USING SESIP TO SUPPORT ISO/SAE 21434 COMPLIANCE

John BOGGIE
Senior Director, Head of Cybersecurity Certification

Global Platform event Tokyo
September 2023

SECURE CONNECTIONS FOR A SMARTER WORLD

1 MINUTE INTRODUCTION TO SESIP

- SESIP (EN 17927)
  - Security Evaluation Standard for IoT Platforms EN 17927: SESIP is a certification standard developed to allow re-use of security testing across complex connected products.
  - It provides a technology agnostic approach (lego-box) to allow technology to define a set of security requirements and common security vulnerability assessment and testing approach.
  - It is built around the security services provided by all layers of a system from sub-component to final product.
  - It is written in easy to understand language and provides a cost/time effective approach to security validation and testing.

ISO/SAE 21434

ISO/SAE 21434 – MANDATORY THREAT AND RISK ANALYSIS

- TARA – A Threat Analysis and Risk Assessment must be performed for each component in the Automotive Supply Chain up to and including the vehicle (OEM)
- It requires:
  - Secure development Process
  - Item Definition defining threats and risks
  - Incident management and resolution

- The TARA approach is very much based on the end Vehicle
  - Attacks on sub-components maybe excluded or not taken into account

READY FOR ISO/SAE 21434 COMPLIANCE CLAIM AT PRODUCT LEVEL

- ISO/SAE 21434 defines cybersecurity process, and it is typically tied to a company development process
- In SESIP, one can further claim the process has been applied for the certified component
  - SESIP EN 17927:2022 CEN/JTC 13

6.2 Secure development

6.2.1 Requirement

For the development of the platform, the secure development process specified in <standard/specification> has been applied to the platform.

6.2.2 Value

The inclusion of this package claim in a SESIP Security Target or profile allows the generation of evidences that secure development requirements from a referenced specification/standard have been applied to the platform under evaluation.

Example: application of security-by-design process from a specification/standard e.g. ISO/SAE 21434:2021.

6.2.3 Considerations

Complete the variable parts of this SPP as follows:

- The specification or standard to be implemented by the environment and applied to the platform.

GENERIC TARA FOR A SPECIFIC TECHNOLOGY

- Using SESIP threats and risk assessments (mitigation) can be specified for a generic type of sub-component (technology type)
- This is a generic TARA and can be generated for a specific type of technology
- For example Global Platform have generated a generic TARA for MCU/MPU components
  - GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs Version 1.0 (GP_SESIP_Profile_Secure_MCU_MPU_V1.0)

https://higherlogicdownload.s3.amazonaws.com/GLOBALPLATFORM/transferred-from-WS5/GPT_SESIP_Profile_Secure_MCU_MPU_v1.0_PublicRelease.pdf

ISO/SAE 21434 and SESIP

ASSET DEFINITION

- SESIP Methodology lists the main assets of a Connected Platform

Asset	Protections
User data (local)	Privacy concerns are essential. Protections of integrity, authenticity, and confidentiality must be provided.
User data (authentication data)	Confidentiality is required for secrets. Secondary data (like counters) must be appropriately protected (integrity, confidentiality).
Data in transit (internet)	Confidentiality and integrity are often essential, as are authenticity and authentication of the other party.
Data in transit (local)	Integrity is often essential. Confidentiality is not a systematic requirement. Authenticity and authentication of the other party are less common.
Code, including platform code and application code	Integrity and authenticity are strong requirements. Confidentiality is optional.
Product identity	Integrity and unicity are required.
Configuration and system data	Integrity and authenticity are required.
Life cycle related data	Integrity is required.

SESIP ALREADY COVERS ISO/SAE 21434 INFORMATIVE REQUIREMENTS IN APPENDICES

- ISO/SAE 21434 Annex E: Cybersecurity assurance levels (CAL)

Example of Annex E CAL4 (Highest level)	SESIP
Search for vulnerabilities by exploratory methods	Yes; by definition of SESIP methodology
Cybersecurity assessments are carried out by a person who is independent	Totally independent; 3rd party certification
Independence of verification of cybersecurity concept and design activities	Security target is assessed (ASE); Process application can be covered by independent 3rd party (SPP)
Independence of verification of the implementation and integration of components	Covered by independent 3rd party (ADV)
Independence of cybersecurity validation	Covered by independent 3rd party evaluation
Independence of cybersecurity assessment	Covered by independent 3rd party evaluation and certification
Functional testing	Covered (ATE)
Vulnerability scanning	Covered (AVA)
Fuzz testing	Can be covered (AVA)
Vulnerability testing	Covered (AVA)

SESIP ALREADY COVERS ISO/SAE 21434 INFORMATIVE REQUIREMENTS IN APPENDICES

- ISO/SAE 21434 Annex G2: Guidelines for the attack potential-based approach
- SESIP Rating table separates Identification and Exploitation phase
- Results should be interchangeable

Table G.6 — Example aggregation of attack potential

Elapsed time		Specialist expertise		Knowledge of the item or component		Window of opportunity		Equipment	
Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value
≤1 day	0	Layman	0	Public	0	Unlimited	0	Standard	0
≤1 week	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
≤1 month	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
≤6 months	17	Multiple experts	8	Strictly confidential	11	Difficult/ none	10	Multiple bespoke	9
>6 months	19								

Table B-1: Attacks Rating

Factors	Identification	Exploitation	Notes
Elapsed time			
< one hour	0	0	
< one day	1	3	
< one week	2	4	
< one month	3	6	
> one month	5	8	
Not practical	*	*	
Expertise			
Layman	0	0	
Proficient	2	2	
Expert	5	4	
Multiple Expert	7	6	
Knowledge of the TOE			
Public	0	0	Critical or higher can only be claimed if all sites with access to that information are included in the scope of the evaluation at ALC_DVS.2 level (i.e. SESIP5).[1]
Restricted	2	2	
Sensitive	4	3	
Critical	6	5	
Very critical hardware design	9	NA	
Access to TOE			
< 10 samples	0	0	
< 30 samples	1	2	
< 100 samples	2	4	
> 100 samples	3	6	
Not practical	*	*	
Equipment			
None	0	0	
Standard	1	2	
Specialized	3	4	
Bespoke	5	6	
Multiple Bespoke	7	8	
Open samples			
Public	0	NA	Sensitive or higher can only be claimed if all sites with access to such open samples are included in the scope of the evaluation at ALC_DVS.2 level (i.e. SESIP5).[2]
Restricted	2	NA	
Sensitive	4	NA	
Critical	6	NA	

MCU/MPU PROFILE – GENERIC PRODUCT TYPE THREAT ANALYSIS (GENERIC TARA -1)

Assets	Threats	MCU/MPU profile coverage
Sensitive data End-user information (identity, other personal information, related keys/password) Environment data (e.g. road traffic information, environment measurements) Internal sensitive data (configuration data, keys, life cycle state)	**Modification [and disclosure] of sensitive data while stored** ➔ Impersonation leading e.g. to access to internal or external restricted services ➔ Privacy concerns ➔ Diffusion of wrong environment information ➔ Access to sensitive data and/or restricted services	Secure [Confidential/External] Storage – protections of sensitive data Secure KeyStore – protections of user crypto data e.g. keys, password Secure Debugging – protection of data access through debug interfaces Residual Information Purging – ensures erasure of sensitive data when needed (e.g. to ensure privacy in case of Field Return, Factory Reset, Decommissioning of the device) [Physical Attacker Resistance – protection against physical intrusions as simple probing]
	Modification [and disclosure] of sensitive data during manipulation ➔ Same potential impacts as above	All features – each claimed feature include the protection of assets related to the security feature [Software Attacker Resistance: Isolation of Platform – additional protections against software attacks using untrusted local code] [Physical Attacker Resistance – protections against local attacks]
	Modification [and disclosure] of sensitive data during exchanges with external entity (e.g. remote server, secure element of the integrating SoC) ➔ Diffusion of wrong environment information	Secure Communications – protections of the overall establishment of communications including related keys (generation/derivation, exchange, storage, binding, etc.)
Code	**Modification or replacement of stored code** ➔ Deletion of parts of original code ➔ Execution of attacker code replacing original code ➔ Disabling of part or all security features, access to sensitive data	Secure Initialization of Platform / Secure Update – check code authenticity and integrity before running Secure Update – allow security breaches fix All features– protection of security features execution
	Modification code at execution ➔ Bypass of parts of the code ➔ Execution of attacker code illegally loaded in memory ➔ Disabling of part or all security features, access to sensitive data and/or restricted services	[Software Attacker Resistance: Isolation of Platform – protection against malicious interactions with executing code through local untrusted code] [Physical Attacker Resistance – protections against local attacks disrupting code execution e.g. HW fault injections]

MCU/MPU PROFILE – GENERIC PRODUCT TYPE THREAT ANALYSIS (GENERIC TARA -2)

Assets	Threats	MCU/MPU profile coverage
Life-Cycle	**Modification of MCU/MPU life-cycle state verification** + See modification of sensitive data for threats against life cycle state while stored and at runtime ➔ Access to restricted life cycle state, giving access to restricted features e.g. debug/test ➔ Access to sensitive data and/or restricted services	Secure Initialization of Platform – include control of boot modes/tests access depending on life cycle [Secure Attestation of Platform State – can include MCU/MPU life cycle state for external check] [Software Attacker Resistance: Isolation of Platform – protection against malicious interactions with executing code through local untrusted code]
Secure services Cryptographic services	**MCU/MPU weak cryptographic services** ➔ Generation of weak cryptographic material ➔ Disclosure of cryptographic secrets ➔ Access to sensitive data and/or restricted services	Cryptographic Operations, Cryptographic Key Generation, Cryptographic KeyStore, Cryptographic Random Number Generation - ensure cryptographic services following secure crypto rules [Software Attacker Resistance: Isolation of Platform – protection against malicious interactions with executing code through local untrusted code] [Physical Attacker Resistance – protections against local attacks disrupting code execution e.g. HW fault injections, disclosing involved cryptographic keys or secrets]
MCU/MPU identification	**Modification of MCU/MPU identification** **Non unique MCU/MPU identification** ➔ Unexpected use of non-certified MCU/MPU	Verification of Platform Identity – check if right type and version of the MCU/MPU

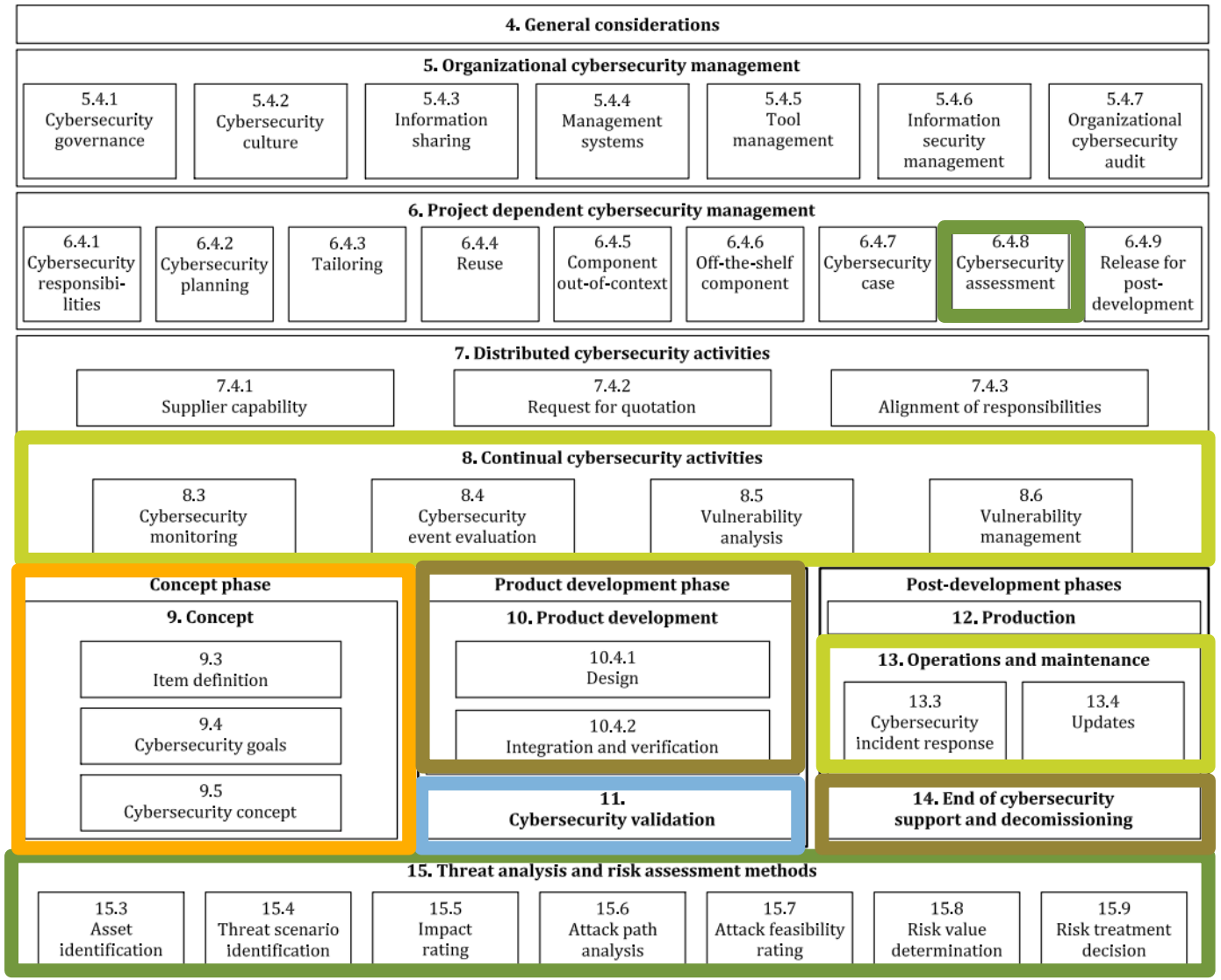
MCU/MPU PROFILE - THREAT ANALYSIS SUMMARY (GENERIC TARA - 3)

- **Details on considered attacks**

– Remote attacks (by default)
  - Remote logical attacks (e.g. ill formed messages targeting remote services as FW/SW update, environment measurements/probing, ranging calculation, etc.
  - Remote side channel attacks (e.g. timing attacks, cache attacks)
  - Remote hardware attacks (e.g. clkscrew)

– Local attacks (if applicable i.e. use cases depending)
  - Local logical attacks (e.g. via USB interfaces)
  - Local side channel with “basic/standard” material (e.g. power/EM/clock measurements)
  - Local hardware attacks with “basic/standard” material (e.g. voltage/clock glitching, EMFI, simple probing)

SESIP EVALUATION PROVIDES ISO/SAE21434 COMPLIANCE EVIDENCE



SESIP requires clear Security Target and Claims

SESIP can assess development process and product feature

SESIP verifies Security Claims and provide assessment

SESIP methodology is for Threat Analysis and Risk Assessment

SESIP requires Incident Management

SUMMARY

- Generic TARA for a sub-component can be created using SESIP
- The SESIP catalogue covers the key security requirements coming from ISO/SAE 21434
- The report that is generated by SESIP can be delivered to a customer up to the OEM and be used as an artifact to show that the supply chain has followed the ISO/SAE 21434 standard
- Reports can be used to show proof that due diligence was completed to mitigate or test for potential known threats

NXP Semiconductors usage of SESIP for Automotive

AUTOMOTIVE NXP CERTIFICATIONS

CAVP – NIST
Cryptographic Compliance

ESV – NIST
Random Number
Compliance – SP800 90B

SESIP Certification

ISO/SAE 21434 Process
Certification

TISAX (ISO 27001)
Trusted Information Security
Assessment Exchange

BRIEF OVERVIEW OF EACH CERTIFICATION TYPE 1/3

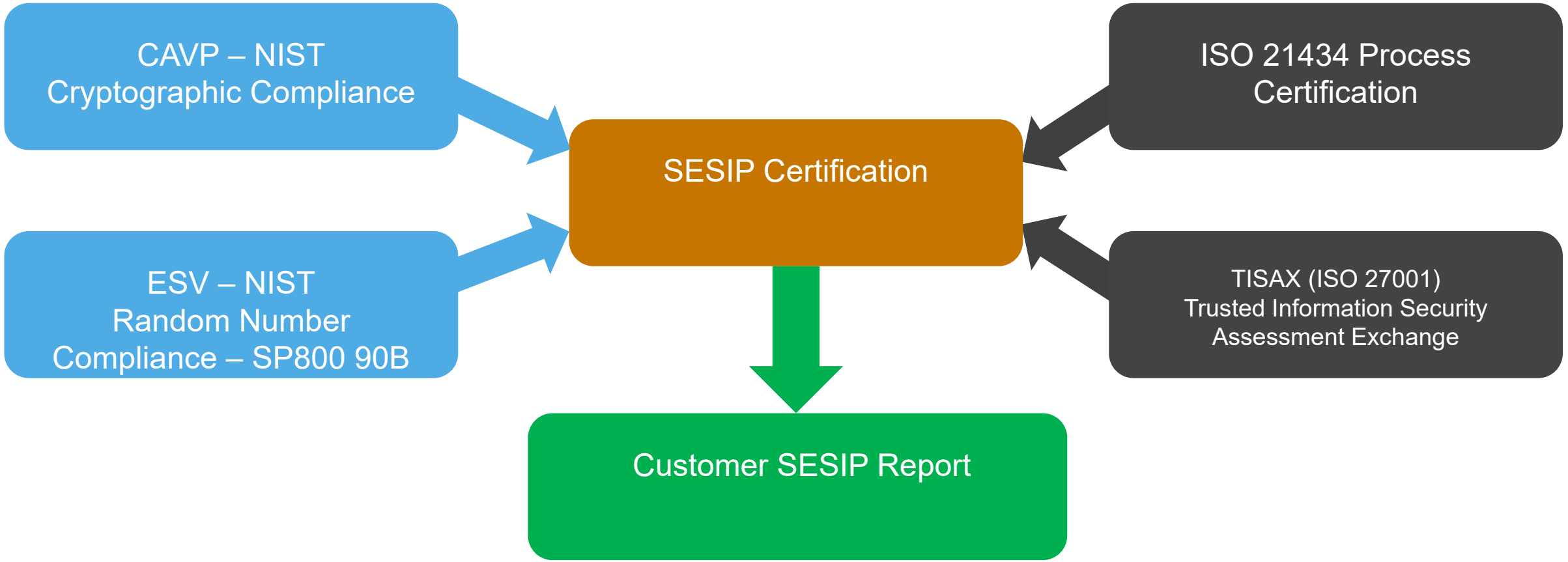
- NIST Certifications
  - Cryptographic Algorithm Validation Program (CAVP): The NIST CAVP program provides validation testing of NIST approved cryptographic Algorithms, i.e. each algorithm implemented in our products is validated that it complies with the NIST standard. Each algorithm receives a separate certificate.
  - Entropy Validation Server (ESV): ESV is the process where an accredited lab submit compliance and testing proof to NIST to show compliance to SP 800-90B (Random Number Generator)
- TISAX
  - Trusted Information Security Assessment Exchange: Provided by the ENX Association, TISAX is a Automotive specific variant of the Information Security Management System (ISO 27001). TISAX asses a companies security practices and how the organization deals with information and data protection. It includes management buy-in, disaster recovery and how the organization handles security incidents.

BRIEF OVERVIEW OF EACH CERTIFICATION TYPE 2/3

- ISO/SAE 21434
  - ISO/SAE 21434: Specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic systems in road vehicles, including their components and interfaces. It requires a company to:
    - Perform Risk Assessments - Identify potential security vulnerabilities
    - Address these vulnerabilities as part of the product design/development
    - Test to show the risks have been mitigated

    UN R155 and UN 156 made this mandatory across the Automotive supply chain from July 2022

AUTOMOTIVE NXP CERTIFICATIONS –SESIP PROVIDES A PROOF POINT FOR THE OTHER CERTIFICATION STANDARDS



AUTOMOTIVE NXP CERTIFICATIONS – WHAT THE SESIP CERTIFICATE COVERS

Certificates proving that the Cryptography is implemented correctly

Proof that the random number generator complies to a industry standard

Certificates provided by US Government

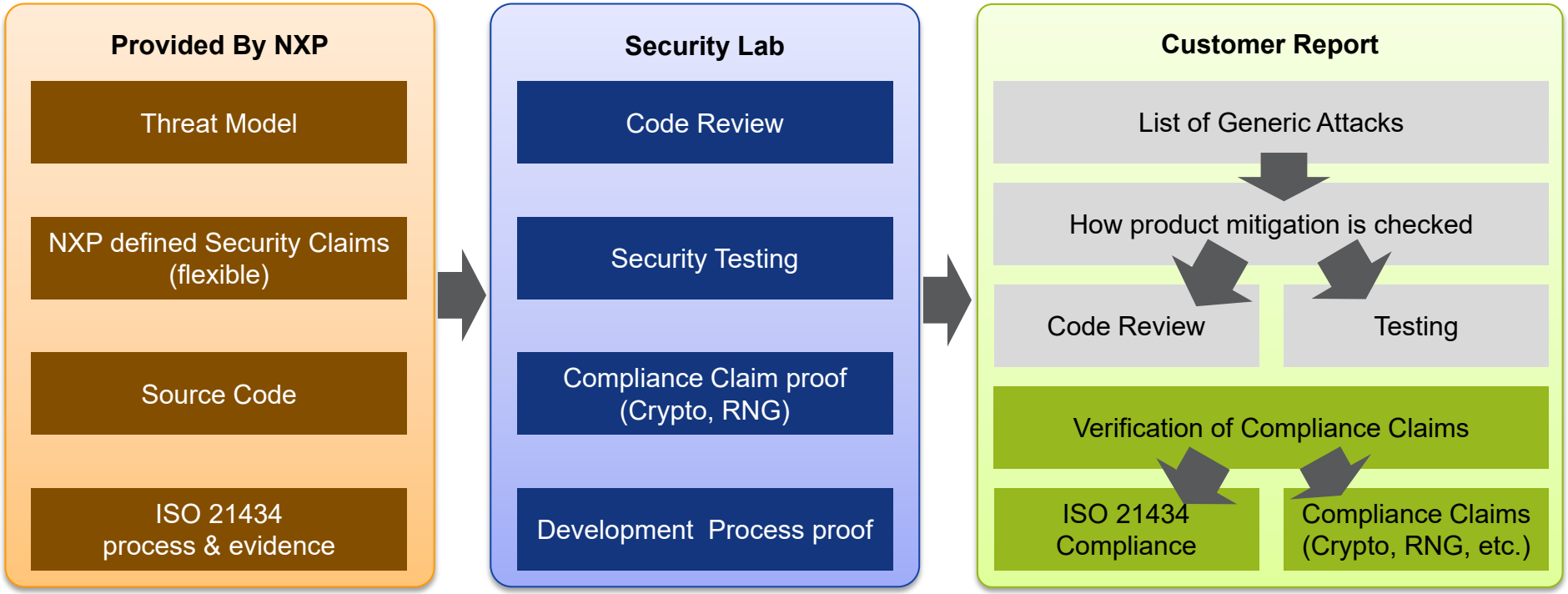
The Device has been defined using a common threat model and details of how it mitigates these threats.

Proof that the ISO 21434 certified processes and procedures were followed for the product's development cycle

Details how security sensitive information is handled within NXP

Proof that the Device follows the Product Security Response Incident Team (PSIRT) Process

NXP ROADMAP FOR ACCELERATED COMPLIANCE TO ISO 21434



SESIP Certificate

- Provides proof of assurance
- Shows the certification cope

Test Report

- Test Report for Customer (supports customer compliance)
- Shows how the security requirements were verified
- Details what testing was performed
- ISO 21434 Compliance validated

- Threat Modelling
- Threat Mitigation (Security Mechanisms)
- Security Guidance (environment objective)
- Standard/Common Requirement mapped in
- ISO/SAE 21434 Process Compliance claim mapped in

- Include Cryptographic compliance and security: Compliance proof to customers
- A lab report that can be shared with customers: Reducing/Compatible with customer ISO/SAE 21434 certification effort

IN SUMMARY

- SESIP provides evidence that the product security claims are tested and verified
- Verification and testing is performed by an external highly experienced test lab
- The certificate is awarded by a third part independent party
- A report can be delivered to customers all the way to the OEM and can be then shown as an artifact in their TARA
- SESIP already covers requirements coming from government legislation

Test Labs

- SGS Brightsight
- Riscure
- TUV Informationstechnik
- APPLUS
- Serma
- Dekra (preliminary accreditation)
- UL (preliminary accreditation)
- ATSEC (preliminary accreditation)

SECURE CONNECTIONS
FOR A SMARTER WORLD