Model-Based Testing

From theory to practice (3/3)

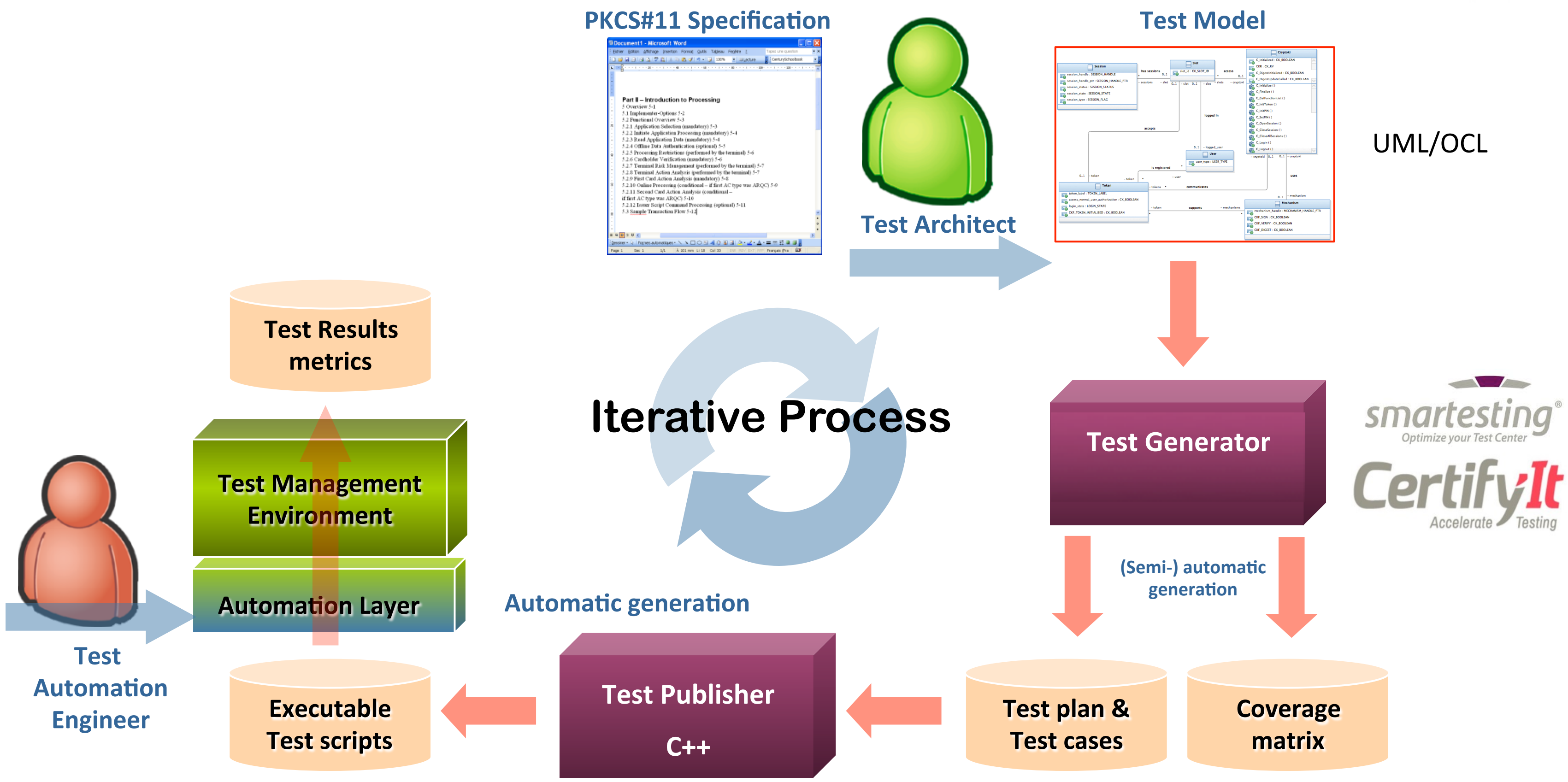
Bruno Legeard, Frédéric Dadeau, **Elizabeta Fourneret**

Ecole de Jeunes Chercheurs en Programmation – Nancy – 24 juin 2015

Agenda

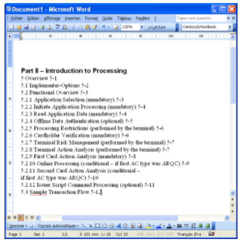
1. PKCS#11 Specification
2. Designing the PKCS#11 test model
3. PKCS#11 test selection criteria & test generation process
4. The test harness, the test publication and the test concretization
5. Test execution and results

Model-Based Testing with CertifyIt



Model-Based Testing with CertifyIt

PKCS#11 Specification

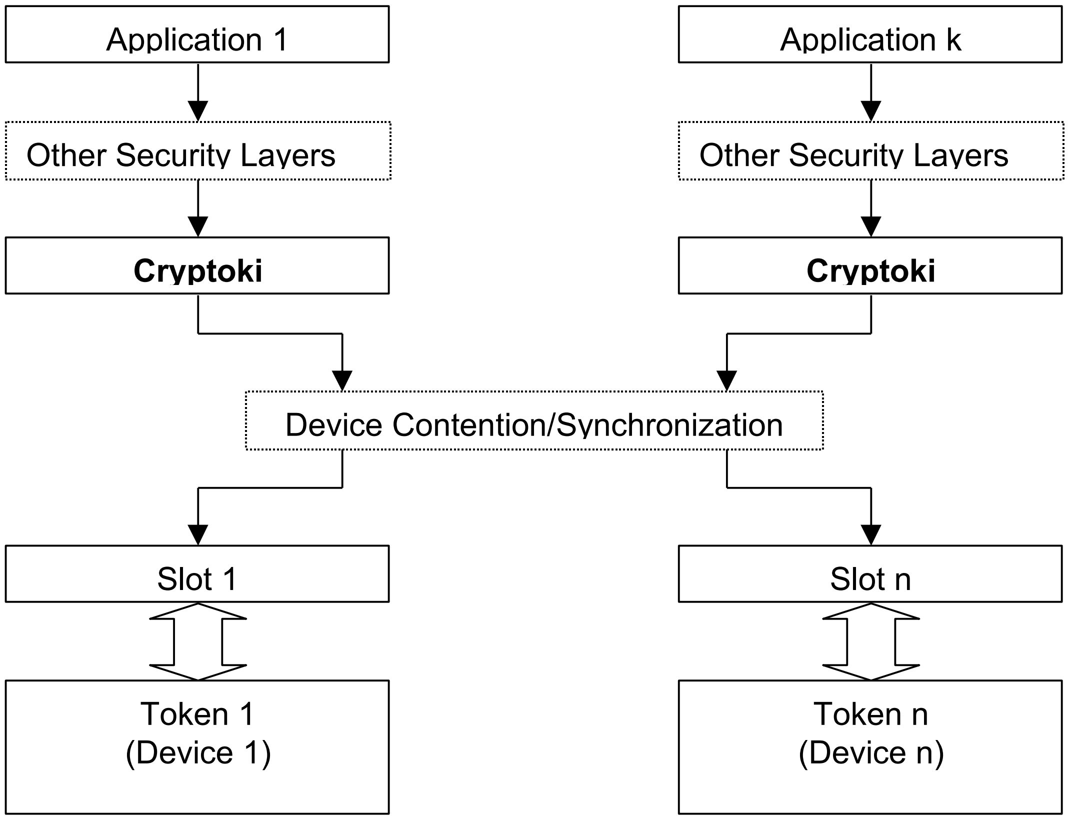


PKCS#11 Specification

- The PKCS#11 specification defines a standard for interfacing with cryptographic tokens.

- Defines an API, called « Cryptoki » with a set of C functions, including cryptographic functions.

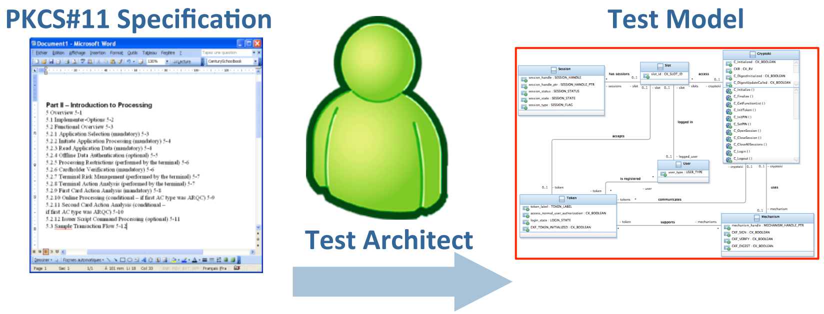
General Cryptoki model



PKCS#11 Scope

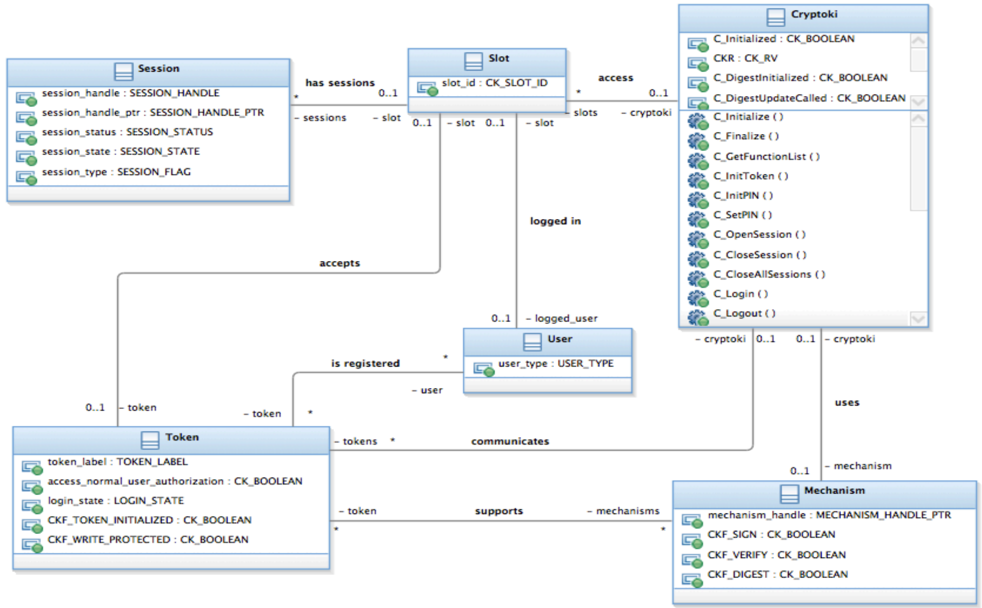
- General purpose functions
  - Ex. Initialize / terminate communication
- Session management
  - Ex. Open / close session, login/logout
- Token management
  - Ex. Initialize token, pin, modify pin
- Cryptographic functions
  - Sign, verify, digest funcitons, cryptographique key generation

Model-Based Testing with CertifyIt

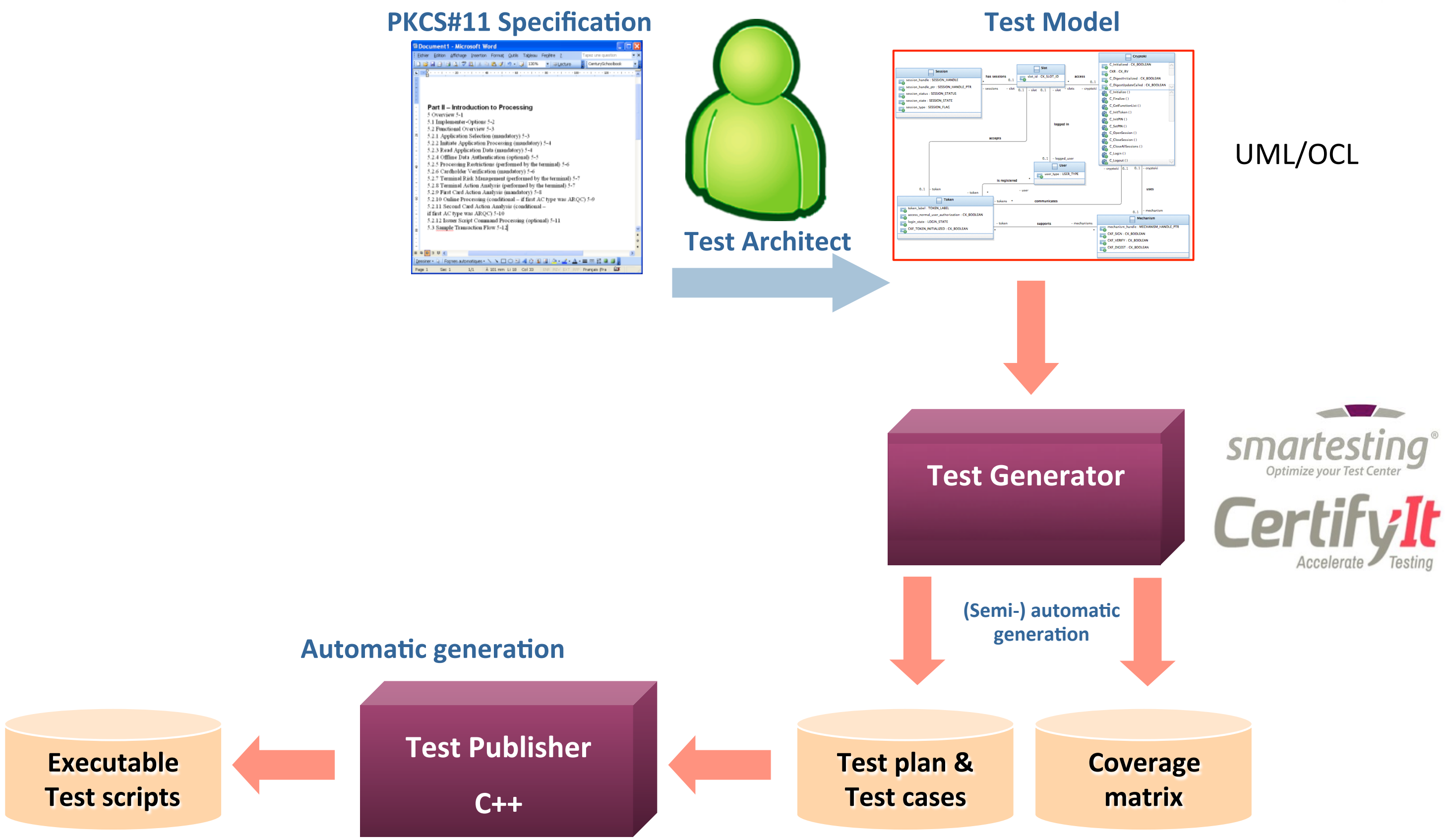


UML/OCL

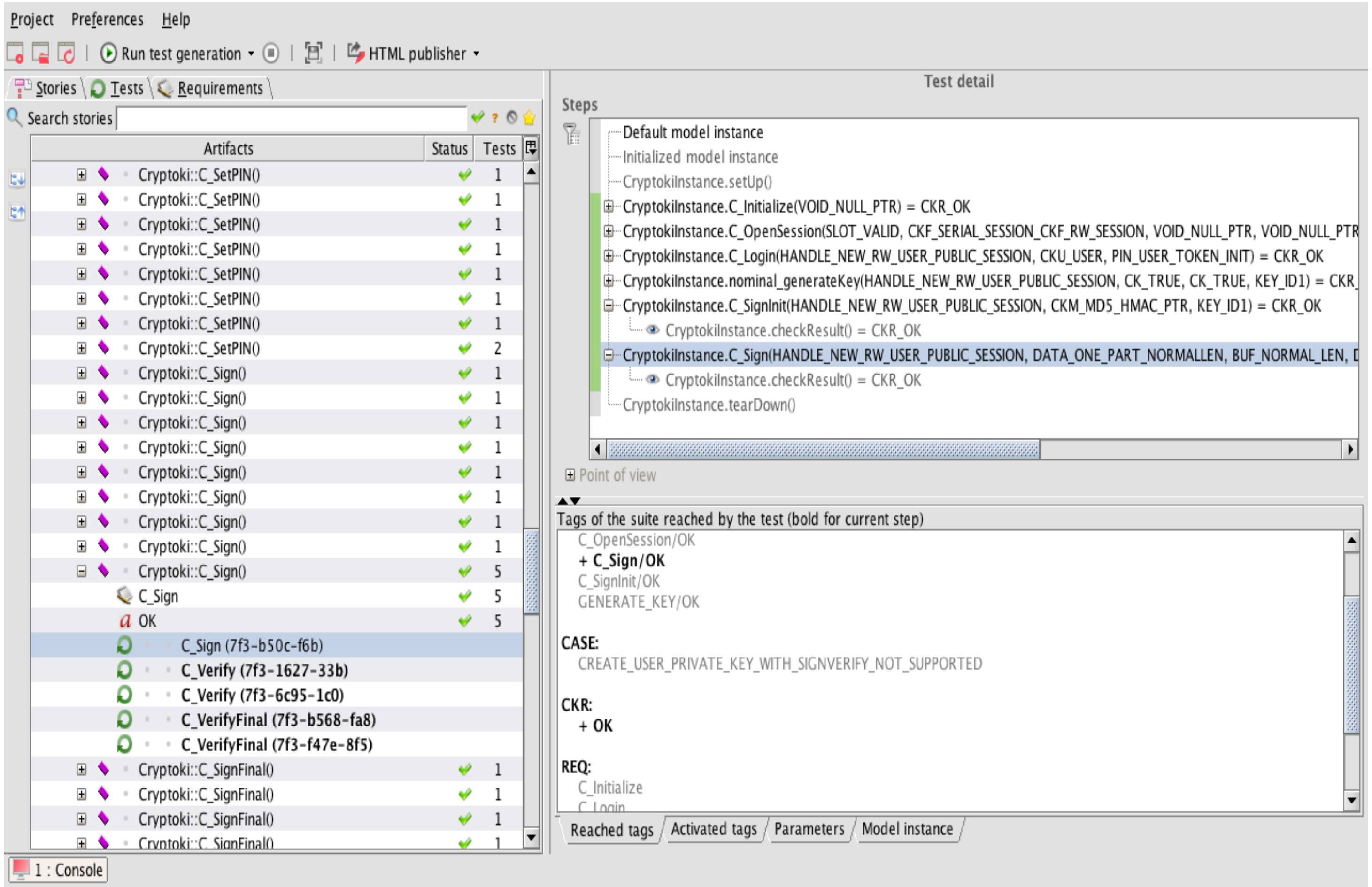
PKCS#11 test model - demo



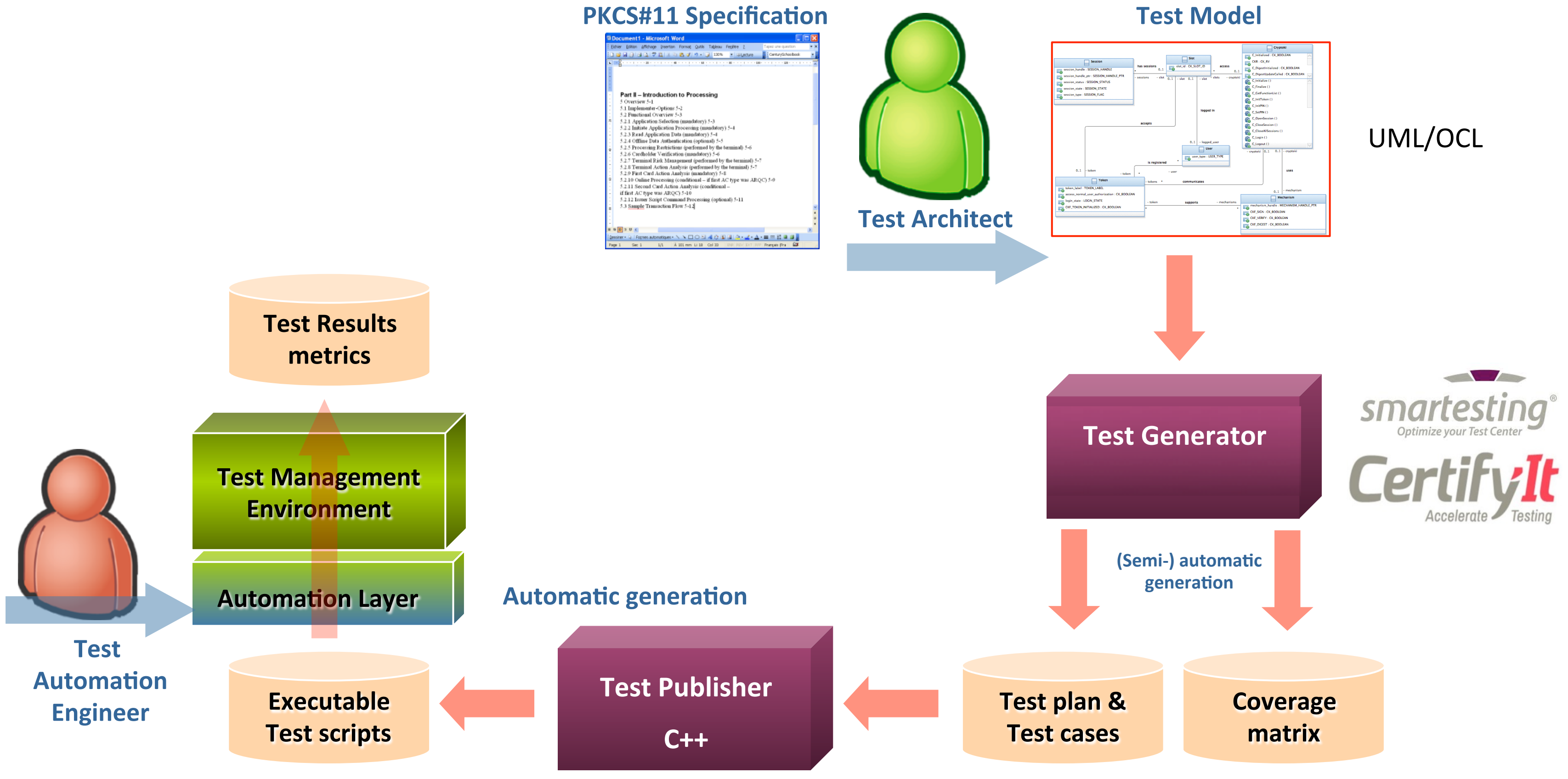
Model-Based Testing with CertifyIt



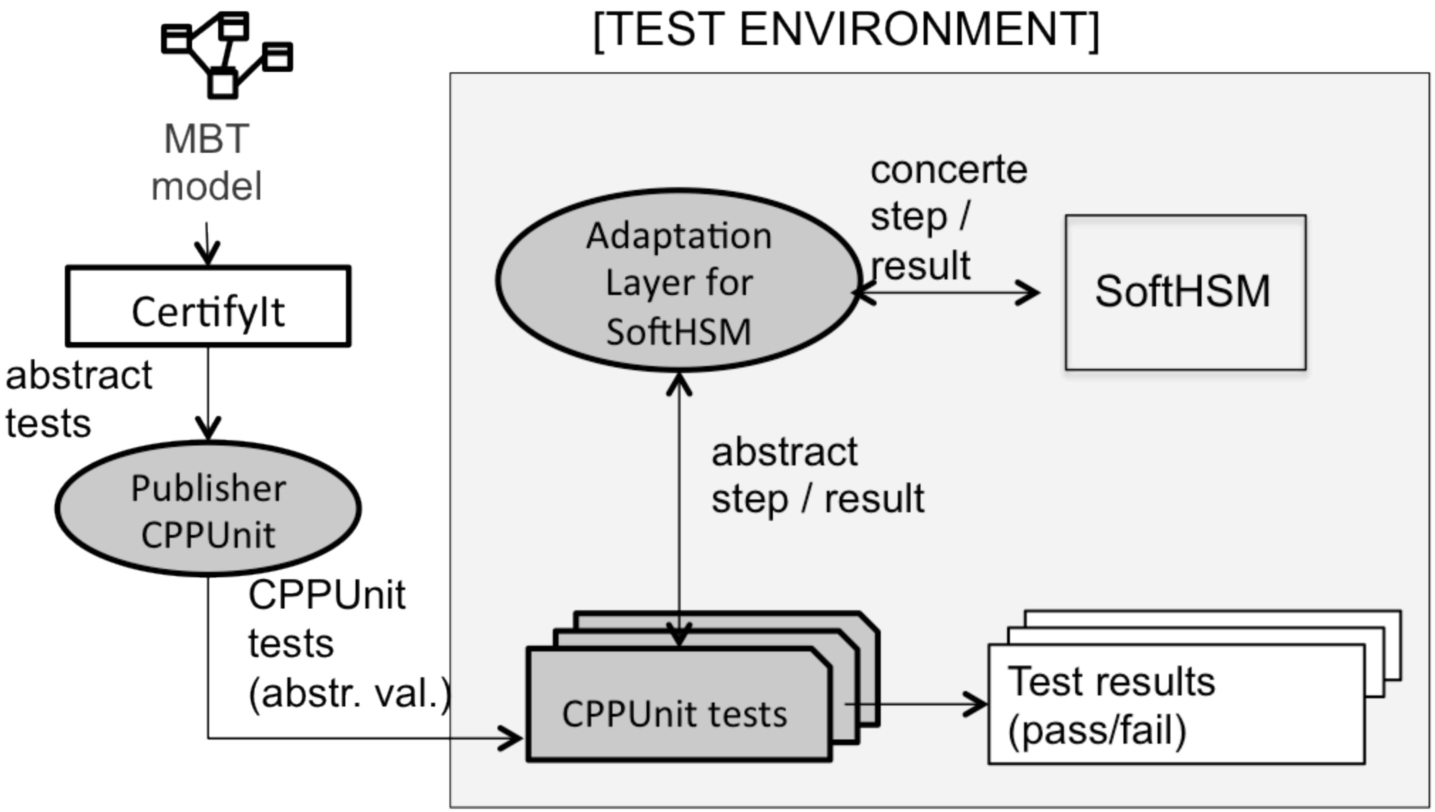
Test generation and test evaluation - demo



Model-Based Testing with CertifyIt

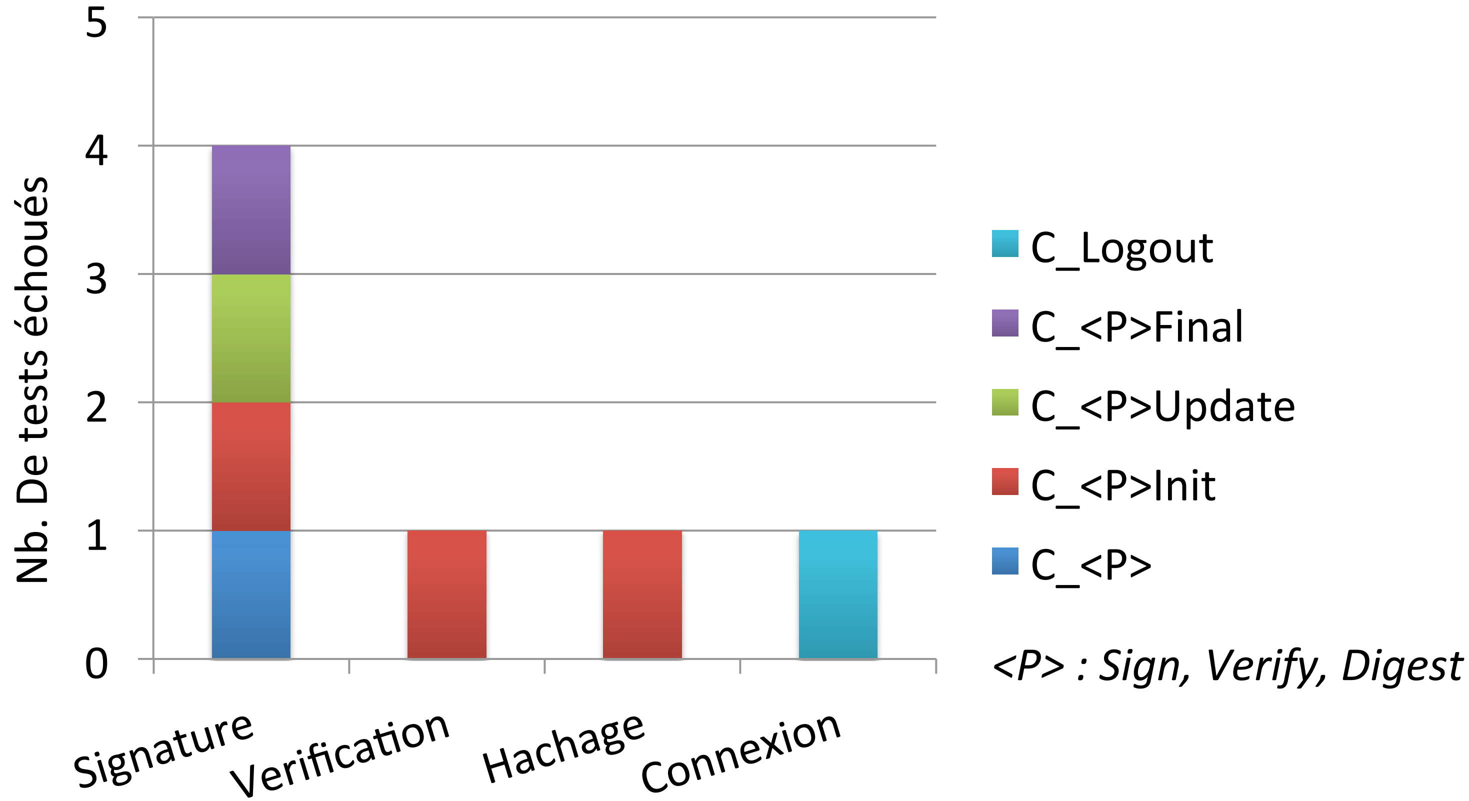


Test harness, test publication and concretization



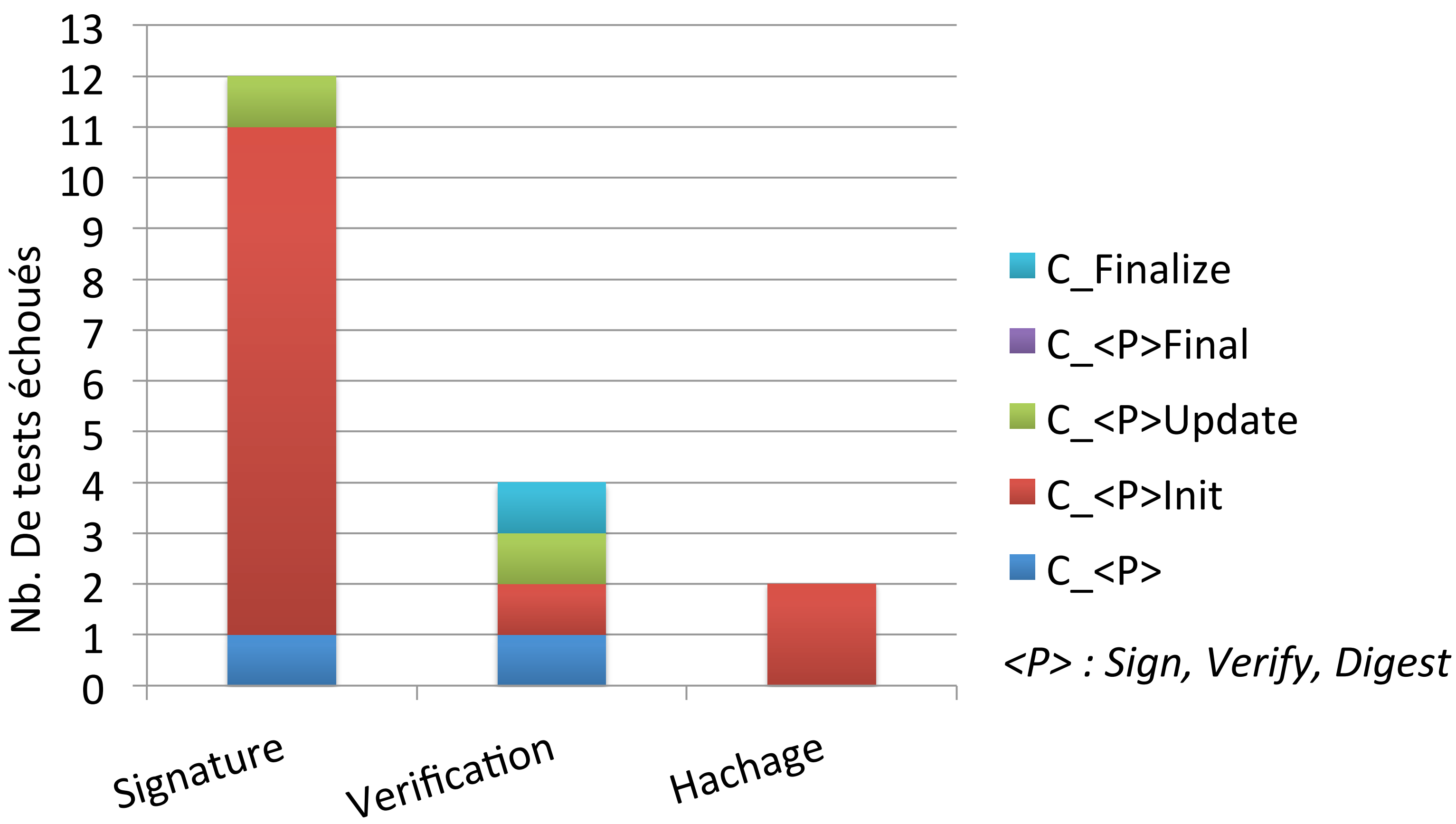
Test execution and results -demo

- Functional test suite (Total : 189 tests)
  - **183** tests **OK , 6** tests **FAILED**



Test execution and results - demo

- Security test suite (Total : 107 tests) - **90** tests **OK** , **17** tests **FAILED**



Now, It's YOUR Turn...