SECURE-iC
THE SECURITY SCIENCE COMPANY

ICCC2023

CC 2022 IN ACTION: SECURING CRYPTOGRAPHIC PROTOCOLS AND THEIR IMPLEMENTATIONS

Ritu-Ranjan SHRIVASTWA, Certification & Standardization Program Manager, Secure-IC

31/10/2023

Version 1.0

AGENDA

1. ISO/IEC 15408-4

2. ISO/IEC 29128-2/3 PROJECT STATUS

3. ISO/IEC 29128-2/3 EXTENSION OF ISO/IEC 15408-4 FRAMEWORK

4. COMMENTS AND RESOLUTIONS FROM ISO/IEC JTC1/SC27 WG2/3

5. NEXT STEPS

ISO/IEC 15408-4

- **CC2022** Publication formally announced in ICCC2022 (Toledo, Spain)

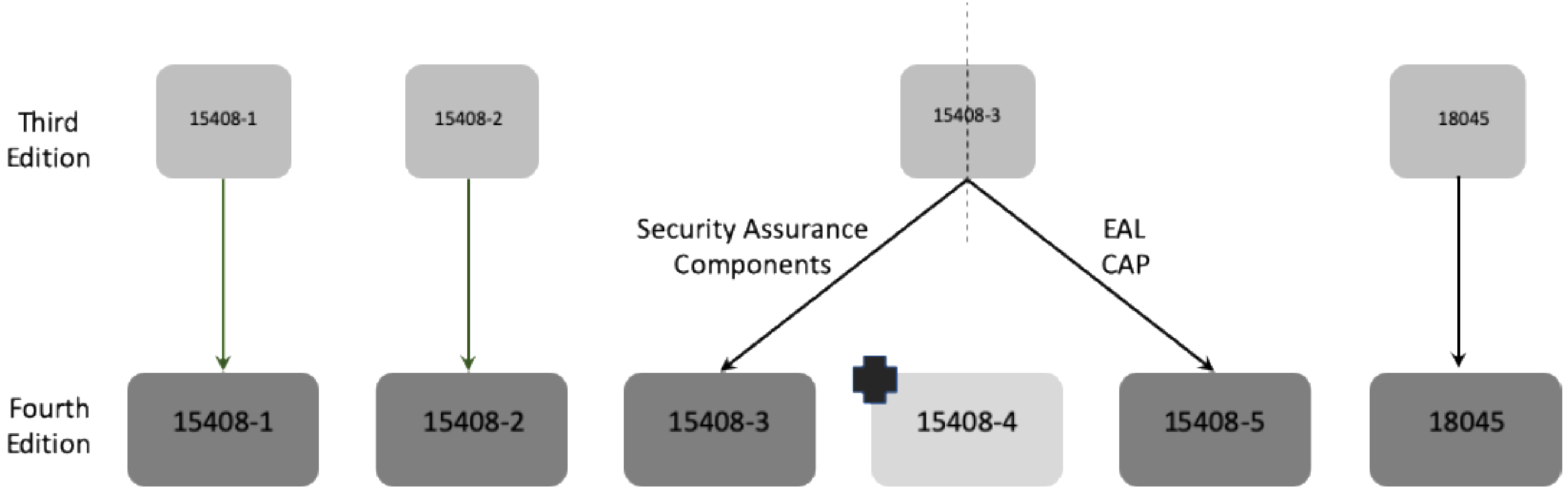


Figure 1 — Mapping between the third and fourth editions

- CC Part 4 (**ISO/IEC 15408-4**): Framework for the specification of evaluation methods and activities

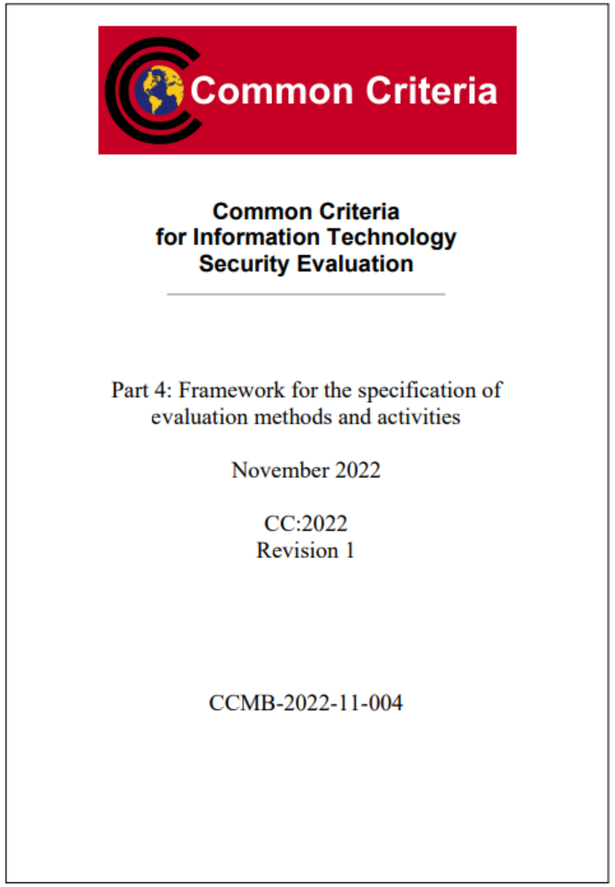
ISO/IEC 15408-4

New approaches introduced in the new CC2022

- Keywords:
  - Exact conformance
  - Direct Rationale PPs
  - TOE specific evaluation methods
- TOE to be strictly compliant to the given set of requirements (nothing more or nothing less)
- All the tests are known beforehand, no requirement for tailored test plan during evaluation
- Evaluation not focused on evaluator’s strength (such as the ability to fine-tune a test)
- Compliance focused on meeting listed requirements strictly rather than protection against given set of threats

ISO/IEC 15408-4

- The new Part 4: Standardized framework for Specifying: **objective, repeatable and reproducible** evaluation methods and evaluation activities.
- “each action from part 3 is represented in the CEM as a set of work units that are carried out by an evaluator.”
- Part 4 “*specifies the ways in which new evaluation activities can be derived from the generic work units in the CEM, and combined into an evaluation method that is intended for use in some particular evaluation context.*”



Common Criteria

Common Criteria
for Information Technology
Security Evaluation

Part 4: Framework for the specification of
evaluation methods and activities

November 2022

CC:2022
Revision 1

CCMB-2022-11-004

Generic

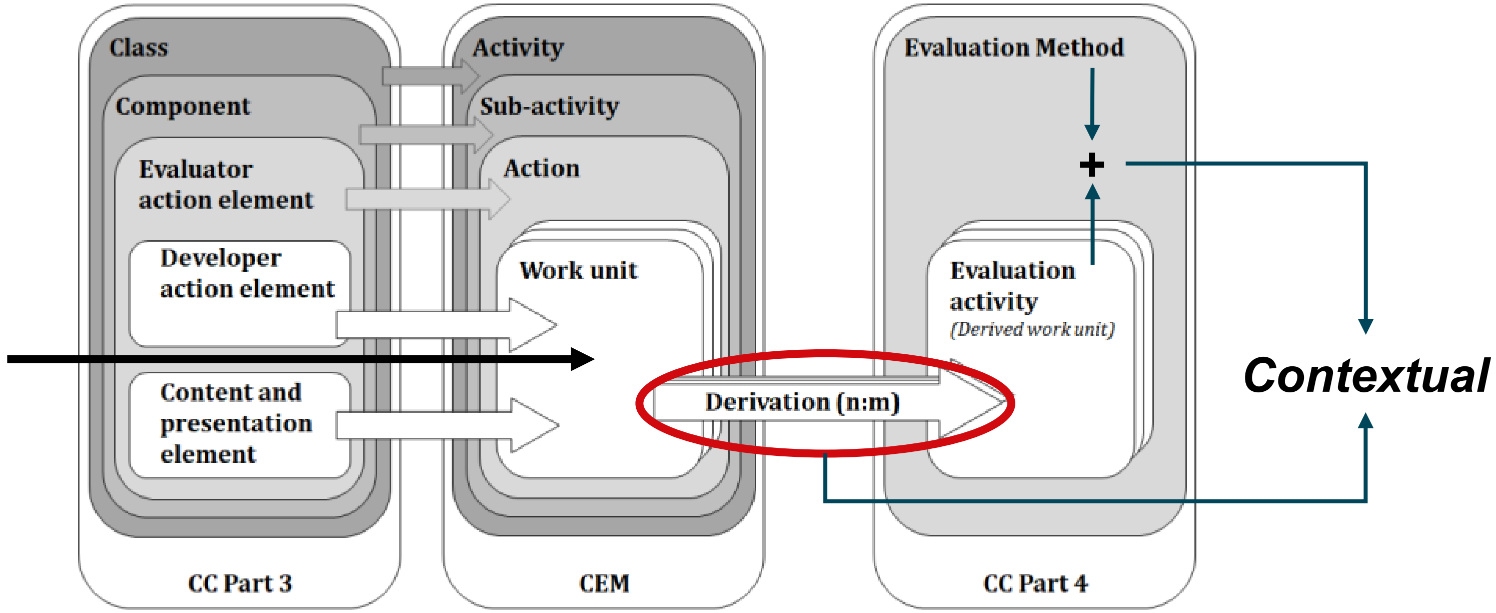


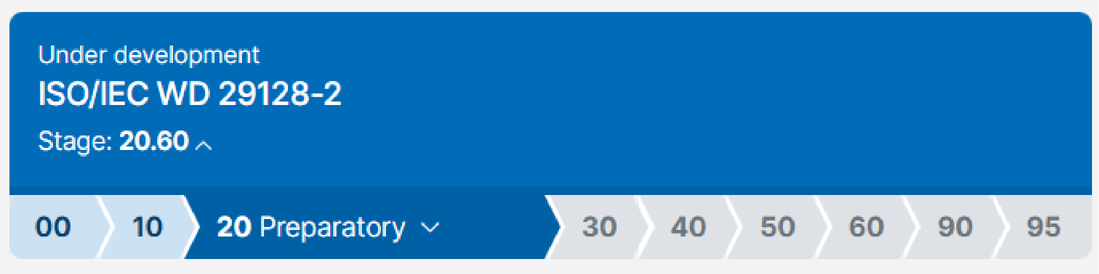
Figure 1 — Mapping of CC Part 3 and CEM structures to structures of this document

ISO/IEC 15408-4

- Applying to **ISO/IEC 29128-2/3**
  - Context: Verification of Cryptographic Protocols and their implementation
  - Framework for evaluation of cryptographic protocols is presented in ISO/IEC 29128-1
  - Evaluation methods for cryptographic protocols is presented to in ISO/IEC 29128**-2**
    - Evaluation activities derived based on methods presented for each security property of cryptographic protocols
  - Evaluation methods for cryptographic protocol **implementation** verification is presented in ISO/IEC 29128**-3**
    - Evaluation activities derived based on methods presented for each security asset of cryptographic protocol implementation

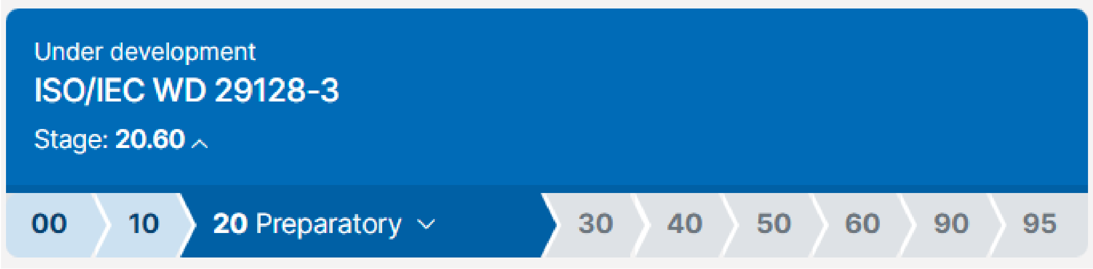
ISO/IEC 29128-2/3 PROJECT STATUS

- **2021** – Resolution to split ISO/IEC 29128 in 3 parts
- **2022** – Revision to ISO/IEC 29128-1 (FDIS submitted in the same year) and NWIP for ISO/IEC 29128-2/3 approved
- **2023 March** – ISO/IEC 29128-1:2023 published and ISO/IEC 29128-2/3 balloted to start as new project (new projects registered)
- **2023 September** – ISO/IEC 29128-2/3 1st WD submitted
- **2023 October** – Comments received – Resolved to submit 2nd WD



Under development
ISO/IEC WD 29128-2
Stage: **20.60**

00 10 **20 Preparatory** 30 40 50 60 90 95



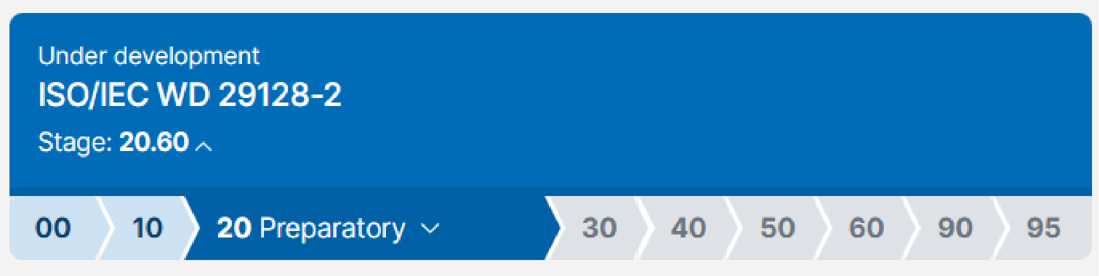
Under development
ISO/IEC WD 29128-3
Stage: **20.60**

00 10 **20 Preparatory** 30 40 50 60 90 95

ISO/IEC 29128-2/3 PROJECT STATUS

- **Editor details**

- ISO/IEC 29128-1: Carolyn FRENCH
- ISO/IEC 29128-2: Ritu-Ranjan SHRIVASTWA
- ISO/IEC 29128-3: Ritu-Ranjan SHRIVASTWA

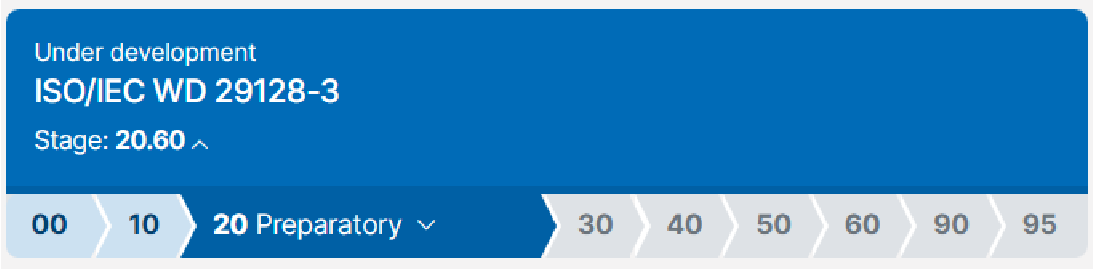


Under development

ISO/IEC WD 29128-2

Stage: 20.60

00 | 10 | 20 Preparatory | 30 | 40 | 50 | 60 | 90 | 95



Under development

ISO/IEC WD 29128-3

Stage: 20.60

00 | 10 | 20 Preparatory | 30 | 40 | 50 | 60 | 90 | 95

ISO/IEC 29128-2/3 PROJECT STATUS

- **Motivation**
- Several cryptographic protocols in use, such as:
  - (D)TLS, IPsec, PKCS#11, SCP11, Matter, etc.
- New communication standards such as 6G shall present new protocol requirements
- We also see new crypto strategies emerging such as PQC, AEAD based encryption functions (ex. ASCON), etc. that could be used in cryptographic protocols
- Therefore, cryptographic protocols are extremely critical, and to cope up with the requirements, new protocols emerge as successors to old versions or as novel additions
- Verification of the protocols, thus, becomes extremely important:
  - Need formal security verification of cryptographic protocols (using tools such as *Tamarin prover, CryptoVerif, EasyCrypt, etc.*)
  - Need formal vulnerability assessment of cryptographic protocol implementation

SECURE-IC
THE SECURITY SCIENCE COMPANY

ISO/IEC 29128-2/3 EXTENSION OF ISO/IEC 15408-4 FRAMEWORK

- **ISO/IEC 29128-1 high level introduction**

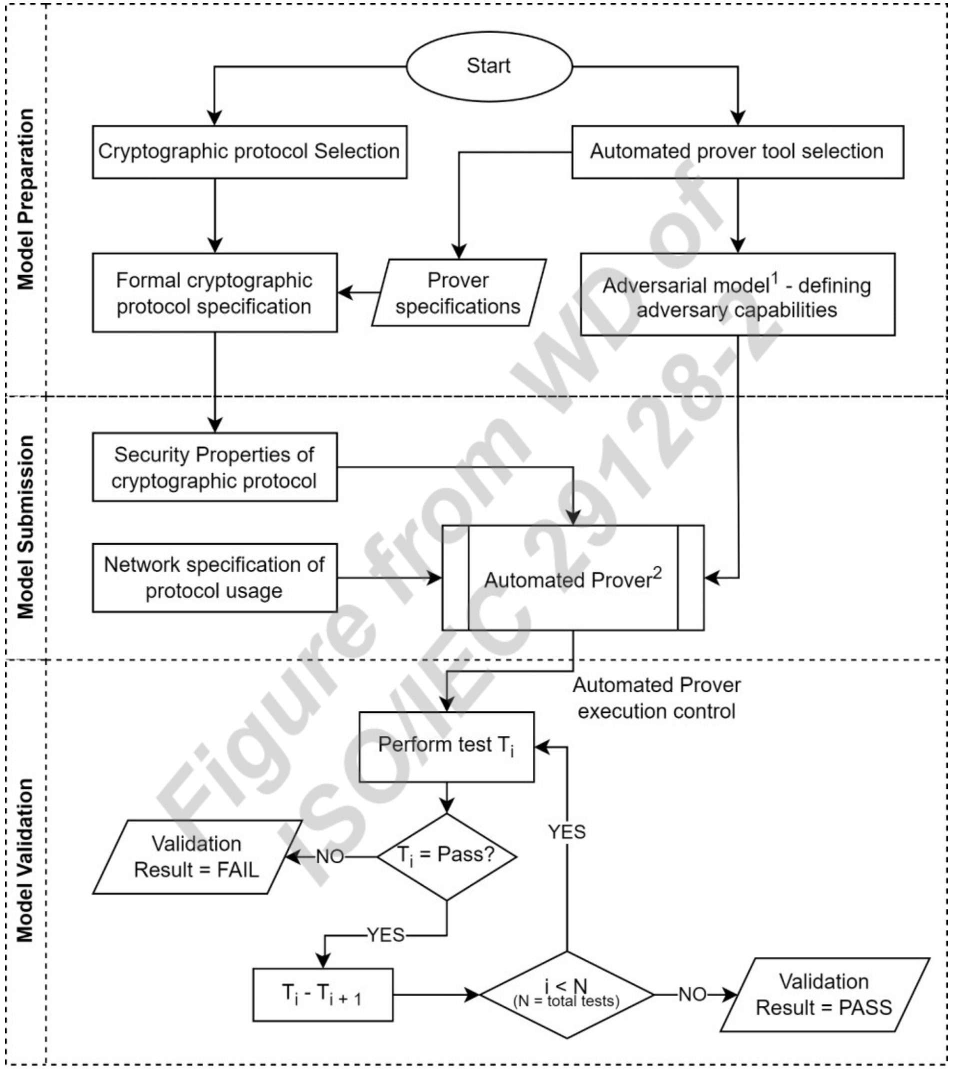
- Symbolic verification: not evaluating the underlying cryptographic protocol (considered secure)

- All security properties, usage of protocol including actors, messages, functions and attributes to be provided as formal specification

- Automated-prover based evaluation

- Every security property to be evaluated

- Successful validation entail passing verification of all security properties



Model Preparation

Start

Cryptographic protocol Selection

Automated prover tool selection

Formal cryptographic protocol specification

Prover specifications

Adversarial model[1] - defining adversary capabilities

Model Submission

Security Properties of cryptographic protocol

Network specification of protocol usage

Automated Prover[2]

Model Validation

Automated Prover execution control

Perform test T_i

T_i = Pass?

NO

Validation Result = FAIL

YES

$T_i - T_{i+1}$

i < N (N = total tests)

YES

NO

Validation Result = PASS

[1] Based on theoretical proof assurance level selection from Table 1

[2] Capabilities of prover based on theoretical proof assurance level selection from Table 1

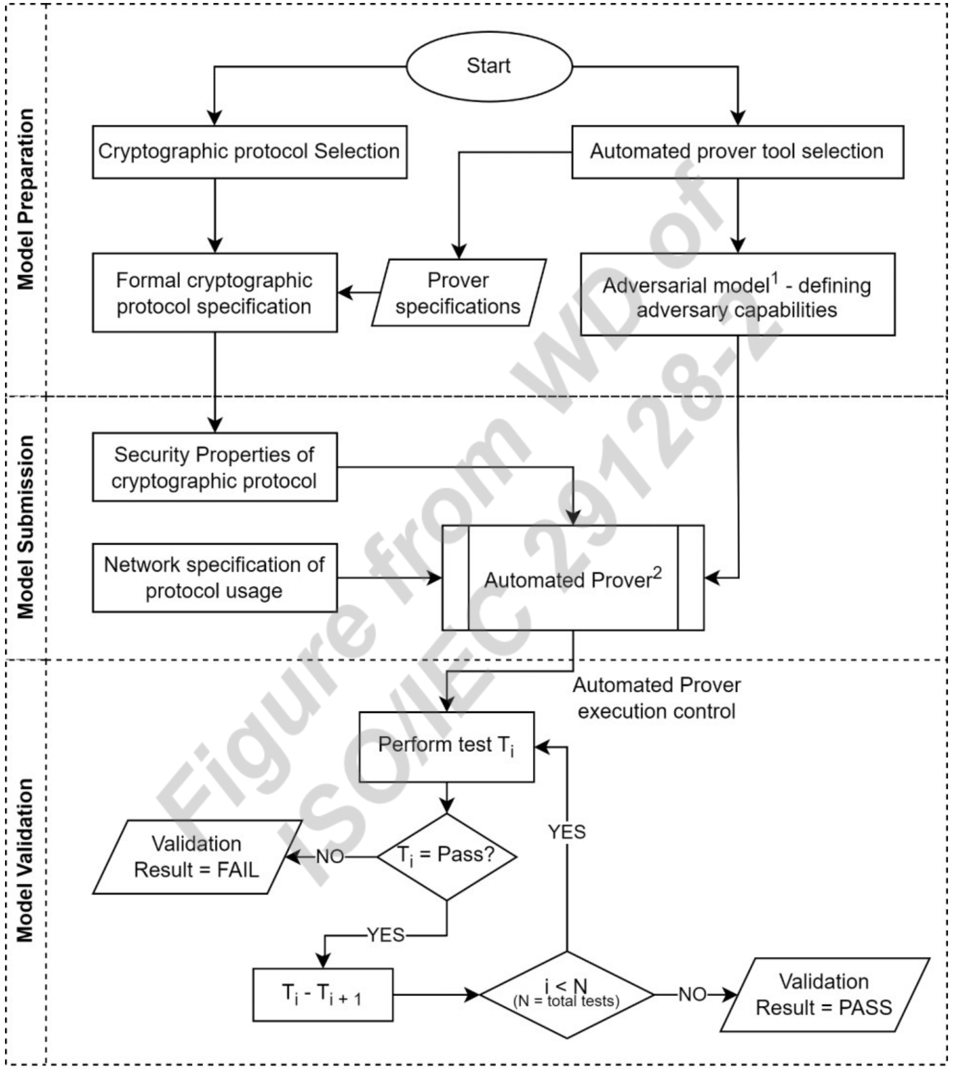
ISO/IEC 29128-2/3 EXTENSION OF ISO/IEC 15408-4 FRAMEWORK

- **ISO/IEC 29128-2/3**

- Provides evaluation methods and activities for framework of part 1

- Methods include:
  - Required inputs
  - Protocol model
  - Adversarial model
  - Scope of evaluation
  - Pass/fail criteria
  - Attack analysis description*
  - Attack feasibility description*
  - Security coverage*

*(part 3)

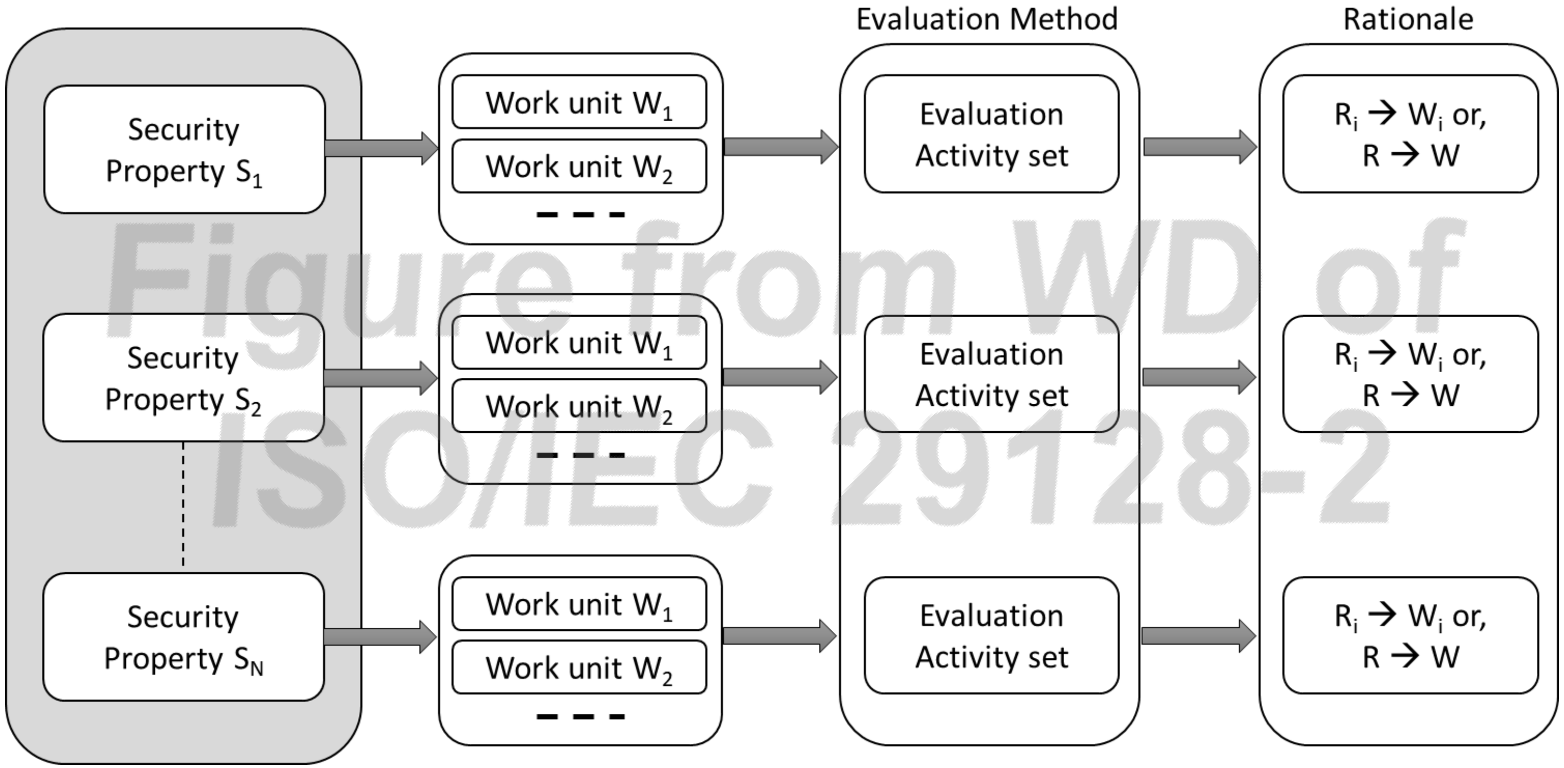

Model Preparation
Model Submission
Model Validation
Start
Cryptographic protocol Selection
Automated prover tool selection
Formal cryptographic protocol specification
Prover specifications
Adversarial model[1] - defining adversary capabilities
Security Properties of cryptographic protocol
Network specification of protocol usage
Automated Prover[2]
Automated Prover execution control
Perform test T_i
Validation Result = FAIL
NO
T_i = Pass?
YES
YES
T_i - T_{i+1}
i < N (N = total tests)
NO
Validation Result = PASS

[1] Based on theoretical proof assurance level selection from Table 1

[2] Capabilities of prover based on theoretical proof assurance level selection from Table 1

ISO/IEC 29128-2/3 EXTENSION OF ISO/IEC 15408-4 FRAMEWORK

- **ISO/IEC 29128-2**
- Evaluation methods provided for: Prover and Model
- Activities mapping:



ISO/IEC 29128-2/3 EXTENSION OF ISO/IEC 15408-4 FRAMEWORK

- **ISO/IEC 29128-2**
- Cryptographic protocols Assurance levels:
  - QM level with minimum maturity
  - **Assurance level 1:**
    - Mandatory verification using automated prover for all security properties
  - **Assurance levels 2 and 3:**
    - Model based (such as Dolev-Yao) verification
  - **Assurance levels 3 and 4:**
    - Model based verification using two different models, one for protocol verification, and the other for cryptographic primitives for robustness

ISO/IEC 29128-2/3 EXTENSION OF ISO/IEC 15408-4 FRAMEWORK

- **ISO/IEC 29128-3**
- Implementation verification of pre-verified cryptographic protocol using ISO/IEC 29128-2
- Evaluation focused on AVA_VAN approach for vulnerability analysis of the implementation
- Evaluation methods presented for cryptographic protocol specific verifications to be made
- Attack based evaluation

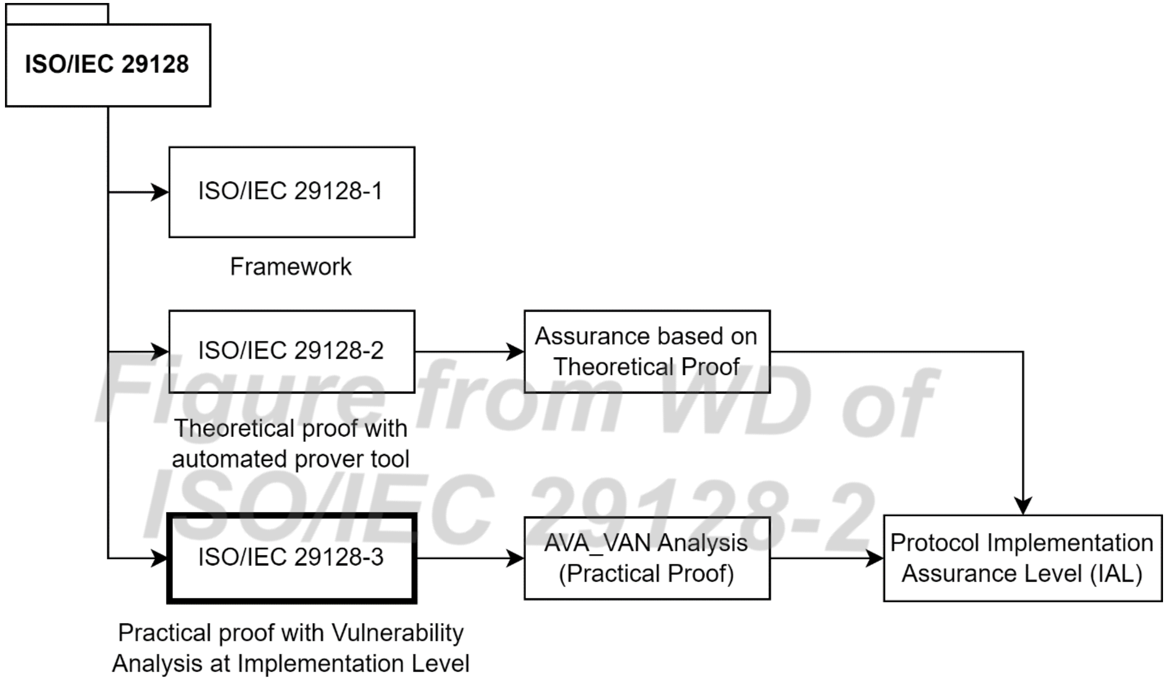

ISO/IEC 29128
ISO/IEC 29128-1
Framework
ISO/IEC 29128-2
Theoretical proof with automated prover tool
Assurance based on Theoretical Proof
ISO/IEC 29128-3
Practical proof with Vulnerability Analysis at Implementation Level
AVA_VAN Analysis (Practical Proof)
Protocol Implementation Assurance Level (IAL)

Figure from WD of ISO/IEC 29128-2

ISO/IEC 29128-2/3 EXTENSION OF ISO/IEC 15408-4 FRAMEWORK

- **ISO/IEC 29128-3**
- Evaluation methods provided for physical implementation verification
- Evaluation methods cover aspects of evaluators responsibilities for verification such as usability access, side-channel analysis, fault injections, etc. and the motivations for each responsibility
- Activities mapping for each attack test:

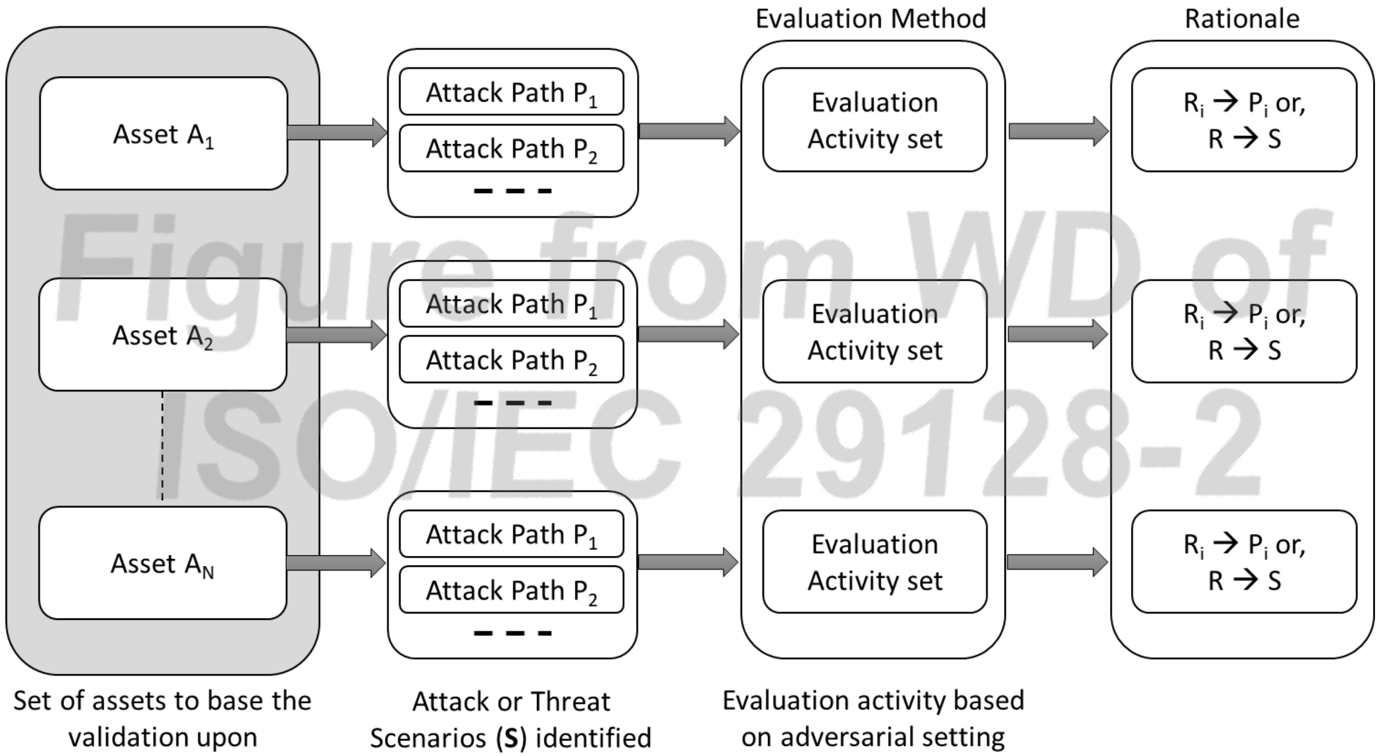

Evaluation Method
Rationale
Asset A_1
Asset A_2
Asset A_N
Attack Path P_1
Attack Path P_2
Attack Path P_1
Attack Path P_2
Attack Path P_1
Attack Path P_2
Evaluation Activity set
Evaluation Activity set
Evaluation Activity set
$R_i \rightarrow P_i$ or, $R \rightarrow S$
$R_i \rightarrow P_i$ or, $R \rightarrow S$
$R_i \rightarrow P_i$ or, $R \rightarrow S$
Set of assets to base the validation upon
Attack or Threat Scenarios (**S**) identified
Evaluation activity based on adversarial setting

Figure from WD of ISO/IEC 29128-2

ISO/IEC 29128-2/3 EXTENSION OF ISO/IEC 15408-4 FRAMEWORK

- **ISO/IEC 29128-3**
- Implementation Assurance Levels (IALs) introduced
  - Assurance achieved from AVA_VAN testing as well as protocol verification assurance level evaluated from ISO/IEC 26262-2

Theoretical proof assurance from ISO/IEC 29128-2	**AVA_VAN.1**	**AVA_VAN.2**	**AVA_VAN.3**	**AVA_VAN.4**	**AVA_VAN.5**
Level 1	IAL 1	IAL 2	IAL 3	IAL 4	IAL 5
Level 2	IAL 1	IAL 2	IAL 3	IAL 4	IAL 5
Level 3	IAL 2	IAL 3	IAL 4	IAL 5	IAL 6
Level 4	IAL 3	IAL 4	IAL 5	IAL 6	IAL 7

COMMENTS AND RESOLUTIONS FROM ISO/IEC JTC1/SC27 WG2/3

- Comments on ISO/IEC 29128-2 (all resolved)
  - 22 general
  - 8 technical
  - 7 editorial
- Main areas covered in comments:
  - Generalization of the use of adversarial models and not any specific type – difficult given that the part 1 (framework) specify a single type
  - Parameterization of automated prover tools to be used for verification
  - Tools selection criteria
  - Tools verification methods and activities
  - Expansion of requirements to make distinct various implicit notions (such as verification of algebraic properties is a part of verification process but should be explicitly expressed as a verification requirement)
  - KAT based security property evaluation
- Part 3 received 1 comment (resolved)

NEXT STEPS

- 2nd WD to be submitted by Jan 2023 incorporating all changes accepted in resolution of comments

- Upcoming changes/updates:
  - Modified assurance tables
  - Tools selection criteria and parameters in ISO/IEC 29128-2
  - Methods for assessment and verification of tools in ISO/IEC 29128-2
  - KAT for verification of security properties in ISO/IEC 29128-2
  - Adversarial model capabilities refined and selection criteria
  - Update of Annexes with more adversarial model examples for use
  - Improved cross-referencing
  - Example evaluation for both ISO/IEC 29128 parts 2 and 3

SECURE-IC
THE SECURITY SCIENCE COMPANY

THANK YOU FOR YOUR ATTENTION

CONTACTS

EMEA	sales-EMEA@secure-IC.com
APAC	sales-APAC@secure-IC.com
CHINA	sales-CHINA@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
TAIWAN	sales-TAIWAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com

FOLLOW US ON SOCIAL MEDIA