Re-usability of SESIP Certificates

Wouter Slegers at GP SESIP workshop in Austin 2022-05-14

TRUST AND VERIFY

Who is this Wouter Slegers?

- ✔ Founder and CEO of TrustCB
- ✔ 20+ years of experience in the security evaluation domain
- ✔ 30+ “innovative” evaluations, 80+ certifications, 8+ schemes setup, …
- ✔ Primary author of SESIP with Dirk-Jan Out (SGS Brightsight)





What does TrustCB do?

Make and operate optimized certification schemes

(including governance, requirements, methodology, standards)

What does a CB “sell”?

TRUSTCB
TRUST AND VERIFY

SESIP™

Certificate ID	SESIP-2100010-01
	TrustCB B.V. declares that
Product	W77Q16/32 version C
	of
Sponsor (and Developer)	Winbond Electronics Corporation *in* Taichung City, Taiwan
	complies to the requirements described in Standard and ST Reference
Standard	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1, June 2021 **Based on** Common Criteria for Information Technology Security Evaluation (CC) Parts 1-3, Version 3.1 Revision 5 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3)
ST Reference	Security Target for W77Q16/32 Secure Flash Memory, Version 1.5, 2022-03-02
	Summarised:
Assurance Package	SESIP2 *with* Physical Attacker Resistance
SESIP Profile	SESIP Profile for Secure External Memories v1.0
	As evaluated by:
Evaluation Facility	SGS Brightsight located in Barcelona, Spain
	Under scheme:
Scheme	SESIP *As described in* TrustCB Scheme Procedures v2.1
Validity	Date of issue: 2022-04-04 Date of expiry: 2024-03-02
Certification Mark	SESIP™2.0
Signatory	Wouter Slegers, CEO

TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com | Van den Berghlaan 48, 2132 AT Hoofddorp, The Netherlands

TRUSTCB

What does a CB “sell”?

TRUSTCB
TRUST AND VERIFY

SESIP™

Certificate ID	SESIP-2100010-01
	TrustCB B.V. declares that
Product	W77Q16/32 version C
	of
Sponsor (and Developer)	Winbond Electronics Corporation *in* Taichung City, Taiwan
	complies to the requirements de… and ST Reference
	Gl… Information Technology, Security Evaluation Standard for … Platforms (ESSP_GP_FST_070, Public … 1.1, Jun…
	Ba… Common Criteria for Information Technology Security Evaluation (CC) Parts 1-3, Version 3.1 Revision 5 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3)
…ference	Security Target for W77Q16/32 Secure Flash Memory, Version 1.5, 2022-03-02
	Su…
Assuran… Package	SE… with … Physical … Resi…
SESIP Profile	SESIP Profile for Secure External Memories v1.0
	As evaluated by:
Evaluation Facility	SGS Brightsight located in Barcelona, Spain
	Under scheme:
Scheme	St… As … Tr… CB Scheme Procedures v2…
Validity	Date of issue: 2022-04-04 Date of expiry: 2024-03-02
Certification Mark	SESIP™2.0
Signatory	Wouter Slegers, CEO

TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com | Van den Berghlaan 48, 2132 AT Hoofddorp, The Netherlands

Trusted CB says “it is good” (for me)

TRUSTCB

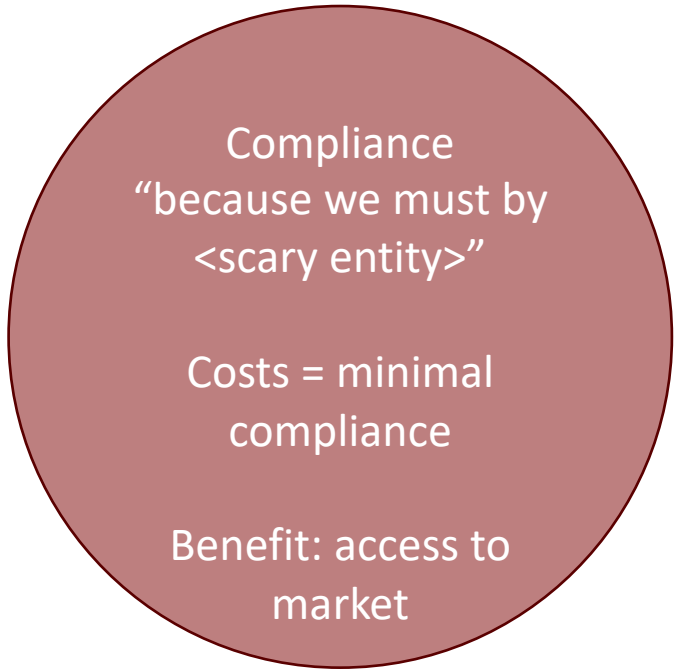
Why to buy certification: 3 Reasons

Underlying reasons to certify

Successful re-use requirements

TRUSTCB

Reasons to certify and finances/motivation



Essence: minimal compliance

Difficulty: alignment compliance requirements under pressue

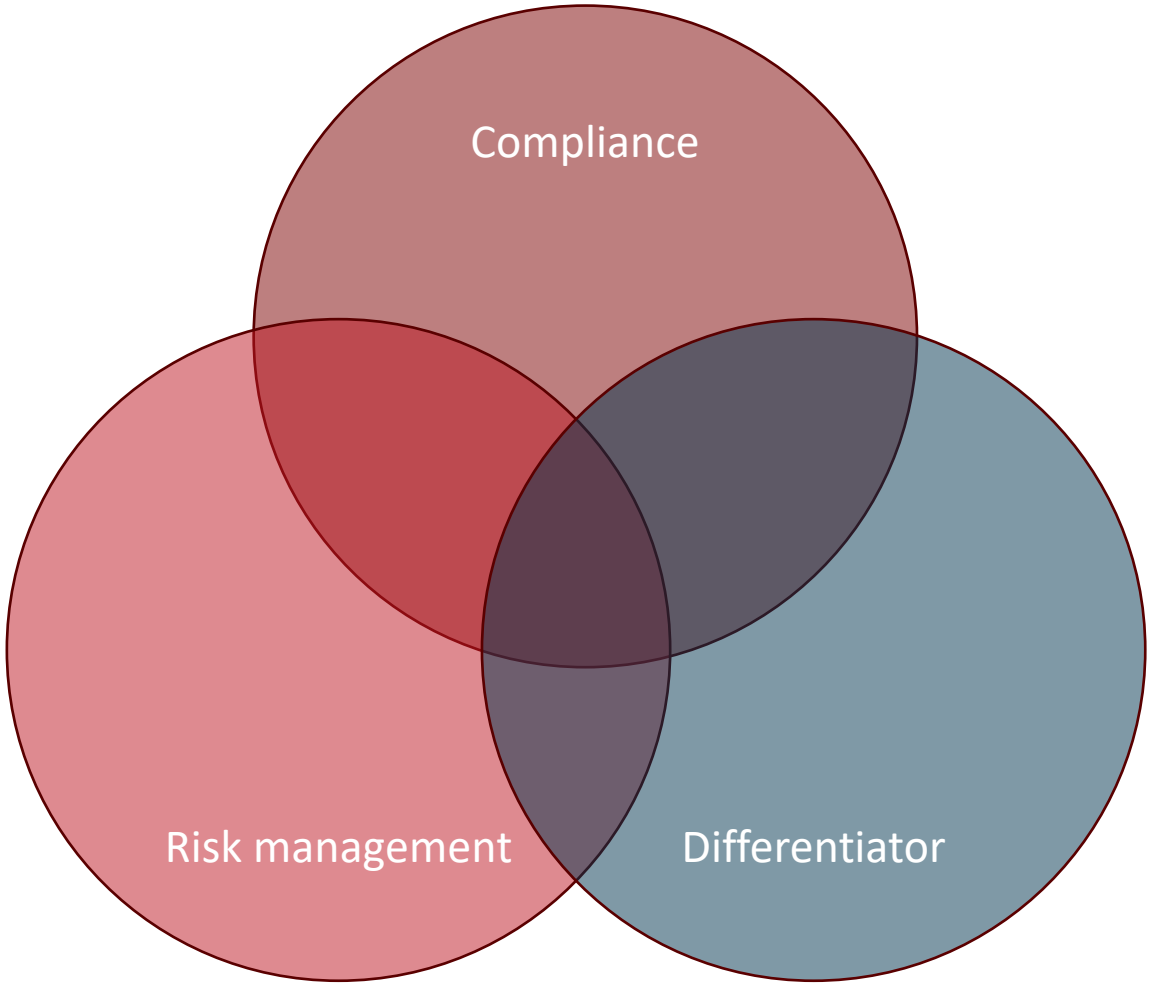
Essence: shown risk reduction

Difficulty: show risk reduction and make small steps valuable

Essence: brand has value

Difficulty: brand must have value to end-user

Reasons and value of certification can overlap



What does a CB “sell”?

TRUSTCB
TRUST AND VERIFY

SESIP™

Certificate ID	SESIP-2100010-01
	TrustCB B.V. declares that
Product	W77Q16/32 version C
	of
Sponsor (and Developer)	Winbond Electronics Corporation *in* Taichung City, Taiwan
	complies to the requirements de… and ST Reference
	Gl… Information Technology, Security Evaluation Standard for … Platforms (ESSP_GP_FST_070, Public … 1.1, Jun…
	Ba… Common Criteria for Information Technology Security Evaluation (CC) Parts 1-3, Version 3.1 Revision 5 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3)
…ference	Security Target for W77Q16/32 Secure Flash Memory, Version 1.5, 2022-03-02
	Su…
Assuran… Package	SE… with … Physical … Resi…
SESIP Profile	SESIP Profile for Secure External Memories v1.0
	As evaluated by:
Evaluation Facility	SGS Brightsight located in Barcelona, Spain
	Under scheme:
Scheme	St… As … Tr… CB Scheme Procedures v2…
Validity	Date of issue: 2022-04-04 Date of expiry: 2024-03-02
Certification Mark	SESIP™2.0
Signatory	Wouter Slegers, CEO

TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com | Van den Berghlaan 48, 2132 AT Hoofddorp, The Netherlands

Trusted CB says “it is good” (for me)

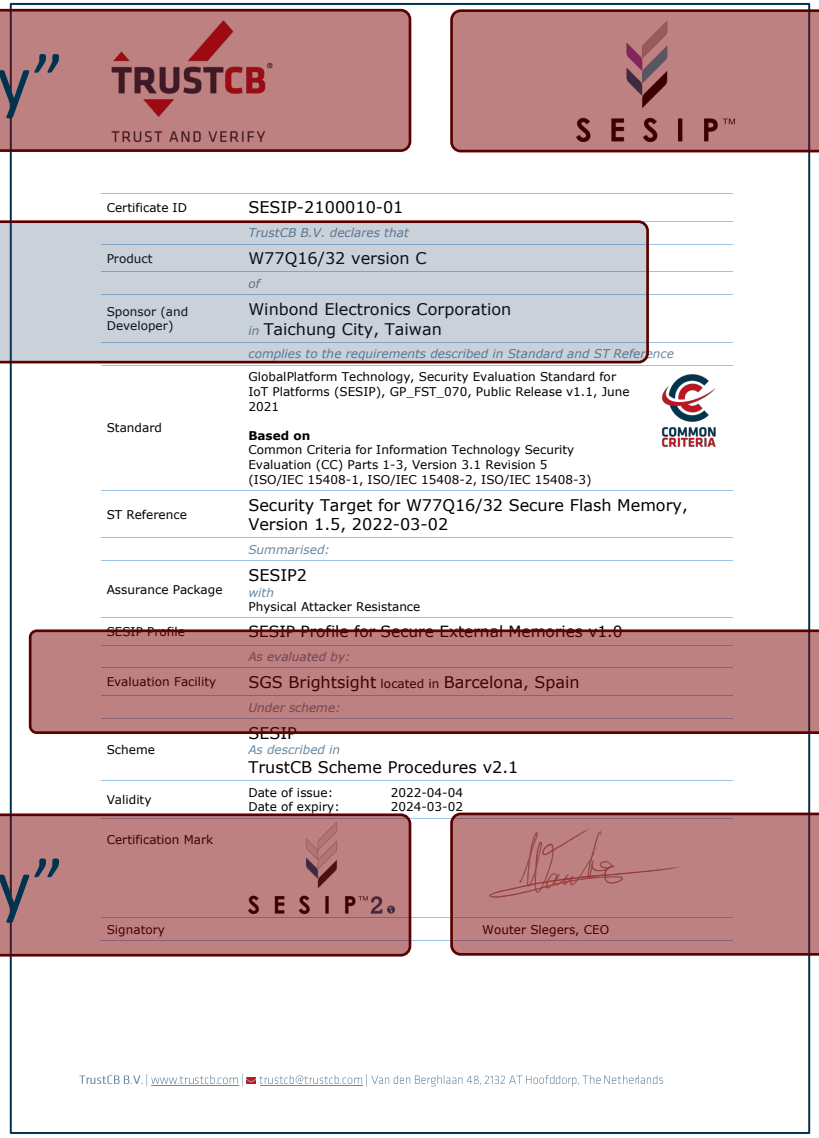
TRUSTCB

What is the value for you as customer?

Brand for ”quality security”

Brand for ”quality security”

Product



Certificate ID	SESIP-2100010-01
	TrustCB B.V. declares that
Product	W77Q16/32 version C
	of
Sponsor (and Developer)	Winbond Electronics Corporation *in* Taichung City, Taiwan
	complies to the requirements described in Standard and ST Reference
Standard	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1, June 2021 **Based on** Common Criteria for Information Technology Security Evaluation (CC) Parts 1-3, Version 3.1 Revision 5 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3)
ST Reference	Security Target for W77Q16/32 Secure Flash Memory, Version 1.5, 2022-03-02
	Summarised:
Assurance Package	SESIP2 *with* Physical Attacker Resistance
~~SESIP Profile~~	~~SESIP Profile for Secure External Memories v1.0~~
	As evaluated by:
Evaluation Facility	SGS Brightsight located in Barcelona, Spain
	Under scheme:
Scheme	~~SESIP~~ *As described in* TrustCB Scheme Procedures v2.1
Validity	Date of issue: 2022-04-04 Date of expiry: 2024-03-02
Certification Mark	SESIP2
Signatory	Wouter Slegers, CEO

TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com | Van den Berghlaan 48, 2132 AT Hoofddorp, The Netherlands

Brand for ”quality security”

Brand for ”quality security”

Brand for ”quality security”

Brand for ”quality security”

What is the value for you as customer?

Brand for ”quality security”

Brand for ”quality security”

Brand for ”quality security”

Brand for ”quality security”

Brand for ”quality security”

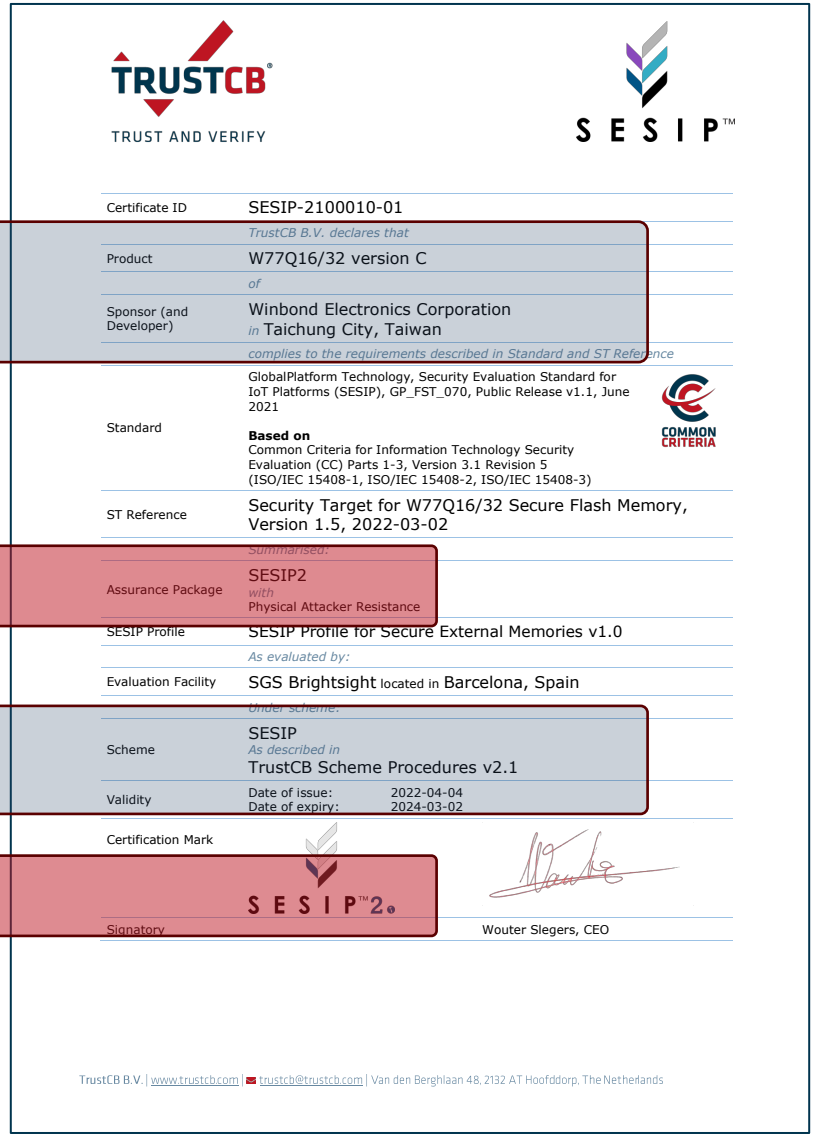
What is the value for your customer?

Product

Strength of attacker

Validity limits

Strength of attacker



TRUSTCB
TRUST AND VERIFY

SESIP™

Certificate ID	SESIP-2100010-01
	TrustCB B.V. declares that
Product	W77Q16/32 version C
	of
Sponsor (and Developer)	Winbond Electronics Corporation *in* Taichung City, Taiwan
	complies to the requirements described in Standard and ST Reference
Standard	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1, June 2021 **Based on** Common Criteria for Information Technology Security Evaluation (CC) Parts 1-3, Version 3.1 Revision 5 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3)
ST Reference	Security Target for W77Q16/32 Secure Flash Memory, Version 1.5, 2022-03-02
	Summarised:
Assurance Package	SESIP2 *with* Physical Attacker Resistance
SESIP Profile	SESIP Profile for Secure External Memories v1.0
	As evaluated by:
Evaluation Facility	SGS Brightsight located in Barcelona, Spain
	Under scheme:
Scheme	SESIP *As described in* TrustCB Scheme Procedures v2.1
Validity	Date of issue: 2022-04-04 Date of expiry: 2024-03-02
Certification Mark	SESIP2
Signatory	Wouter Slegers, CEO

TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com | Van den Berghlaan 48, 2132 AT Hoofddorp, The Netherlands

TRUSTCB

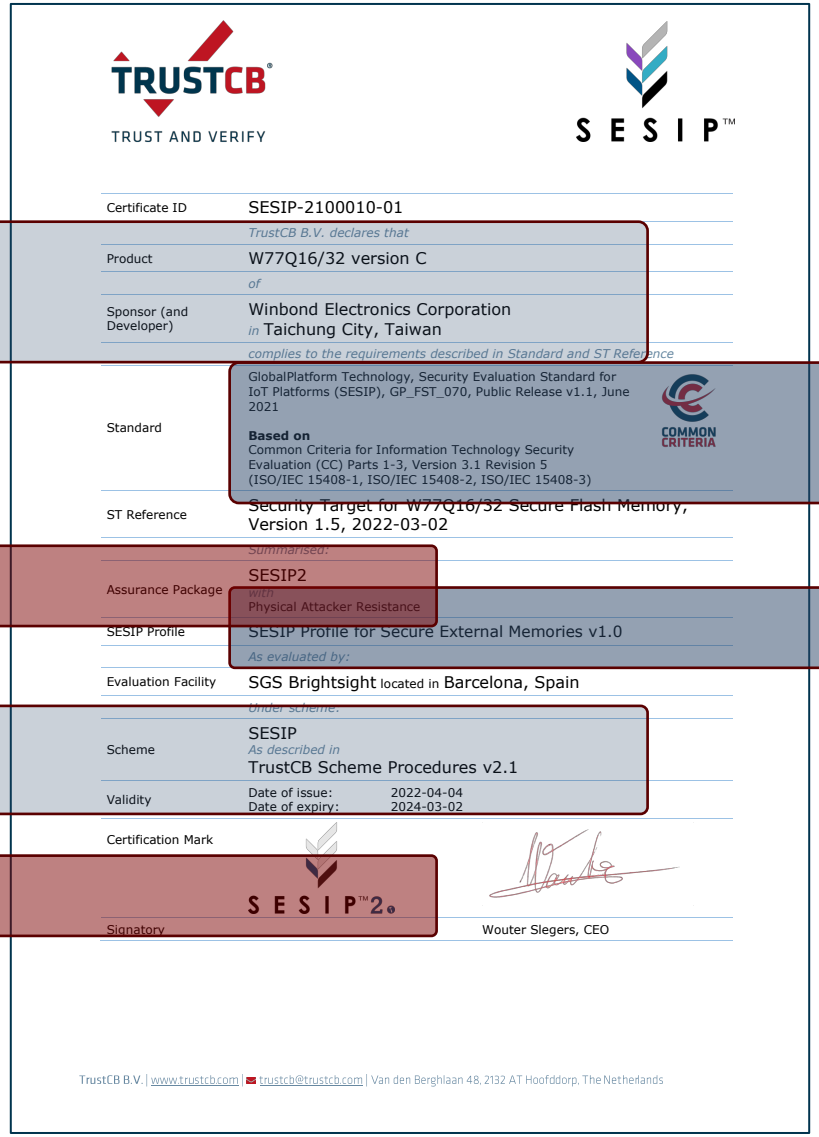
What is the real value for you and your customer?

Product

Strength of attacker

Validity limits

Strength of attacker



TRUSTCB
TRUST AND VERIFY

SESIP™

Certificate ID	SESIP-2100010-01
	TrustCB B.V. declares that
Product	W77Q16/32 version C
	of
Sponsor (and Developer)	Winbond Electronics Corporation *in* Taichung City, Taiwan
	complies to the requirements described in Standard and ST Reference
Standard	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1, June 2021 **Based on** Common Criteria for Information Technology Security Evaluation (CC) Parts 1-3, Version 3.1 Revision 5 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3)
ST Reference	Security Target for W77Q16/32 Secure Flash Memory, Version 1.5, 2022-03-02
	Summarised:
Assurance Package	SESIP2 *with* Physical Attacker Resistance
SESIP Profile	SESIP Profile for Secure External Memories v1.0
	As evaluated by:
Evaluation Facility	SGS Brightsight located in Barcelona, Spain
	Under Scheme:
Scheme	SESIP *As described in* TrustCB Scheme Procedures v2.1
Validity	Date of issue: 2022-04-04 Date of expiry: 2024-03-02
Certification Mark	SESIP™2
Signatory	Wouter Slegers, CEO

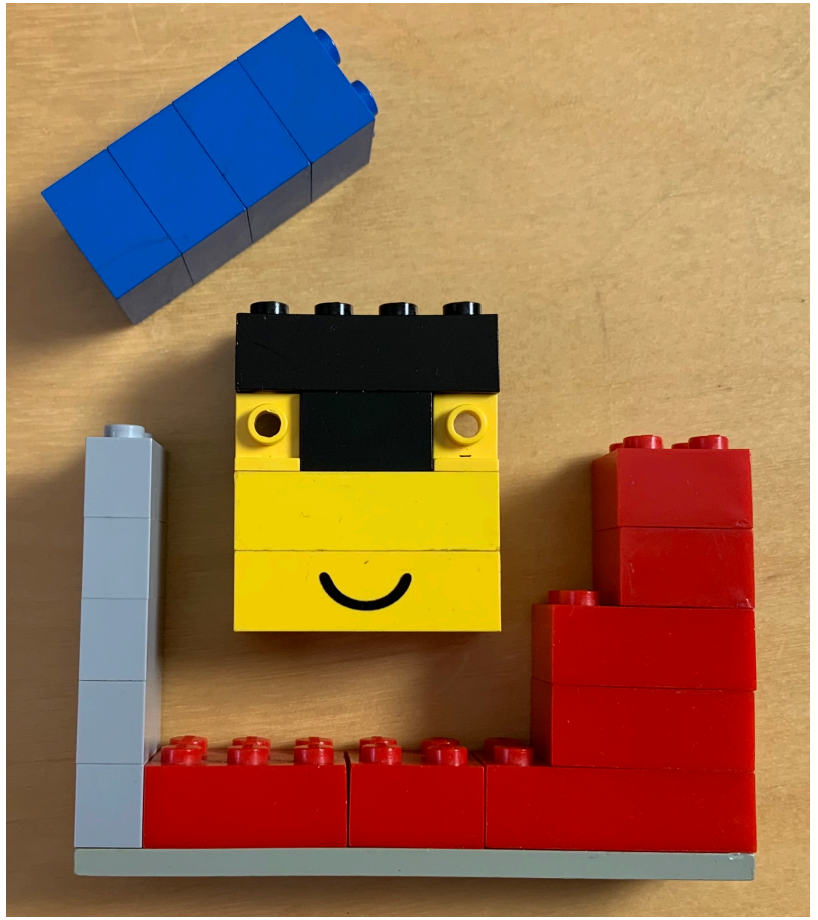
TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com | Van den Berghlaan 48, 2132 AT Hoofddorp, The Netherlands

Re-use possibilities

Domain specific security

TRUSTCB

SESIP -> SESIP



Re-use in SESIP

Must be recognized CB

Must be GP SESIP licensed

Use SFRs

Needs to be valid

Certificate ID	SESIP-2100010-01
	TrustCB B.V. declares that
Product	W77Q16/32 version C
	of
Sponsor (and Developer)	Winbond Electronics Corporation *in* Taichung City, Taiwan
	complies to the requirements described in Standard and ST Reference
Standard	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1, June 2021 **Based on** Common Criteria for Information Technology Security Evaluation (CC) Parts 1-3, Version 3.1 Revision 5 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3)
ST Reference	Security Target for W77Q16/32 Secure Flash Memory, Version 1.5, 2022-03-02
	Summarised:
Assurance Package	SESIP2 *with* Physical Attacker Resistance
SESIP Profile	SESIP Profile for Secure External Memories v1.0
	As evaluated by:
Evaluation Facility	SGS Brightsight located in Barcelona, Spain
	Under Scheme:
Scheme	SESIP *As described in* TrustCB Scheme Procedures v2.1
Validity	Date of issue: 2022-04-04 Date of expiry: 2024-03-02
Certification Mark	SESIP 2.0
Signatory	Wouter Slegers, CEO

TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com | Van den Berghlaan 48, 2132 AT Hoofddorp, The Netherlands

PSA Certified

- Co-developed with SESIP
- Two paths: original CSPN-inspired and SESIP
- SESIP Profiles are available
  < https://www.psacertified.org/development-resources/certification-resources/>
- One evaluation, two certificates
- Requires use TrustCB as CB

psacertified™

Re-use for PSA Certified

psacertified™

Must be TrustCB

Must be SESIP

Certificate ID	SESIP-2100010-01
	TrustCB B.V. declares that
Product	W77Q16/32 version C
	of
Sponsor (and Developer)	Winbond Electronics Corporation *in* Taichung City, Taiwan
	complies to the requirements described in Standard and ST Reference
Standard	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1, June 2021 **Based on** Common Criteria for Information Technology Security Evaluation (CC) Parts 1-3, Version 3.1 Revision 5 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3)
ST Reference	Security Target for W77Q16/32 Secure Flash Memory, Version 1.5, 2022-03-02
	Summarised:
Assurance Package	SESIP2 *with* Physical Attacker Resistance
SESIP Profile	SESIP Profile for Secure External Memories v1.0
	As evaluated by:
Evaluation Facility	SGS Brightsight located in Barcelona, Spain
	Under Scheme:
Scheme	SESIP *As described in* TrustCB Scheme Procedures v2.1
Validity	Date of issue: 2022-04-04 Date of expiry: 2024-03-02
Certification Mark	SESIP™2.0
Signatory	Wouter Slegers, CEO

TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com | Van den Berghlaan 48, 2132 AT Hoofddorp, The Netherlands

Needs to claim PSA Certified Profile

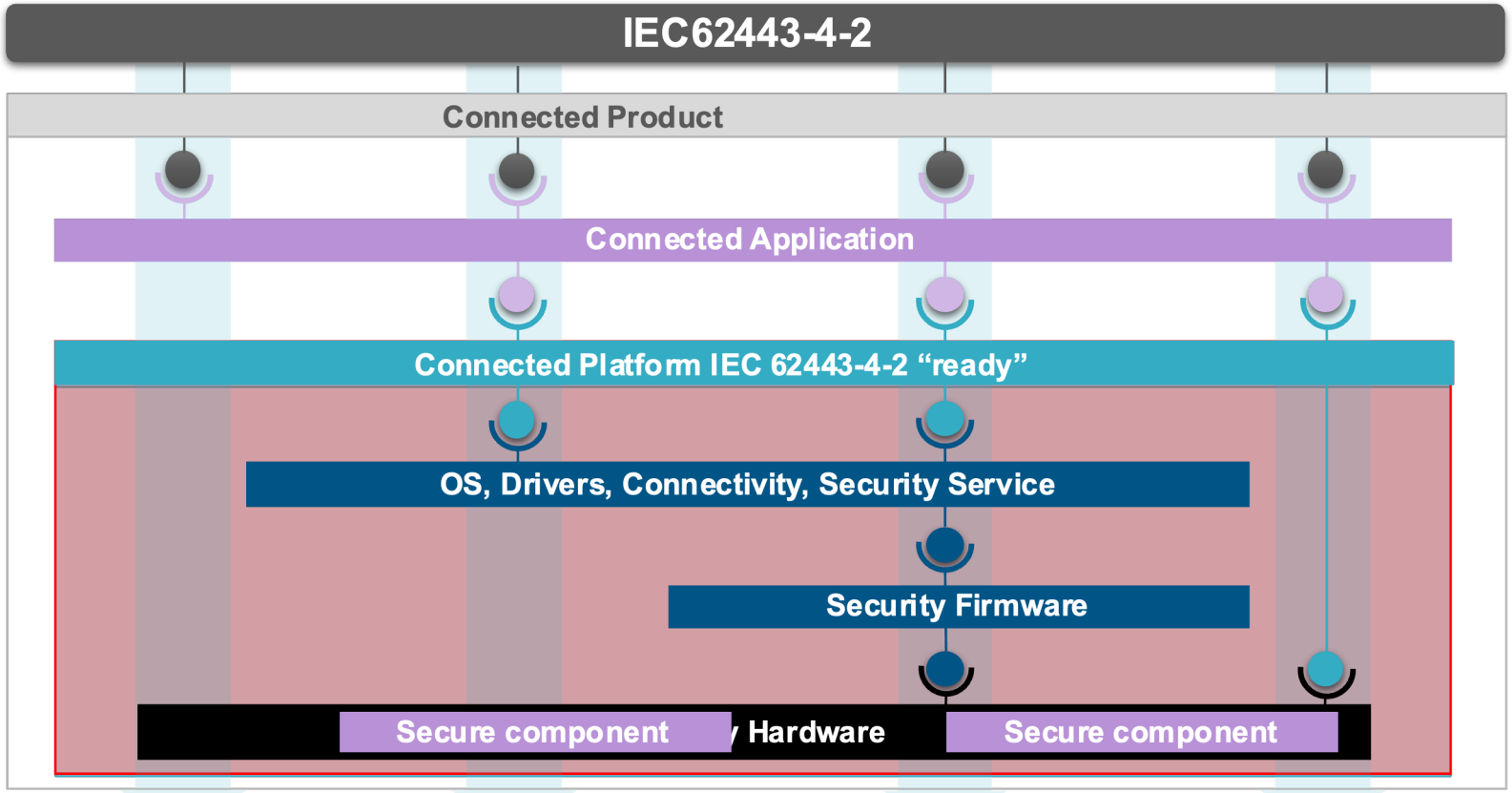
Needs to be valid

TRUSTCB

ISA/IEC 62443

- ISA Secure accreditation:
  - Scheme is long operational and methodology available
  - SESIP recognition possible via CB (both ISA and SESIP accredited)
- IEC accreditation:
  - No schemes, methodology under construction
  - SESIP recognition unknown
- No accreditation:
  - Private schemes operational, no mutual recognition
  - SESIP recognition depends on CB reputation
- Mappings almost completed

Composition model



Re-use for 62443 (ISA Secure)

Must be TrustCB

Must be SESIP

Needs to claim (parts) of 62443-4-2 mapping

Needs to be valid

Strength of attacker matches SLx

TRUSTCB
TRUST AND VERIFY

SESIP™

Certificate ID	SESIP-2100010-01
	TrustCB B.V. declares that
Product	W77Q16/32 version C
	of
Sponsor (and Developer)	Winbond Electronics Corporation *in* Taichung City, Taiwan
	complies to the requirements described in Standard and ST Reference
Standard	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1, June 2021 **Based on** Common Criteria for Information Technology Security Evaluation (CC) Parts 1-3, Version 3.1 Revision 5 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3)
ST Reference	Security Target for W77Q16/32 Secure Flash Memory, Version 1.5, 2022-03-02
	Summarised:
Assurance Package	SESIP2 *with* Physical Attacker Resistance
SESIP Profile	SESIP Profile for Secure External Memories v1.0
	As evaluated by:
Evaluation Facility	SGS Brightsight *located in* Barcelona, Spain
	Under Scheme:
Scheme	SESIP *As described in* TrustCB Scheme Procedures v2.1
Validity	Date of issue: 2022-04-04 Date of expiry: 2024-03-02
Certification Mark	SESIP™2
Signatory	Wouter Slegers, CEO

TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com | Van den Berghlaan 48, 2132 AT Hoofddorp, The Netherlands

TRUSTCB

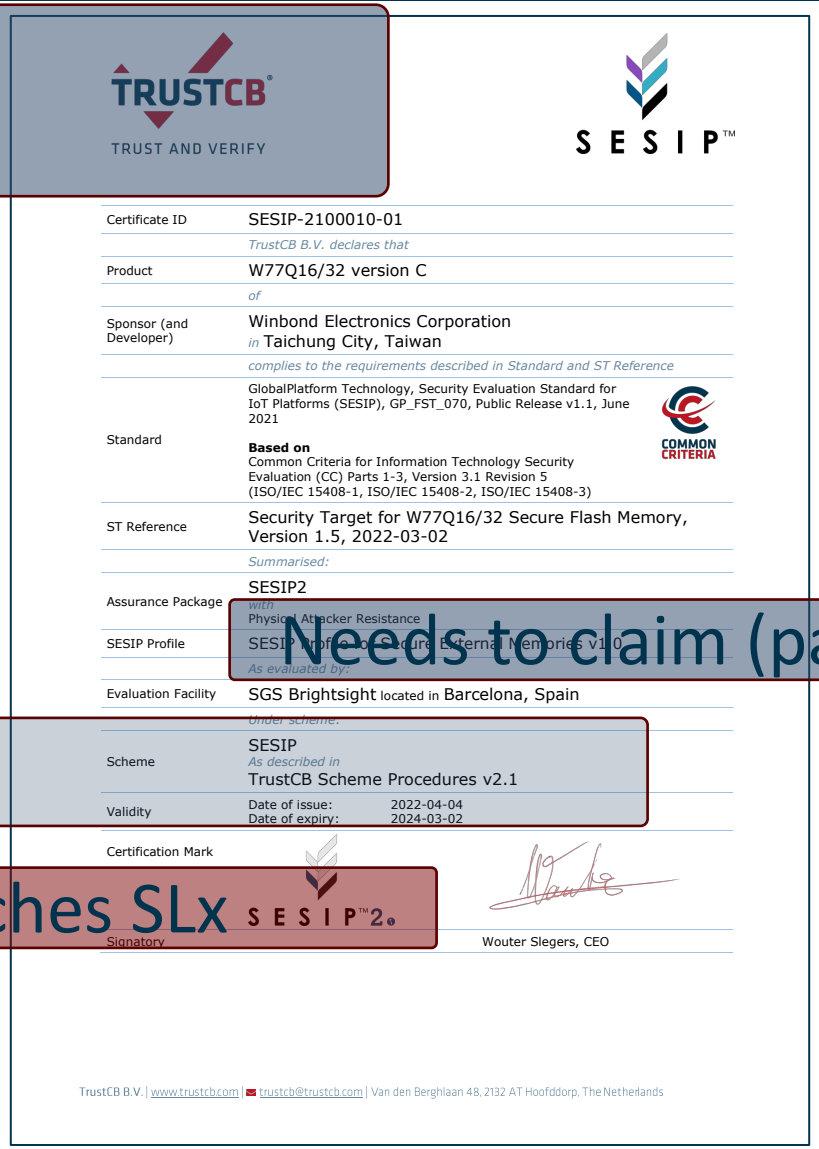
Re-use for 62443 (IEC or unstructured)

Trusted by 62443 CB

Needs to be valid

Strength of attacker matches SLx

Needs to claim (parts) of 62443-4-2 mapping



TRUSTCB
TRUST AND VERIFY

SESIP™

Certificate ID	SESIP-2100010-01
	TrustCB B.V. declares that
Product	W77Q16/32 version C
	of
Sponsor (and Developer)	Winbond Electronics Corporation *in* Taichung City, Taiwan
	complies to the requirements described in Standard and ST Reference
Standard	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1, June 2021 **Based on** Common Criteria for Information Technology Security Evaluation (CC) Parts 1-3, Version 3.1 Revision 5 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3)
ST Reference	Security Target for W77Q16/32 Secure Flash Memory, Version 1.5, 2022-03-02
	Summarised:
Assurance Package	SESIP2 *with* Physical Attacker Resistance
SESIP Profile	SESIP Profile for Secure External Memories v1.0
	As evaluated by:
Evaluation Facility	SGS Brightsight located in Barcelona, Spain
	Under Scheme:
Scheme	SESIP *As described in* TrustCB Scheme Procedures v2.1
Validity	Date of issue: 2022-04-04 Date of expiry: 2024-03-02
Certification Mark	SESIP™2
Signatory	Wouter Slegers, CEO

TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com | Van den Berghlaan 48, 2132 AT Hoofddorp, The Netherlands

TRUSTCB

Security Level 62443 mapping

Strength of attacker matches SLx

Re-use for EN 303 645 / NIST 8259A / …

Must be trusted

Needs to be valid

Needs to claim (parts) of mapping

TRUSTCB
TRUST AND VERIFY

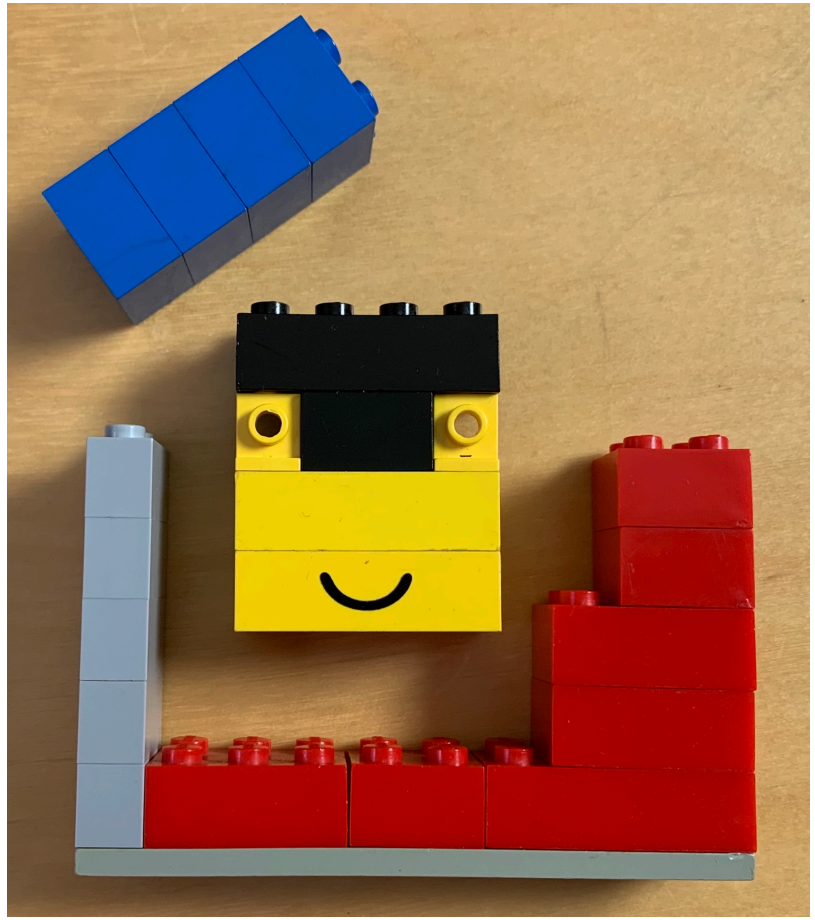
SESIP™

Certificate ID	SESIP-2100010-01
	TrustCB B.V. declares that
Product	W77Q16/32 version C
	of
Sponsor (and Developer)	Winbond Electronics Corporation *in* Taichung City, Taiwan
	complies to the requirements described in Standard and ST Reference
Standard	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1, June 2021 **Based on** Common Criteria for Information Technology Security Evaluation (CC) Parts 1-3, Version 3.1 Revision 5 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3)
ST Reference	Security Target for W77Q16/32 Secure Flash Memory, Version 1.5, 2022-03-02
	Summarised:
Assurance Package	SESIP2 *with* Physical Attacker Resistance
SESIP Profile	SESIP Profile for Secure External Memories v1.
	As evaluated by:
Evaluation Facility	SGS Brightsight located in Barcelona, Spain
	Under Scheme:
Scheme	SESIP *As described in* TrustCB Scheme Procedures v2.1
Validity	Date of issue: 2022-04-04 Date of expiry: 2024-03-02
Certification Mark	SESIP™2.0
Signatory	Wouter Slegers, CEO

TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com | Van den Berghlaan 48, 2132 AT Hoofddorp, The Netherlands

TRUSTCB

CC -> SESIP

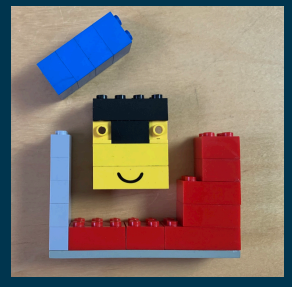


TRUSTCB

TRUST AND VERIFY

TrustCB SESIP Scheme Interpretation 1:
Re-use of CC certification results
Version 1.0

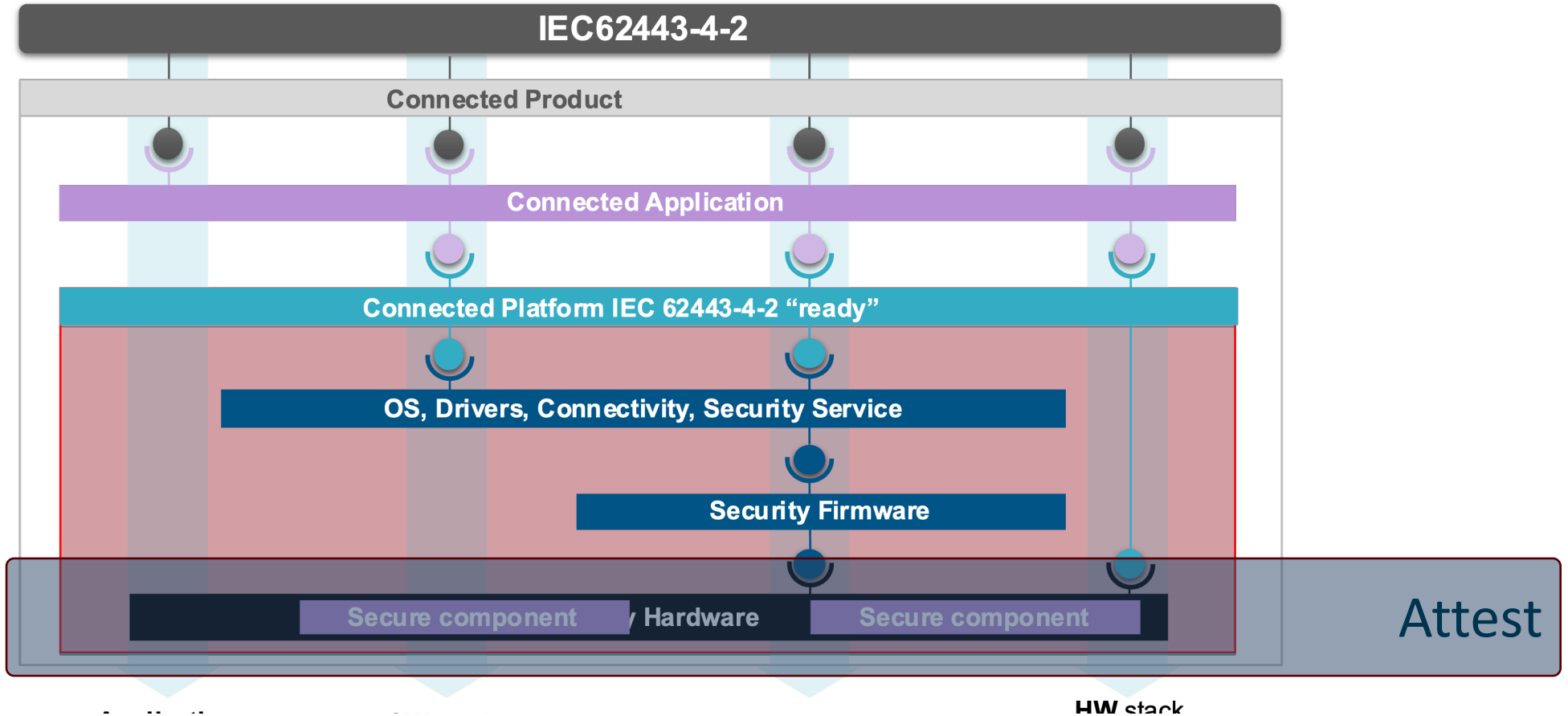
<not yet public>



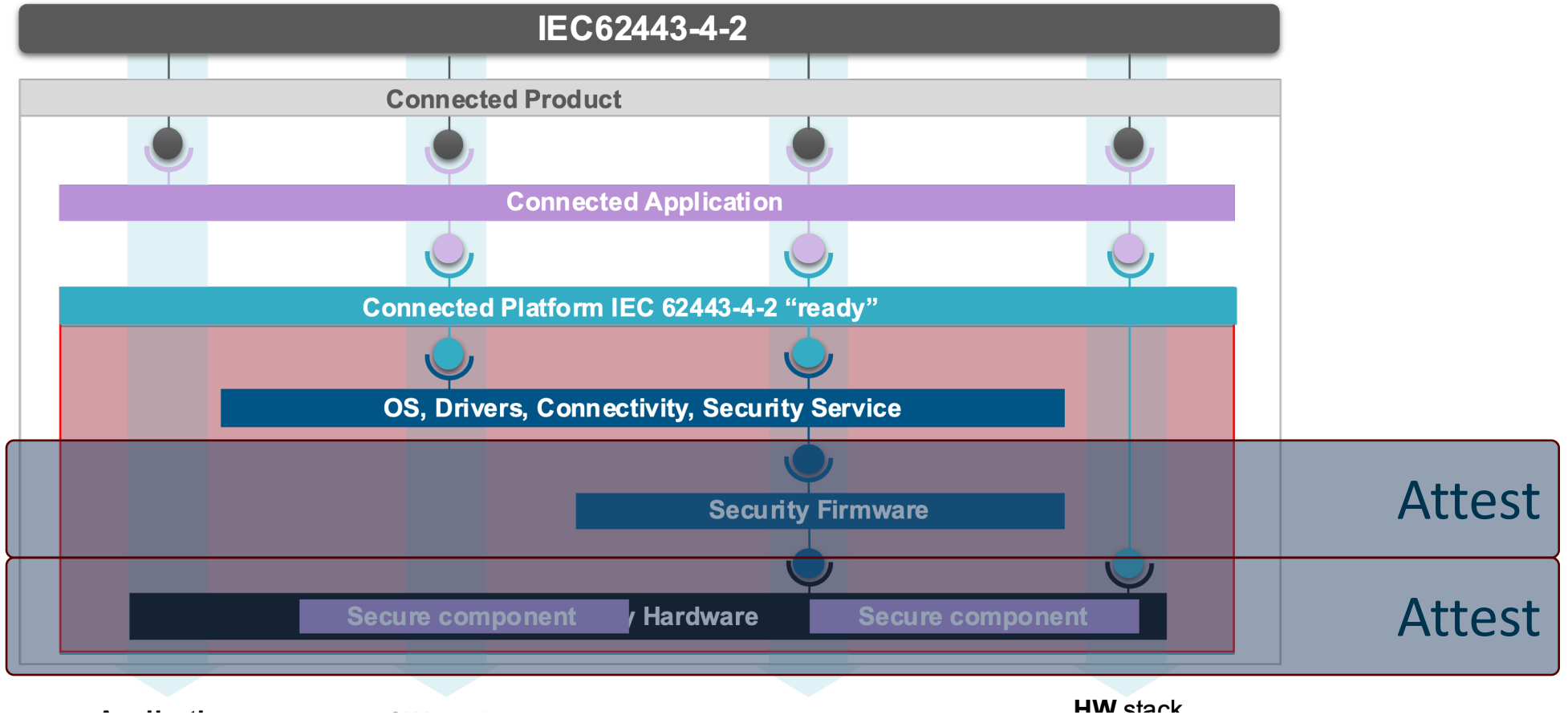
- SESIP3 + re-use of CC EAL4+AVA_VAN.5 Secure Element
- SESIP Profiles will be made
- Scheme owner requires use TrustCB as CB

TRUSTCB

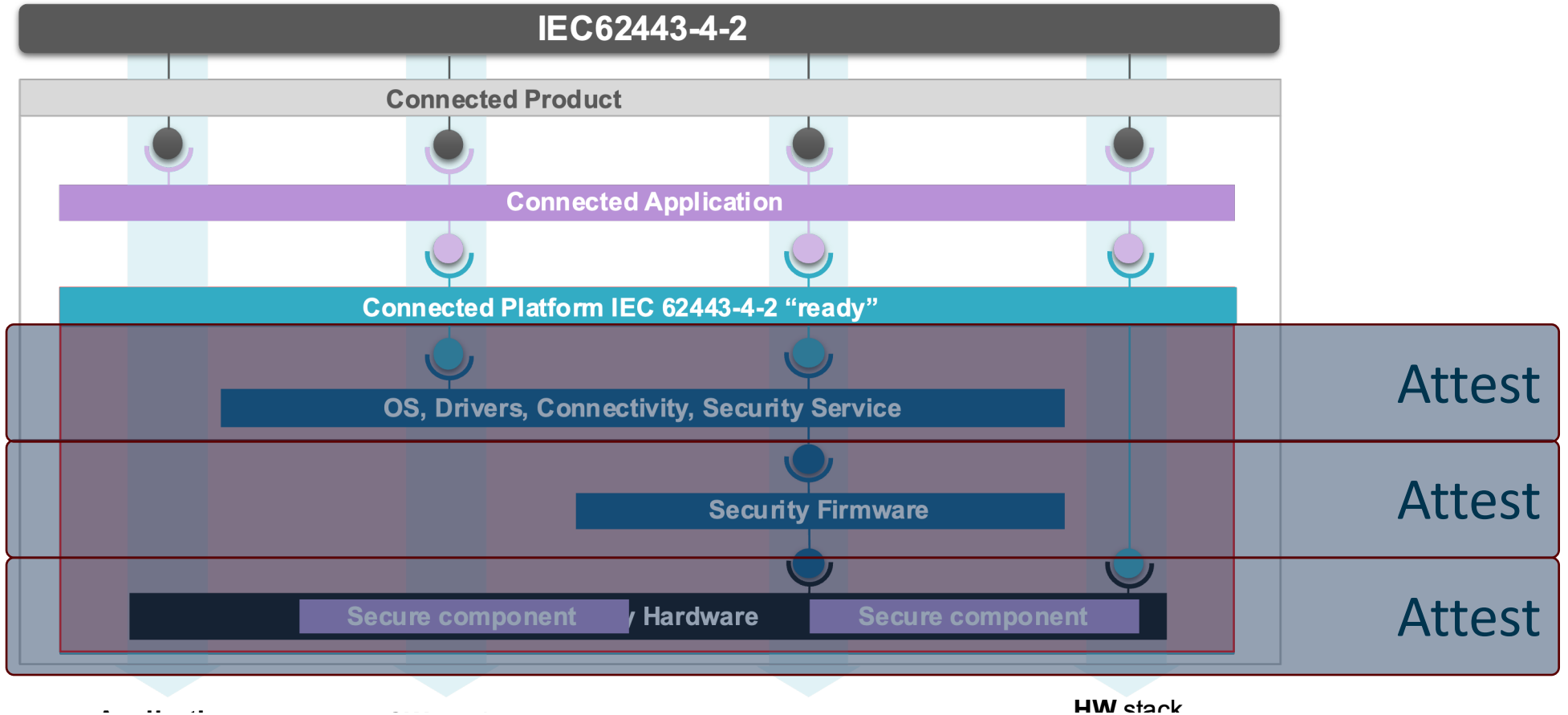
Very near future: attested composition



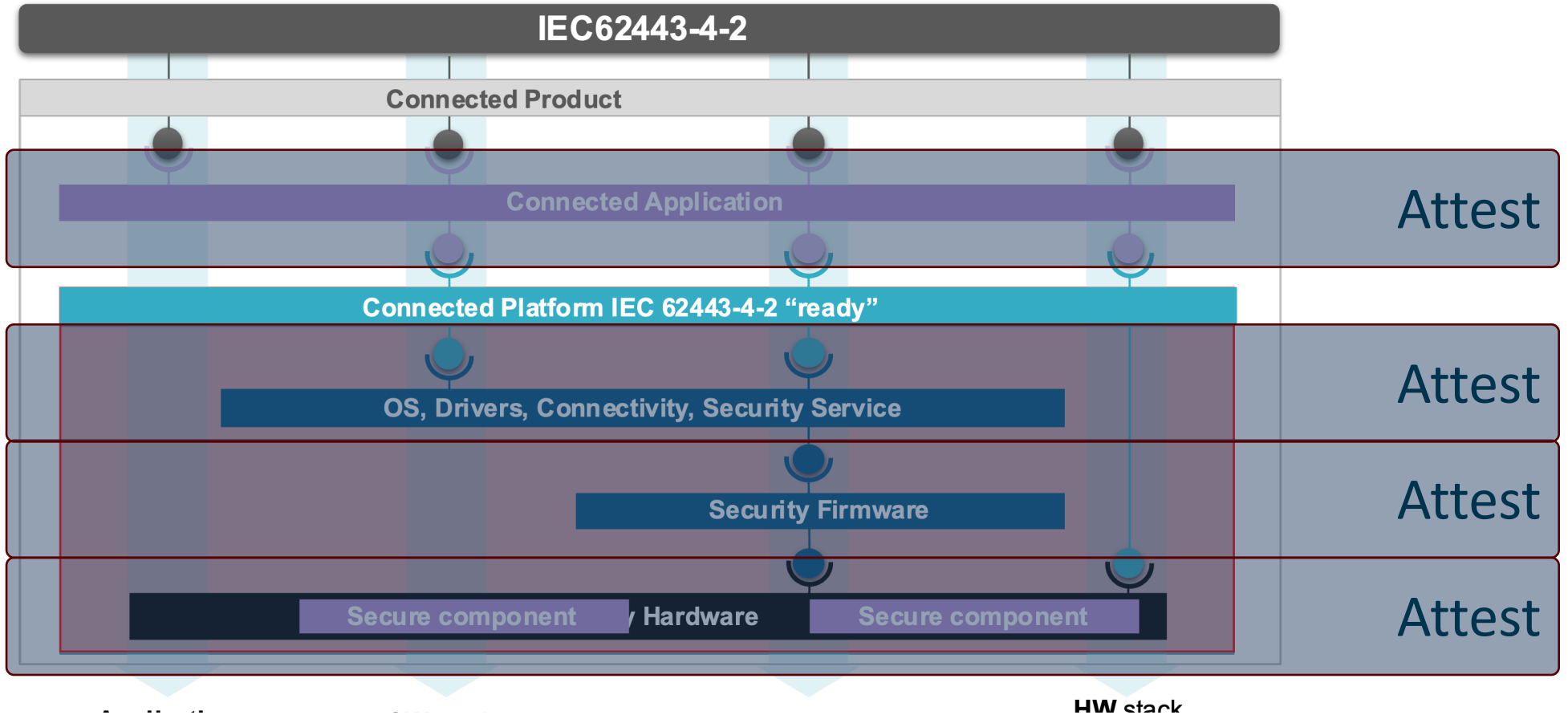
Very near future: attested composition



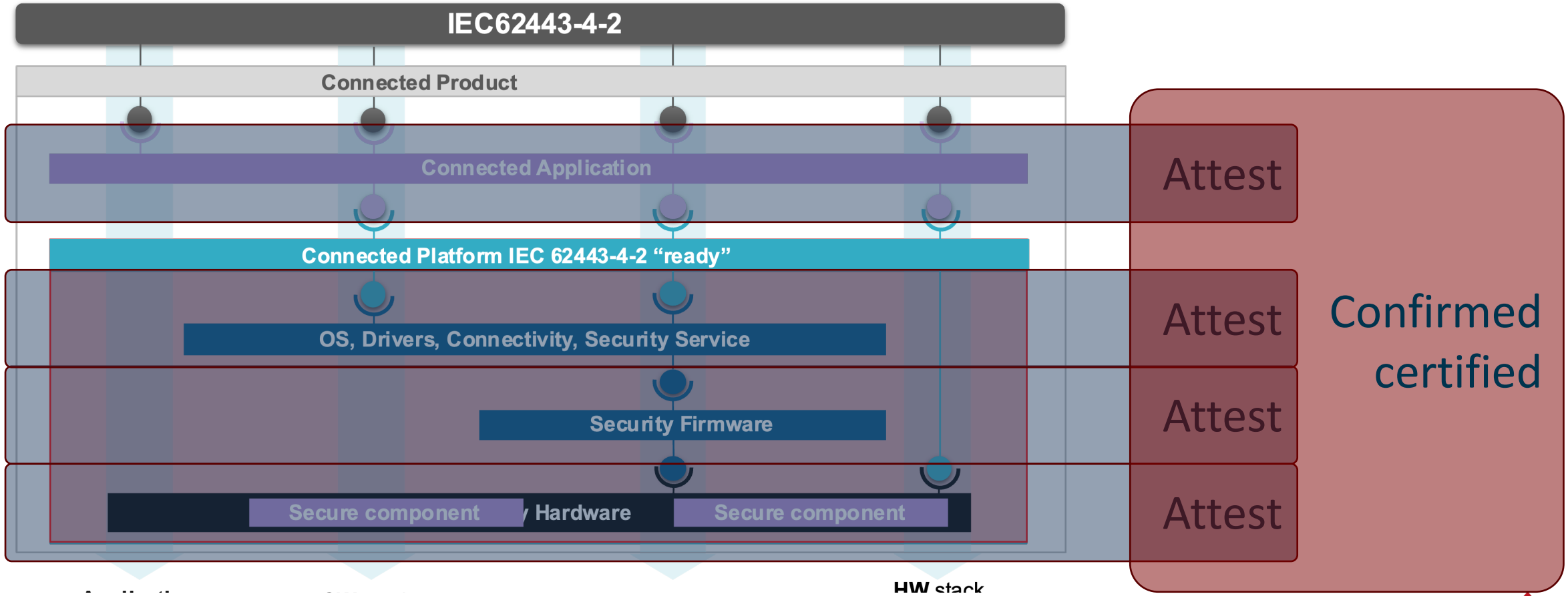
Very near future: attested composition



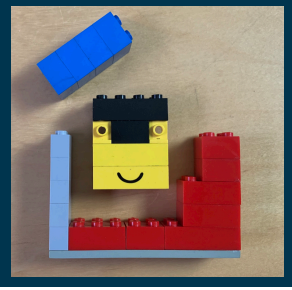
Very near future: attested composition



Very near future: attested composition



Conclusion



- SESIP is a solid methodology for IoT
- Use to show compliance with external requirements use
  - SESIP based: SESIP Profiles (ISA/IEC 62443, PSA Certified, …)
  - Others: mappings (ETSI EN 303 645, NIST 8259, …)
- Composition makes stepwise compliance possible
- Attestation makes SBOM and certificate checks on demand possible.

- Check that the certificate is accepted
  - Requirements fulfilled
  - CB/Scheme recognised

TRUSTCB

Successful re-use requirements

Compliance
“because we must by <scary entity>”

<scary entity> must recognise certificate

Risk management
“because it reduces our overal risk/cost”

Certificate shows “state of art”
/
re-use cost reduction

Differentiator
“because it looks good & we sell more”

Certificate brand must be recognised as “better”

TRUSTCB

Questions?

Including “old man talks about SESIP origins before it goes into CEN / CENELEC” questions

www.trustcb.com

wouter@trustcb.com