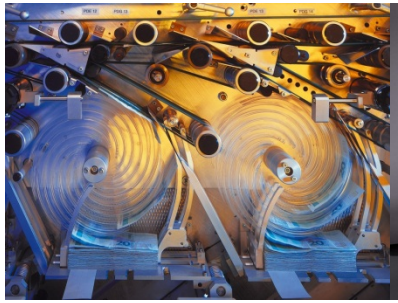
Development and Industrial Application of Multi-Domain Security Testing Technologies

Case Study Experience Sheet
Trusted Service Manager (TSM) Case Study from Gemalto

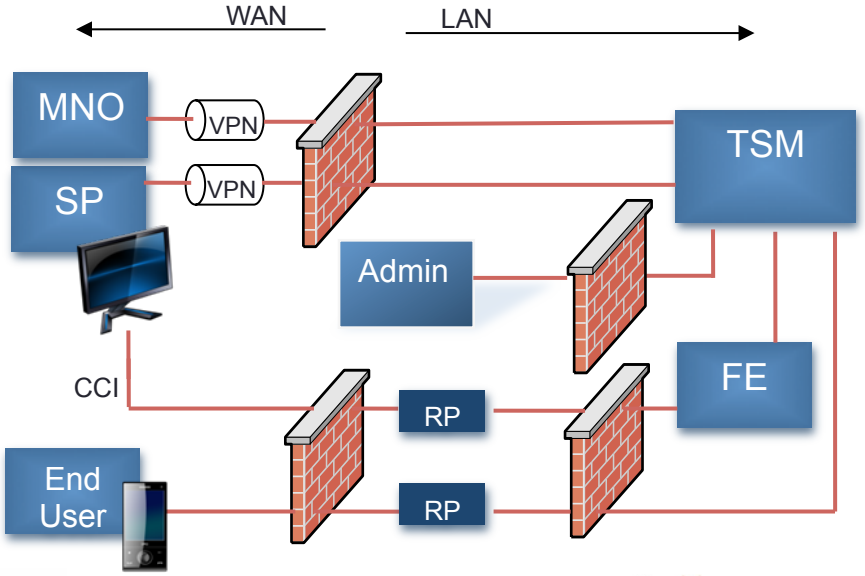



ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

Telecommunication Case Gemalto
Characterization

The Trusted Service Manager (TSM) remotely manages NFC services on behalf of service providers into end user mobile secure elements:

- Secure element can be a SIM card or a µSD
- NFC service could be payment or transport card, hotel key, loyalty card …

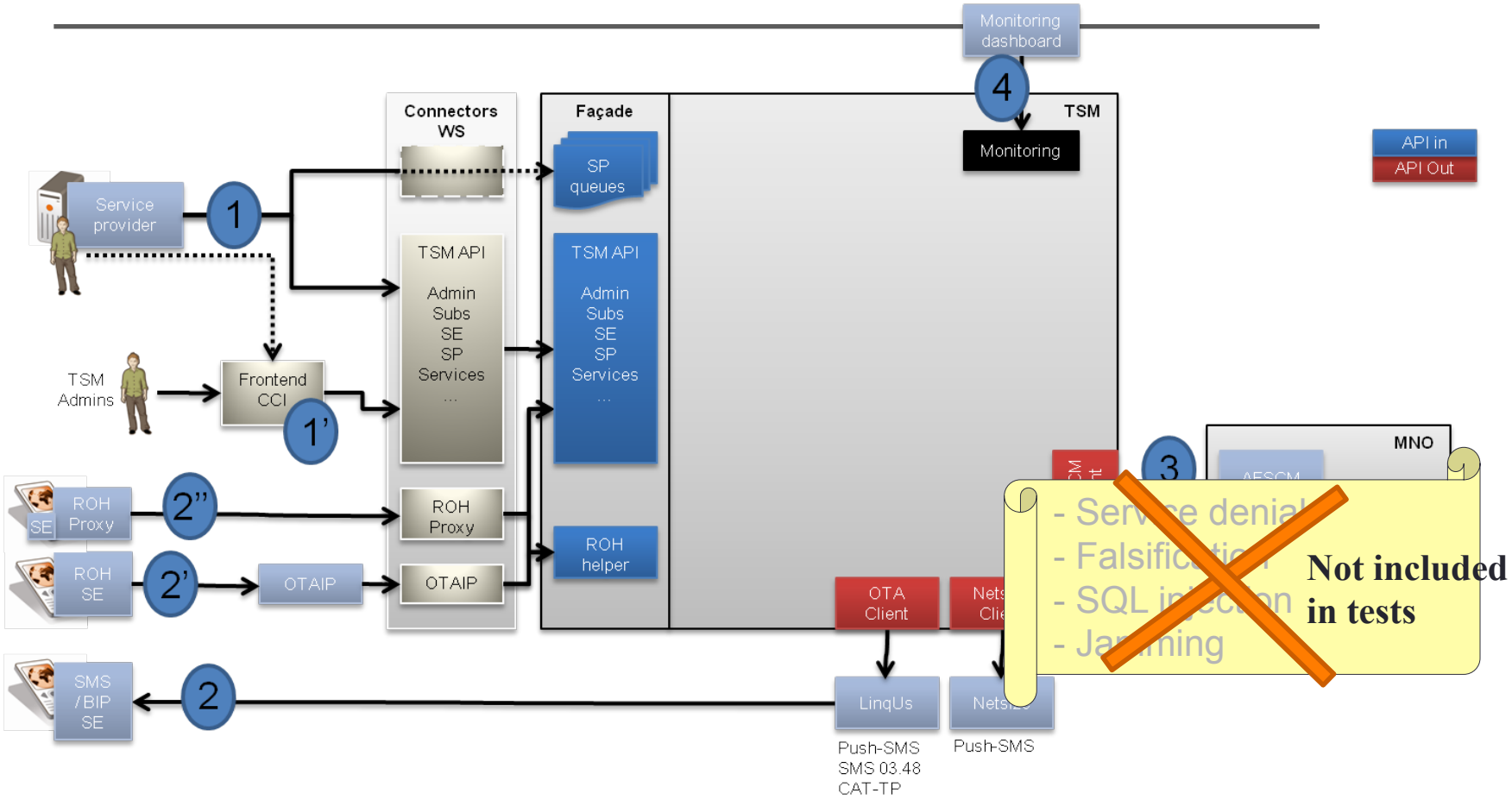


MNO = Mobile Network Operator
SP = Service Provider
Admin = Administrator
RP = reverse proxy
FE = TSM Front End

Telecommunication Case Gemalto
Characterization

- Security challenges
  - **Restricted access to web services:** The access to all web services should be restricted to authorized users. Accessing a web service allows provisioning the Trusted Service Manager and launching service activation, deletion, lock ...
  - **Prevent Admin Hijacking:** The administrator account of the operation system, the database and the TSM application should be secured to prevent hijacking this account. Hijacking an administrator account is used to get the privileges of an administrator account.
  - **Prevent manipulation of database data:** The database contains sensitive information about the end user such as MSISDN or banking personalization data. The data in the database should be secured to prevent manipulation.
  - **Prevent infiltration/manipulation of software:** The trusted service manager should be secured to prevent manipulation and infiltration. Software manipulation can be used to fake data or to provoke errors on the trusted service manager behavior.
- Case study: testing TSM behavior in case of attack
  - Interface 1: Provisioning of database with corrupted data (state-charts) with admin access (restricted access to web service and admin hijacking)
  - Interface 2: Sending back fake data (infiltration / manipulation)

Telecommunication Case Gemalto
Test interfaces



1.SP/Admin ⇦⇨ TSM
2.TSM ⇦⇨ remote secure element (in mobile)
3. TSM ⇦⇨ MNO
4. JMX events for monitoring interface

Telecommunication Case Gemalto
Results

- **Tests run without MMOG**

(Gemalto smart reverse proxy filtering first level of attacks)

  - Only testing of TSM: not full system as in production environment
  - Results to be mitigate compare with MMOG usage

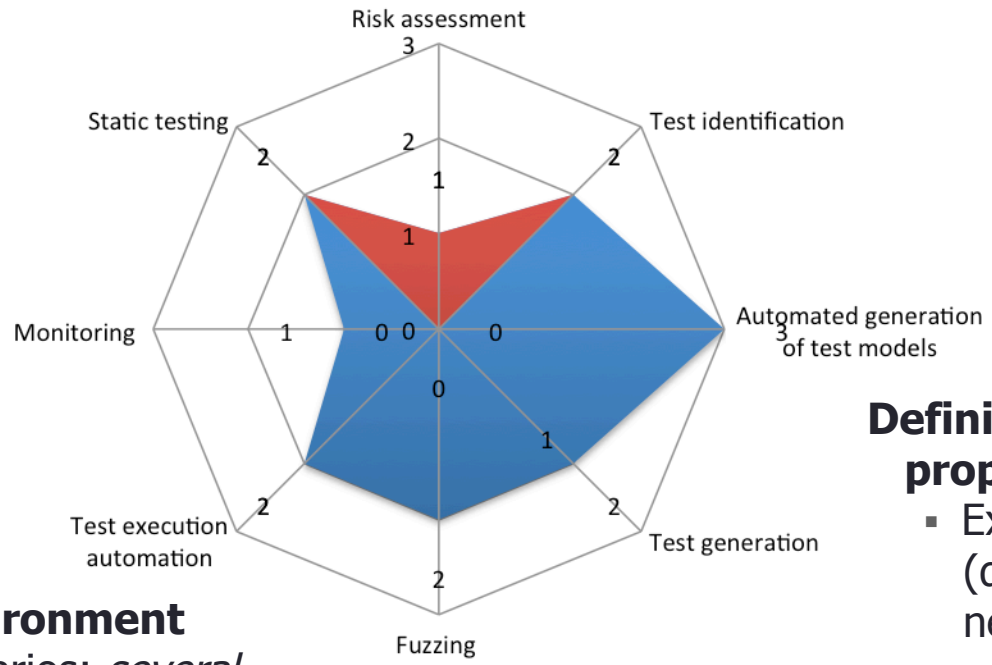
- **Focus on risks related to**
  - Configuration / provisioning modification (interface 1)
  - Manipulation of data (interface 2)
- **Until now, 2 weaknesses were found**
  - Both are corrected in new product version
  - Confidence in the security of the system is strengthened
- **Metrics**
  - TSM stability / robustness
  - Security property definition

Telecommunication Case Gemalto
Exploitation

- **For risk analysis has been proved of value**
  - graphical modelling
  - specification of assets to be protected
- **Saved resources due to**
  - reuse of functional test cases and
  - reuse of test execution environment for non-functional security testing
  - integration of data fuzzing in the TTCN-3 execution environment
    - keeps the behavioural model clean and concise
    - allows easy combination of data and behavioural fuzzing
- **Standardization of DIAMONDS results provides certification options for products with security requirements**

Telecommunication Case Gemalto
Summary

- **Improvement gains according to DIAMONDS STIP:**



Automated test environment

- For complex scenarios: *several approaches combination* (dynamic behavior verification)
- Reusable for functional and non-functional security testing

Definition of security properties

- Extendable model (database check or new properties)