ISO/IEC 24727-5

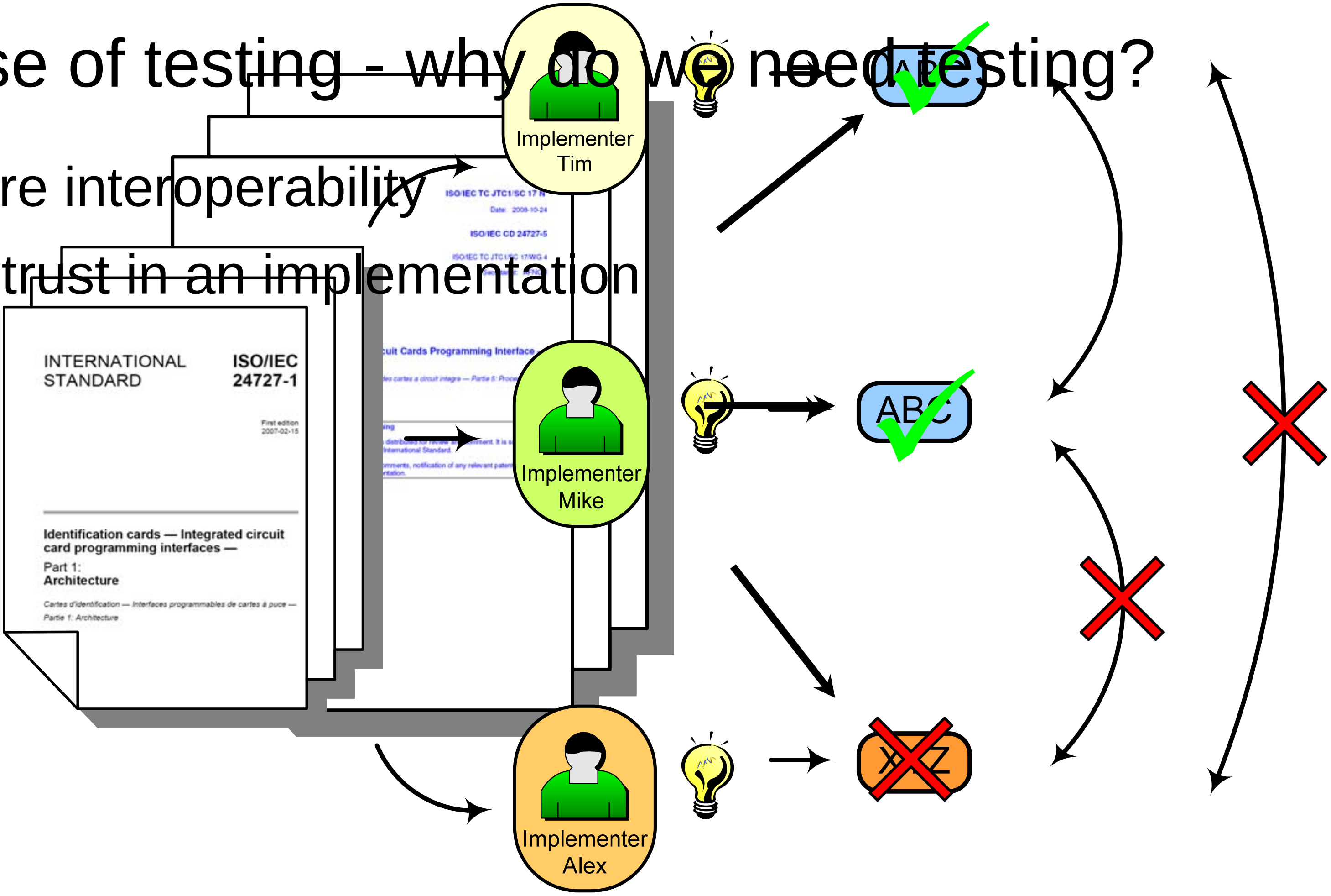
An IAS Interoperability Standard

ISO/IEC 24727-5 Testing Procedures

- **Why** do we need testing?
- **How** are we testing?
- **What** are we testing?

Document structure – Testing procedure Testing methodology

- Purpose of testing - why do we need testing?
  - ○ Ensure interoperability
  - ○ Instil trust in an implementation



Document structure

- ISO/IEC 24727-5 is made up of two distinct parts:
  - Testing procedure (descriptive)
  - Test scenarios and language bindings (functional)

Testing Procedures

- Testing methodology (including test Principles)
- Components
- Authentication protocols
- Secure messaging
- Marshalling
- Stack configuration testing
- Operational testing
- Operational test reporting

Test scenarios and language bindings

- Test Scripts
- Language bindings

Test Principles

- 25 test principles which:
  - Define how to achieve conformance e.g.
    - All applicable tests need to be passed
    - Component based
  - What is in scope e.g.
    - Behavioural tests
  - What is out of scope e.g.
    - Performance testing
  - What is expected of a test facility e.g.
    - Reference test implementation
    - Logging facilities

Conformance vector

- Why conformance vectors?
- Conformance is on components not necessarily a whole system there is no scale of conformance i.e. not like security level attainment where conformance for a particular level implies the level of security e.g. FIPS140-2 levels 1 to 4 where 4 is the highest level.

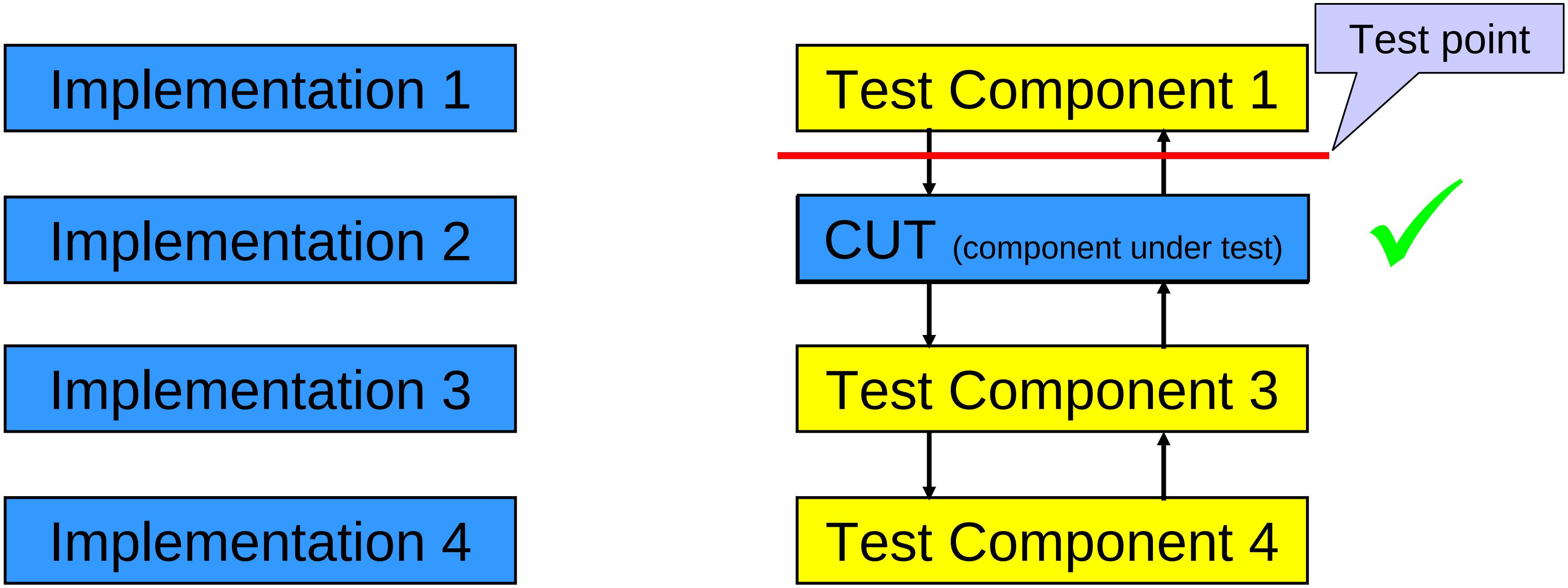
Atomic Tests and Test Sequences

- Atomic Tests
- Test Sequences
  - Application management - alpha card-application data structure construction
  - Application management - application 1 data structure construction
  - Application management - application data structure construction error conditions
  - Application management - application 2 data structure construction
  - Data manipulation - card application path
  - Data manipulation - general
  - Data manipulation - global authentication
  - Application management - data structure destruction

Discoverability tests

- Discoverability is tested at two layers
  - SAL
    - Mapping of off-card representations to on-card representations
    - Uses the Cryptographic Information Application (CIA)
  - GCI
    - Discovers what is contained on the card via the CCD and ACD
    - Bootstraps the procedural element that translates between ISO/IEC 24727-2 commands to proprietary commands

How are components tested?



Implementation 1

Implementation 2

Implementation 3

Implementation 4

Test Component 1

CUT (component under test) ✓

Test Component 3

Test Component 4

Test point

Testing of Authentication Protocols

- APs perform two basic functions
  - Authentication
  - Cryptographic operations
- Authentication is tested for success and failure by executing the commands as specified in each AP definition.
- ISO/IEC 24727-6 APs shall include test specifications as defined in ISO/IEC 24727-5 i.e. it is up to the registering party to provide these test scenarios.

NIST

Testing of Authentication Protocols (cont.)

- The only AP used, in ISO/IEC 24727-5, to test Access Control Lists (ACLs) and security conditions is the Simple Assertion AP. Each implementation must implement the Simple Assertion AP as a minimum.
- All AP cryptographic operations shall be tested for the defined functionality.

Testing of Secure Messaging

- All tests in ISO/IEC 24727-5 are tested without secure messaging because the inputs and outputs cannot be verified with secure messaging.
- So how do we test secure messaging?
  - We specify the parameters for secure messaging:
    - Session keys
    - Request APDU payload and actual APDU
    - Send sequence counter for the request
    - The expected constructed and encrypted request APDU
    - The response APDU payload
    - The send sequence counter for the response
    - The expected constructed and encrypted response APDU

Testing of Marshalling

- There are two types of marshalling defined in ISO/IEC 24727
  - ASN.1 – DER/TLV (Distinguished Encoding Rule / Tag Length Value)
  - Web service presentation – WSDL for SOAP implementations and XML for non SOAP implementations in compliance with the ISOIFD.XSD definition.

Testing of Stack Models

- What needs to be tested:
  - Stack models are a combination of ISO/IEC 24727 components as defined in Part 4
  - Initially components are tested standalone
  - Finally all components that make up the stack models are tested as a complete stack

Test Reports

- Identify which components under test have passed conformance testing.
- Detail why certain components have not achieved conformance.
- Are generated automatically.
- Are used to establish vectors of conformance.

Conclusion

- ISO/IEC 24727-5 ensures that an implemented component that conforms to ISO/IEC 24727 is interoperable with other implementations, which use that component, of that standard
- ISO/IEC 24727-5 is the specification that test laboratories base their conformance tests upon

Questions?

Thank you

Alexander Gagel
Principal Advisor (Solutions Architecture)
New Queensland Driver Licence
Enterprise Information and Systems Division
Department of Transport and Main Roads
Email: alexander.z.gagel@tmr.qld.gov.au

New Queensland Driver Licence
Email: newlicence@tmr.qld.gov.au
Mail: New Queensland Driver Licence Project
GPO Box 1412 Brisbane Qld 4001