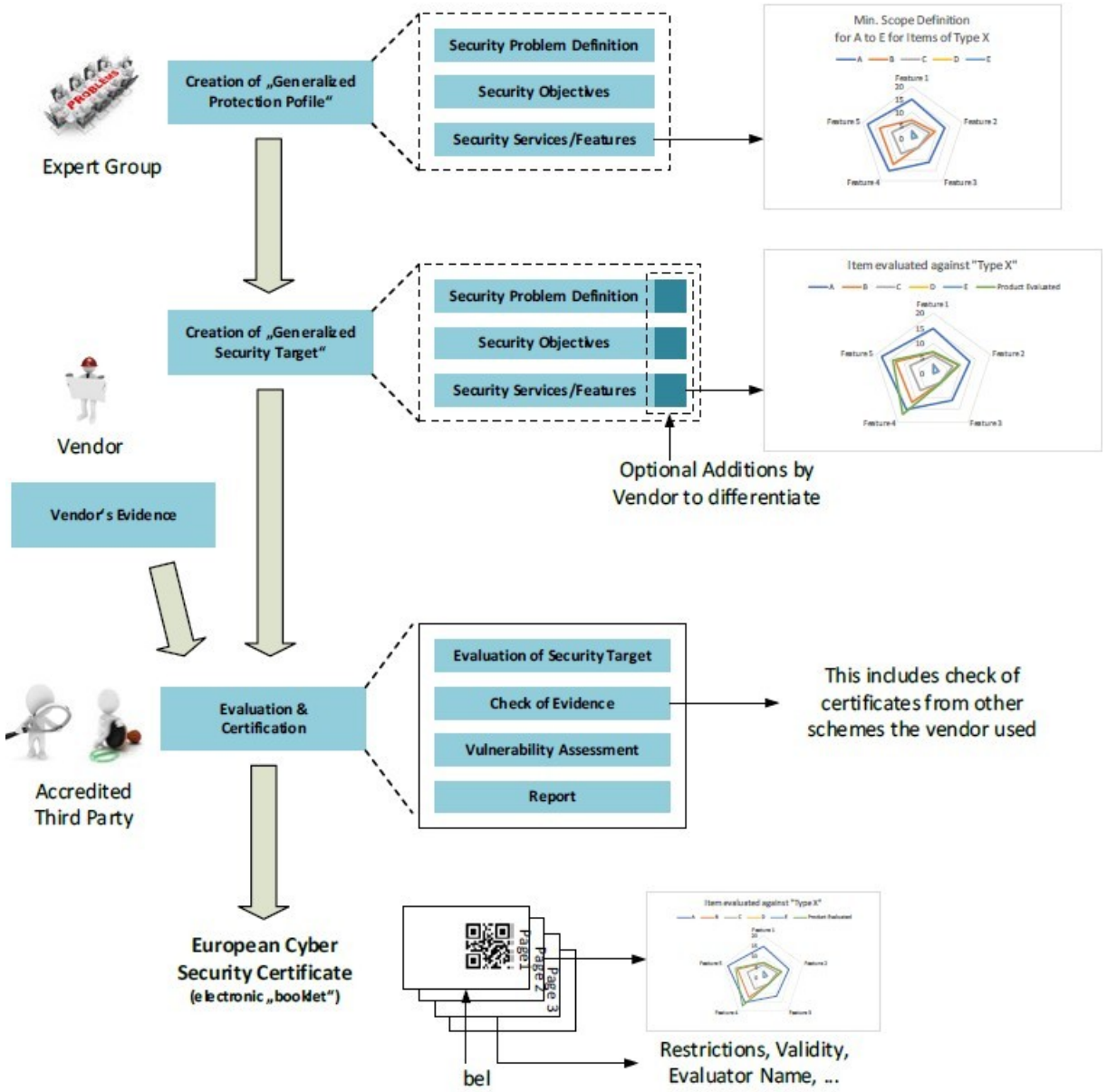
Mapping and of Schemes appropriate for „basic“

Challenges to be solved in meta-scheme level



ECSO : A meta-scheme approach

How to get to a label



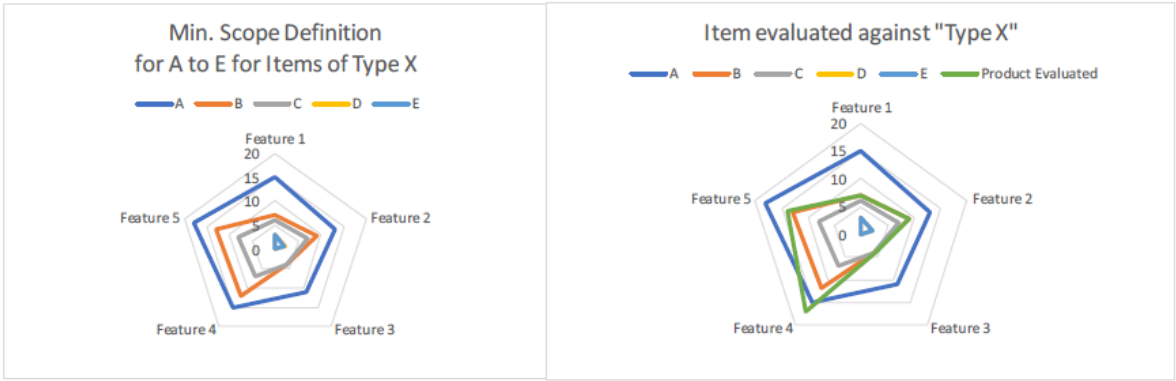


Figure 2 – Example for a Radar-Diagram to visualize Scope of Security Functionality.

Disclaimer: the example of a radar-diagram shall give an understanding that visualization could help a lot to get a feeling on what an item covers. For details in any case one needs to read the details underneath.

Contributing to a dynamic European IoT ecosystem
We aim to strengthen the dialogue and interaction among Internet of Things (IoT) players in Europe, and to contribute to the creation of a dynamic European IoT ecosystem to speed up the take up of IoT.
We are the **Alliance for Internet of Things Innovation**.
https://aioti.eu/

AIOTI - Security in IoT / State of the Art (SOTA)

AIOTI Workshop on Security and Privacy in IoT of 16 June 2016 initiated be the European Commission DG CONNECT

https://ec.europa.eu/digital-single-market/en/news/aioti-workshop-security-and-privacy-etsi-security-week

Final Report Workshop on Security and Privacy in IoT of 16 June 2016:

https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf

It is all about **Baseline Requirements on Security and Privacy in the hyper-connected World** related to

1. **Practical privacy in IoT**
2. **IoT hardware and components**
3. **Interfaces and communications**
4. **Applications**

Final Report European Commission of 13 January 2017 Workshop on Internet of Things Privacy and Security:

https://ec.europa.eu/digital-single-market/en/news/internet-things-privacy-security-workshops-report

-> Looking into Various Domains:

Wearables & Smart Appliance
Connected/Autonomous Vehicles
Industrial IoT
Smart Cities

Security in IoT / State of the Art (SOTA)

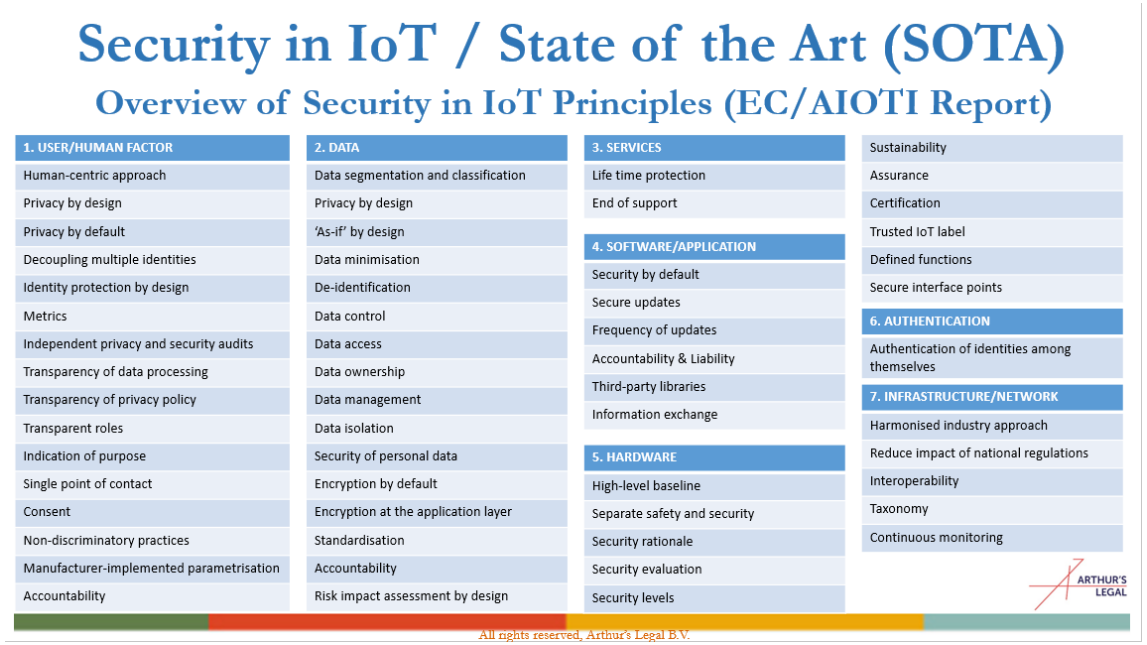
The first set of **Security & Privacy in IoT unique principles** that were found during those two workshop of/with the Commission – in total 58 –, structured in the SOTA way, and made available here https://www.arthurslegal.com/en/IoT

LAYERS:

- Service
- Software/Application
- Hardware
- Infrastructure/Network

DIMENSIONS:

- User/Human Factor
- Data
- Authentication



ARTHUR'S LEGAL

Faud Kahn - TwelveDot

Types of Labels (current)

Management Standards

Electrical and Safety Standards

Security Standards

Considerations when reading a label

- Jurisdiction
  - Some certifications are only for specific jurisdictions
  - i.e. US not global UL2900
- Standard
  - You should obtain a copy and read
  - Ask lots of questions
  - IEC 62443-2-1 – Requirements for IIoT System
- What is ”actually” measured
  - See bullet above you need to understand what is measured and how they measure it.
  - Is it repeatable or subjective to tester/evaluator?

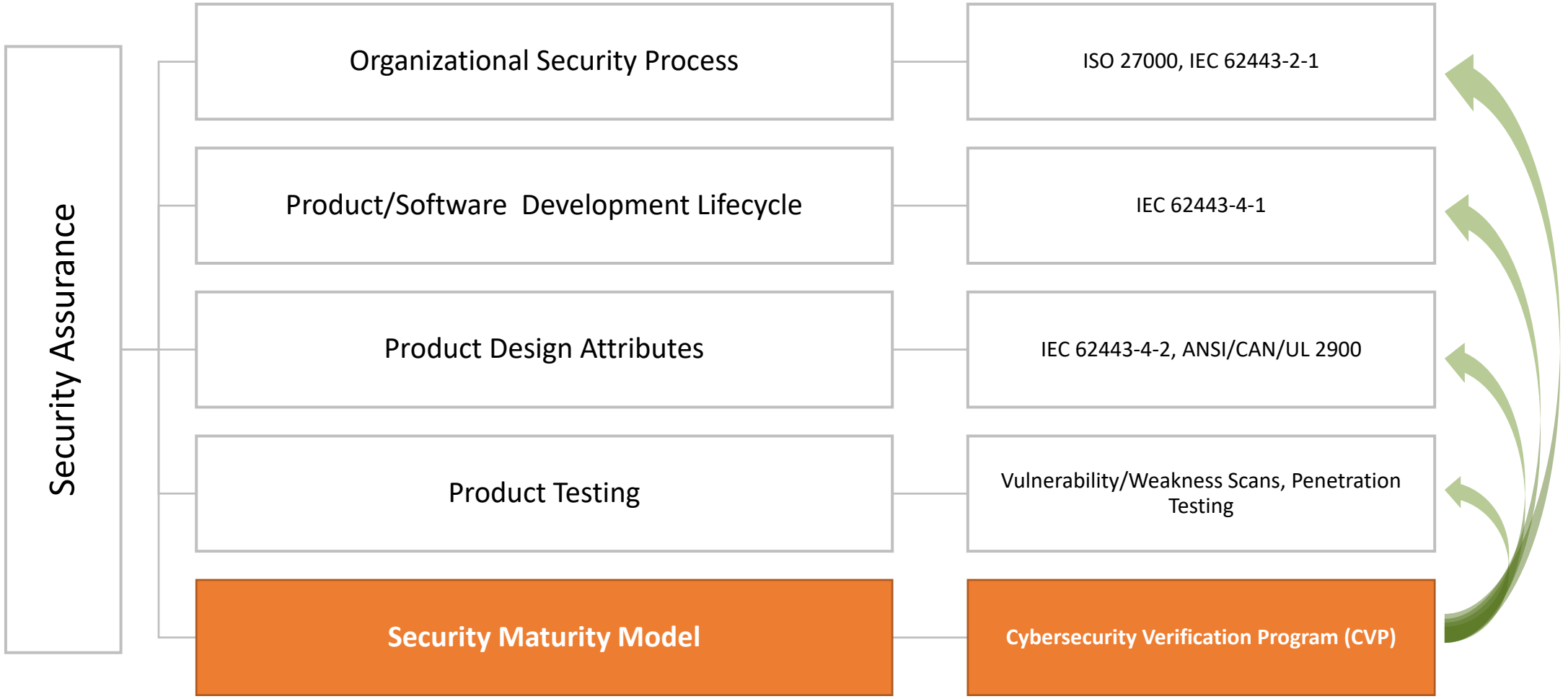
Cyber Label (Future)

- Requirements
  - What protections are the users provided?
  - How was it tested? (i.e. standard used)
  - What version was covered?
  - How was it configured when tested? i.e. home or commercial application
  - Were all components considered?
  - Was company maturity measured and considered?
- User/business must clearly understand the implications to the label and the configuration being tested and evaluated
- How does it relate to current regulatory requirements?

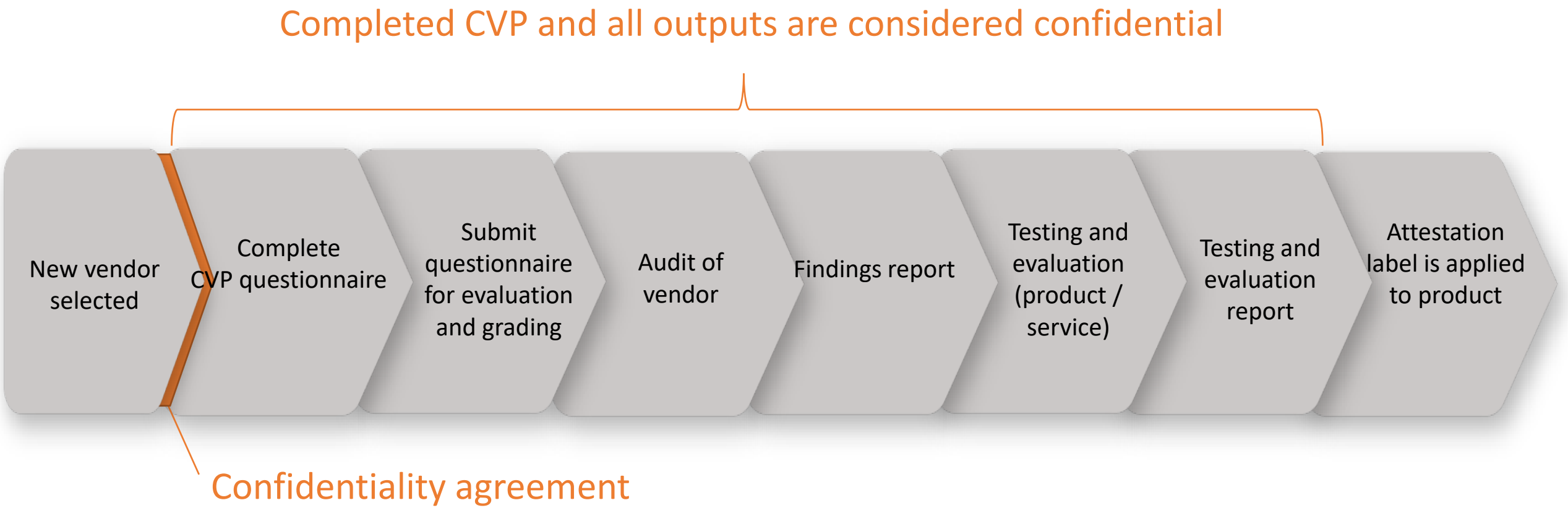
A Case Study

CSA Group Cyber Verification Program

Addressing Challenges Through Security Assessment



CVP Program Vision



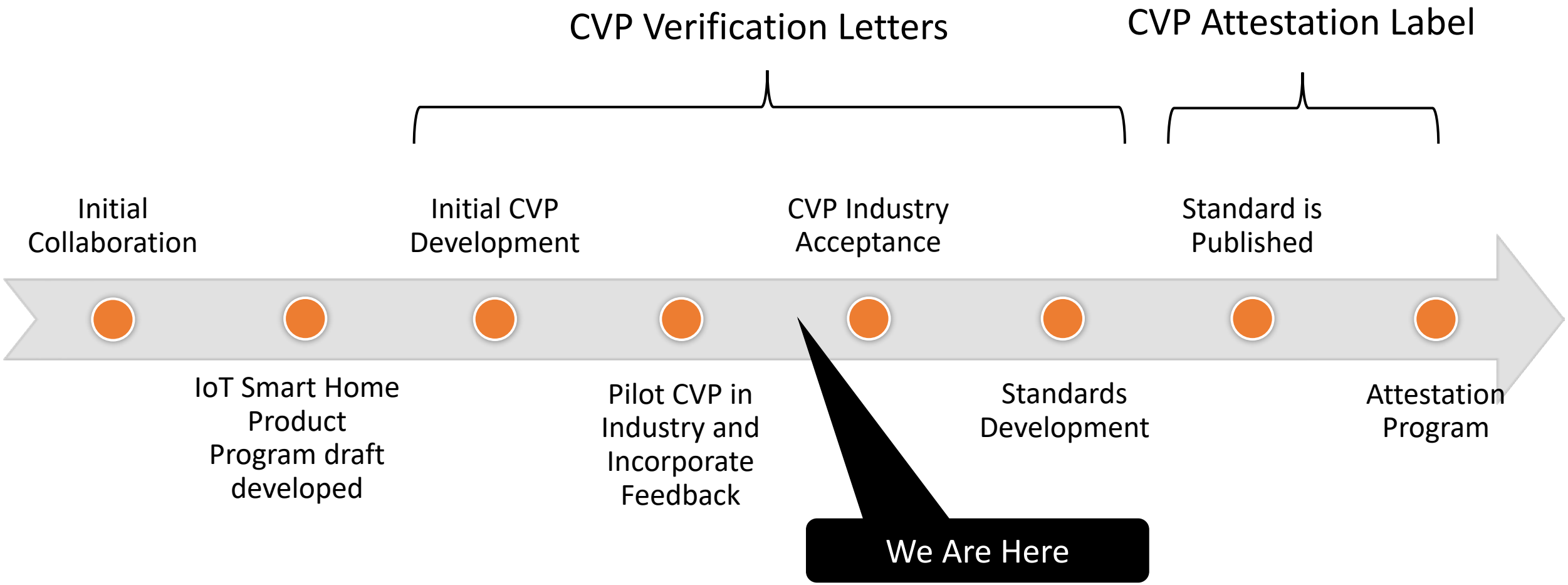
CVP Self-Assessment Methodology

1. Based on BSIMM to quantitatively benchmark cyber security aspects of an organization who develop products and services
2. Can be used across all technology sectors and services
3. Benchmarks observations in 6 key domains
    1. Four focused on governance and business practices
    2. Two focused on IoT products and development in-depth
4. Benchmark considers 18 practice areas
5. Allows companies to quickly identify areas for improvement

CVP Practice Areas

Strategies and Metrics	Penetration Testing	Code Review	Standards and Requirements	Security By Design	Asset Management
Attack Models	Compliance and Policy	Software Environment	Security Testing	Data Protection	Trustworthiness
Architecture Analysis	Security Features and Design	Training	Configuration Management and Vulnerability Management	Security Feature Set	Security Operations

CSA CVP Initiative



Questions?
Suggestions?

Maarten Botterman's bio

Maarten Botterman
Director GNKS Consult, Netherlands

- **Maarten Botterman** is Founder and Director of GNKS, a company known for its policy research on information society issues ("where technology meets society"). He is also Director on the Board of ICANN, Chairman of the Supervisory Board of NLnet Foundation, Chair of the IGF Dynamic Coalition on the Internet of Things, and Director on the Board of the Institute for Accountability in the Digital Age.
- Maarten is independent strategic policy advisor to governments and corporates on European, US and global information society policy issues related to the emergence and evolution of the Internet.
- He has been involved in Information Security policy, Data protection, Future Internet and Internet Governance, both as policy analyst (RAND, GNKS) and as Chairman on the Board of the third largest general Registry in the world (Public Interest Registry, serving .ORG and .NGO, a USA based non-profit business). He has been involved in studies and impact assessments around future internet and other ICT policy related studies since 1999.
- In the project PICASSO "ICT Policy, Research and Innovation for a Smart Society: towards new avenues in EU-US ICT collaboration", he chairs the EU-US ICT Policy Expert Group.

Prof. Dr. J.A.K. Cave's bio

Prof. Dr. J.A.K. Cave
Full Professor at Warwick University, United Kingdom
Economist member of the UK's Regulatory Policy Committee

- **Prof. Dr. J.A.K. Cave** is Professor in Economics at Warwick University. Jonathan Cave holds degrees from Yale (B.Sc.), Cambridge (MA), and Stanford (Ph.D.). In his position as Senior Economist at RAND Europe (up to February 2015), he has led projects on a variety of issues in telecommunications (transition from rate-of-return to price-cap regulation, legal issues arising on the electronic highway, universal service and the Internet), social policy (effects of aging European populations), industrial policy, and government's evolving role (passing on costs of government activity to private parties, market failure in the waste disposal industry, use of government procurement as a tool to spur innovation).

- Many of these projects involved international comparisons and teams spread across different organizations and nations. He is recently appointed as Economist member of the UK's Regulatory Policy Committee.

- Prof. Dr. J.A.K. Cave is member of the EU-US ICT Policy Expert Group in the project PICASSO "ICT Policy, Research and Innovation for a Smart Society: towards new avenues in EU-US ICT collaboration".

Jacques Kruse Brandao’s bio

Jacques is in the identification industry for >15y. As part of Security & Connectivity at NXP Jacques today **advocates partners on Security and Privacy in the hyper-connected world** explaining the related needs and the available solutions. Before Jacques was in charge of Business Development for emerging businesses in the field of **Cyber Security** in the **’IoT - Internet of Things’** focusing on ‘**Connected Systems’** like Smart Grid, Smart Metering, Smart City, Smart Home, Building Automation and Energy Management Solutions.

Today Jacques is actively engaged in shaping the regional and international agenda on cybersecurity together with stakeholders from various regional and international organizations. His passion is to generate a trustworthy connected world.

He is Member of the Board of the European Semiconductor Industry Association including Chair of their Task Force Encryption, Co-Chair of the AIOTI SWG Security, actively participating at ECSO, the European Cyber Security Organization and ENISA Security Expert Group as well as contributing to several other cybersecurity initiatives.

Linkedin: https://www.linkedin.com/in/jacqueskrusebrandao/

Contact: jacques-kruse-brandao@nxp.com

Faud Kahn

- Faud Khan is an industry veteran with more than 23 years of IT security experience with network equipment manufacturers, managed security services provider, financial services, and government agencies. As the CSA for TwelveDot and TwelveDot Labs, Faud is responsible for product strategy, architecture, deployment, and service delivery.
- His focus has been on security network architecture and application delivery through the Internet. This includes MSSPs, Carriers, and Telecom providers globally. Over this time, Faud has been granted 5 patents and has 9 patents pending.
- Currently, TwelveDot is providing security consulting and product development services to large enterprise, NEMs, and government agencies. With a focus on mobile, DNSSEC, smart grid, and cloud computing, his organizations are at the forefront of security risk management.
- Faud is active in ISO/IEC standardization and is the Chair of SMCSC27 the mirror committee to ISO/IEC SC27 in Canada. He is working on the development of standards related to ISMS, cloud computing, vulnerability disclosure, smart grid and IoT.