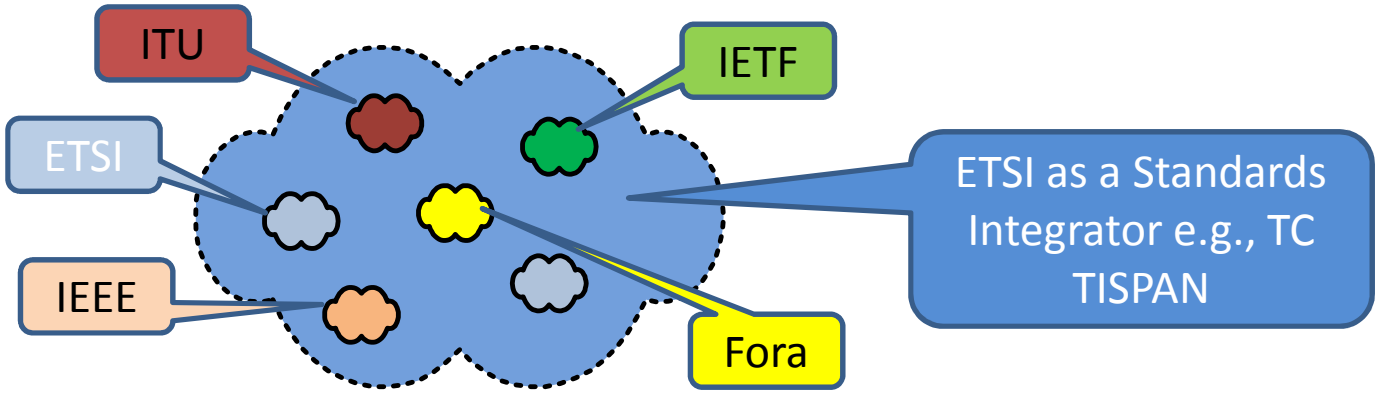
ETSI CENTRE OF TESTING & INTEROPERABILITY

JANUARY 2011

Standardisation and Interoperability

- We live in an interconnected world and interoperability is key to drive it forward
  - *In our homes* - Digital Home, Smart House
  - *In our cars* - Intelligent Transport Systems etc. etc.
  - *Indeed, all around us* - Internet of Things, M2M (embedded communication)
- Users benefit from increased choice from multiple manufacturers
  - Business, Governmental, Private Consumer
  - And they expect 'stuff to work' (Plug&Play)
- Manufacturers benefit from a larger market
  - Economies of scale
- **Standardisation enables interoperability**

ICT Technologies are Multi-Standards

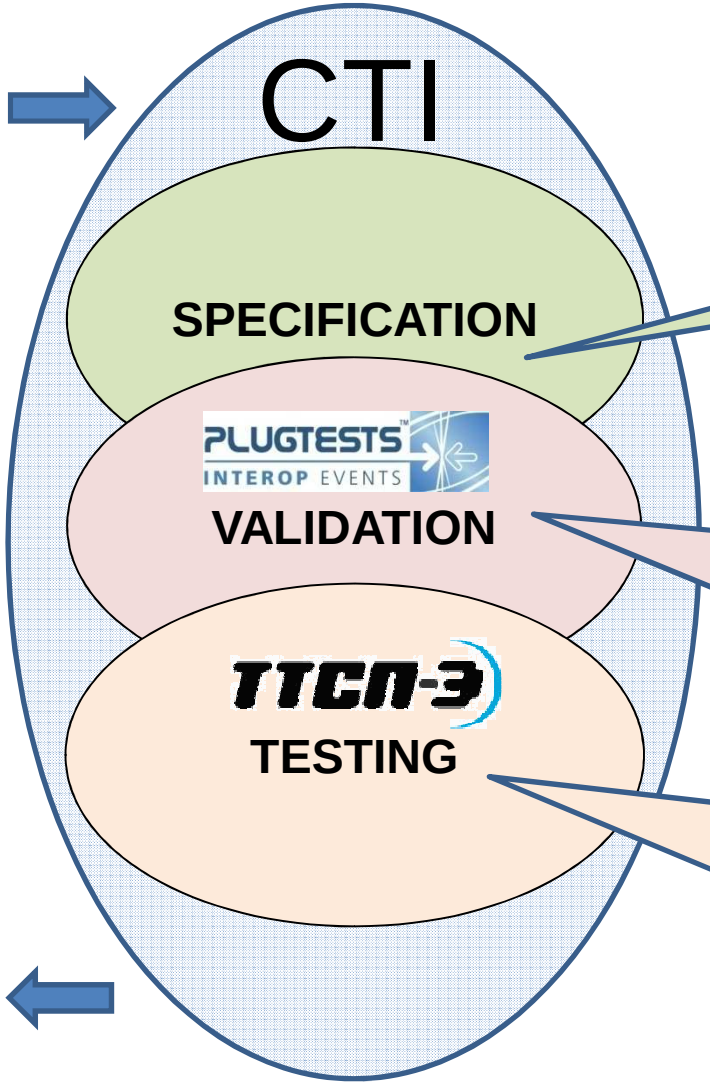


- ICT technologies are often specified by 'islands of standards'
  - From different standardisation bodies or organisations
- Results in potentially non-interoperable standards and/or products
- Varying technical quality
  - Requirements poorly specified (unclear), ambiguous or missing …
  - Lack of clear system overview
- Inadequate handling of
  - Options and/or Error behaviour
- Using standards beyond their original purpose
- Lack of consistent maintenance
- Etc.

CTI Support to TBs for the Development of Interoperable Standards

Customers

3GPP
AERO
ATTM
BRAN
CLOUD
DECT
eHEALTH
ERM
ESI
HF
INT
ITS
LI
MTS
PLT
SCP
STQ
TETRA
TISPAN



Support ETSI Technical Committees on the application of best practice protocol **specification methods**, **techniques** and **tools**.
e.g., ASN.1, UML, MBT (Model Based Testing)

Support ETSI Technical Committees on the **validation of standards**.
Mainly **Plugtests** events (**organisation** and provision of **testing expertise)**

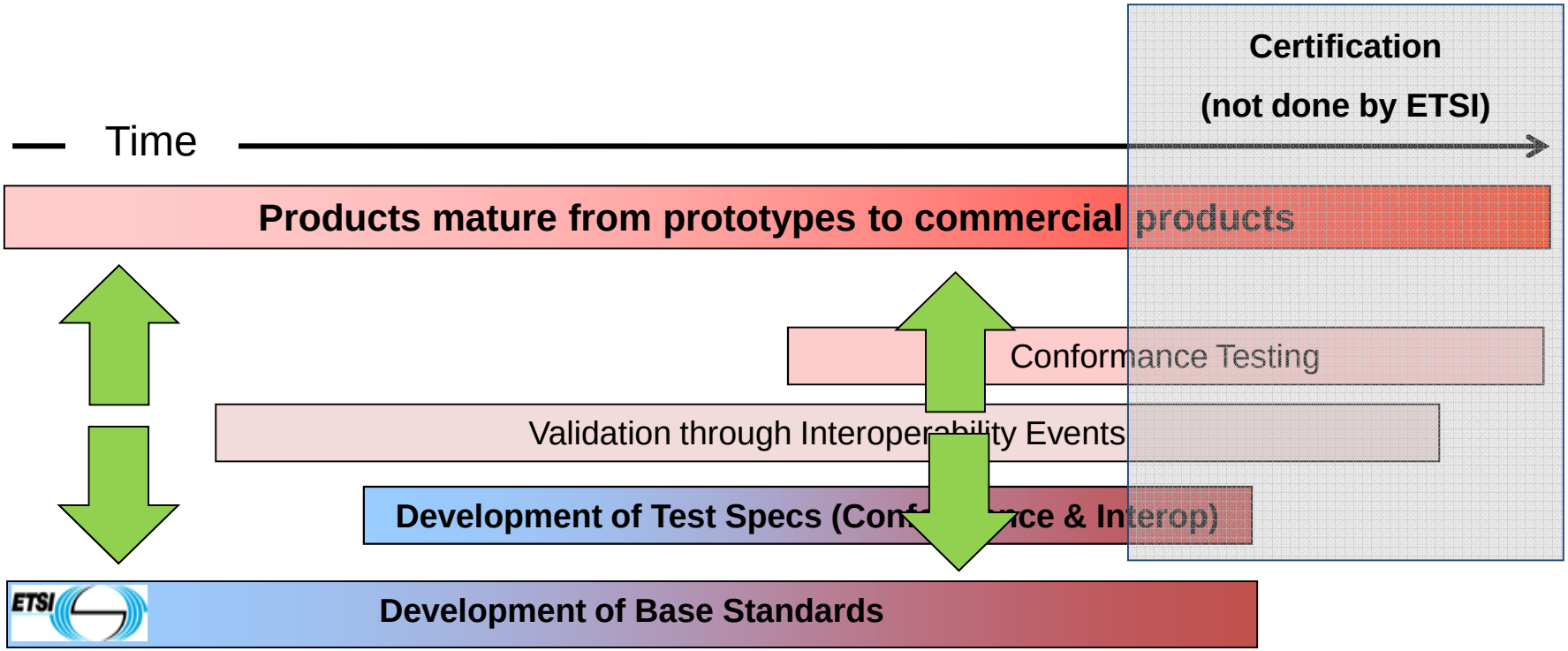
Support ETSI Technical Committees on ALL testing aspects including the development of **test frameworks**, **methodologies**, **test specifications.** Mostly through **participation/leadership of STFs**
e.g., STF 160, ITS, TTCN-3

CTI RESPONSIBLE FOR THE INTEROPERABILITY CLUSTER

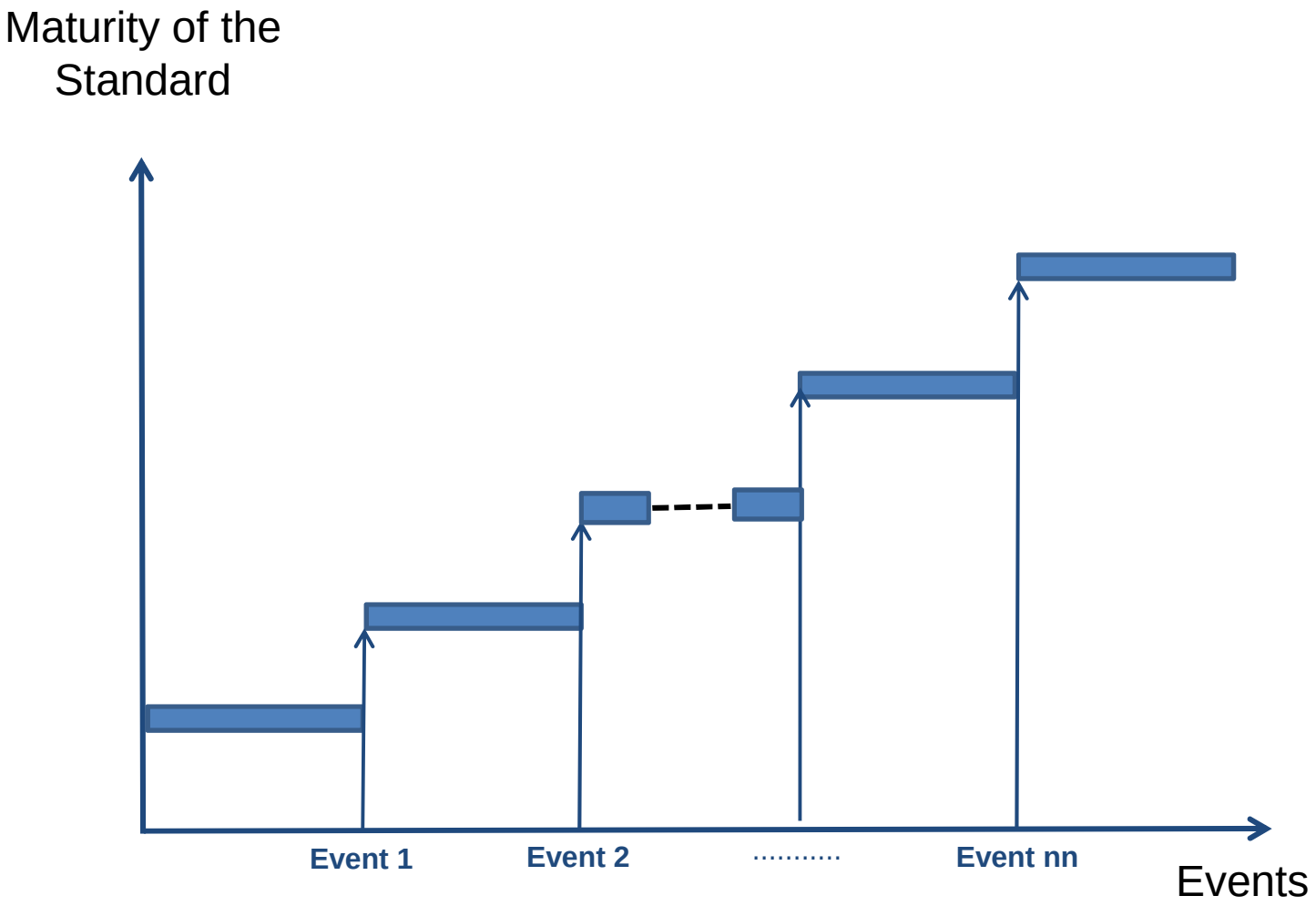
Why Validate Standards?

- Validation reveals problems/errors in
  - Standards and Products
- Validated standards give a higher chance of interoperable products
  - For standardisers gives assurance that they provide right functionality
  - For manufacturers and operators gives confidence to implement and go to market
- Provides an opportunity to correct errors in a controlled manner
  - Late fixes in the product cycle are more expensive than early ones
  - Decreases time to market
- **Standards can be validated by several means but one of the most practical and cost effective is by** PLUGTESTS™ INTEROP EVENTS

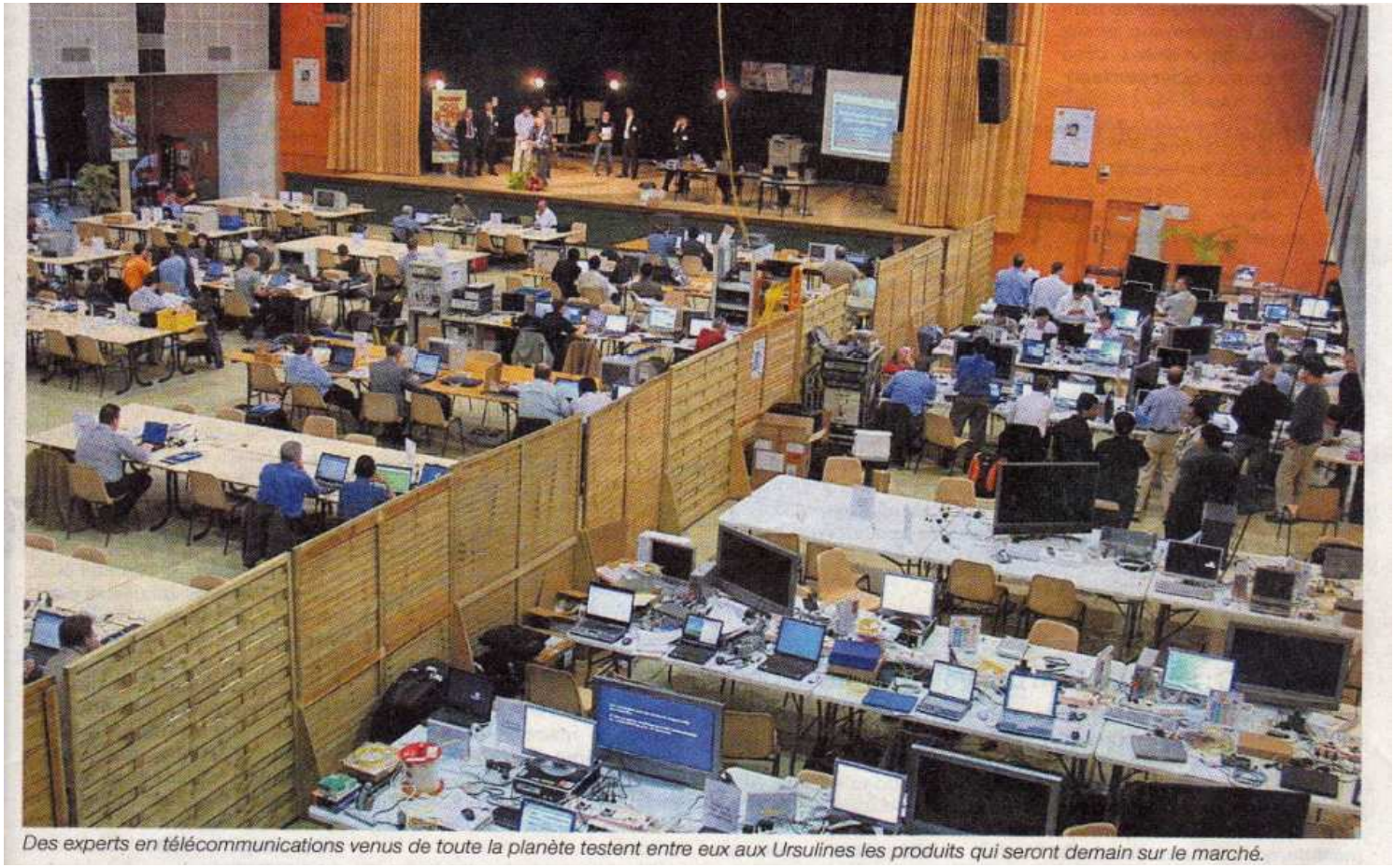
Relationship Between Standards, Validation and Testing



Series of IOP Events



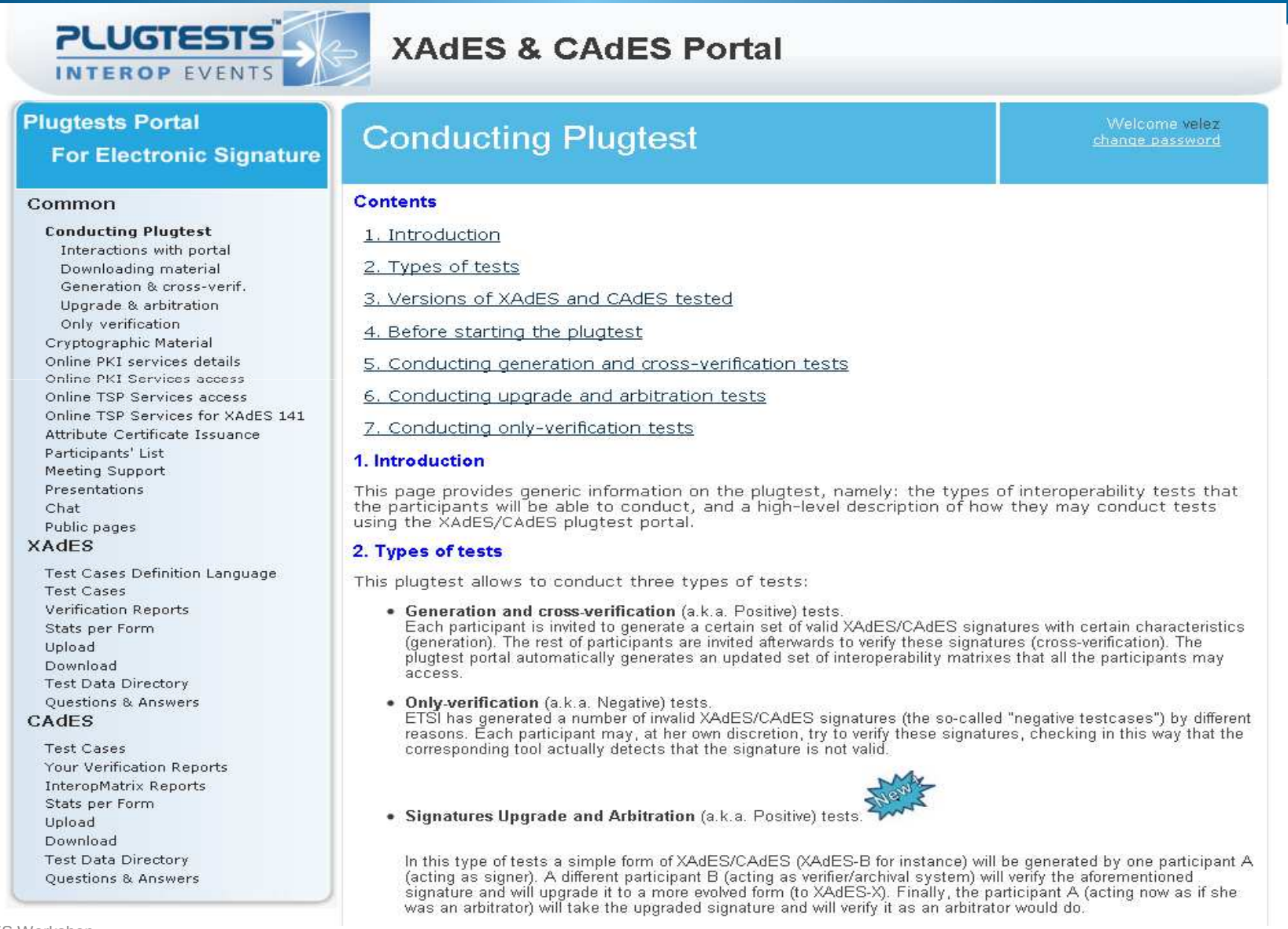
Plugtests™ can look like this…



Des experts en télécommunications venus de toute la planète testent entre eux aux Ursulines les produits qui seront demain sur le marché.

… or this (Car2Car Interop)

… or this (XAdES/CAdES Remote IOP)



PLUGTESTS INTEROP EVENTS

XAdES & CAdES Portal

Plugtests Portal
For Electronic Signature

Common
- **Conducting Plugtest**
  - Interactions with portal
  - Downloading material
  - Generation & cross-verif.
  - Upgrade & arbitration
  - Only verification
- Cryptographic Material
- Online PKI services details
- Online PKI Services access
- Online TSP Services access
- Online TSP Services for XAdES 141
- Attribute Certificate Issuance
- Participants' List
- Meeting Support
- Presentations
- Chat
- Public pages

XAdES
- Test Cases Definition Language
- Test Cases
- Verification Reports
- Stats per Form
- Upload
- Download
- Test Data Directory
- Questions & Answers

CAdES
- Test Cases
- Your Verification Reports
- InteropMatrix Reports
- Stats per Form
- Upload
- Download
- Test Data Directory
- Questions & Answers

Conducting Plugtest

Welcome velez
change password

Contents

1. Introduction

This page provides generic information on the plugtest, namely: the types of interoperability tests that the participants will be able to conduct, and a high-level description of how they may conduct tests using the XAdES/CAdES plugtest portal.

2. Types of tests

This plugtest allows to conduct three types of tests:

- **Generation and cross-verification** (a.k.a. Positive) tests.
  Each participant is invited to generate a certain set of valid XAdES/CAdES signatures with certain characteristics (generation). The rest of participants are invited afterwards to verify these signatures (cross-verification). The plugtest portal automatically generates an updated set of interoperability matrixes that all the participants may access.
- **Only-verification** (a.k.a. Negative) tests.
  ETSI has generated a number of invalid XAdES/CAdES signatures (the so-called "negative testcases") by different reasons. Each participant may, at her own discretion, try to verify these signatures, checking in this way that the corresponding tool actually detects that the signature is not valid.
- **Signatures Upgrade and Arbitration** (a.k.a. Positive) tests. New

  In this type of tests a simple form of XAdES/CAdES (XAdES-B for instance) will be generated by one participant A (acting as signer). A different participant B (acting as verifier/archival system) will verify the aforementioned signature and will upgrade it to a more evolved form (to XAdES-X). Finally, the participant A (acting now as if she was an arbitrator) will take the upgraded signature and will verify it as an arbitrator would do.

Typical Plugtests Events

- In operation since 1999 (in CTI since 2007)
- Nearly 150 events, involving more than 4000 engineers
- For many diverse technologies

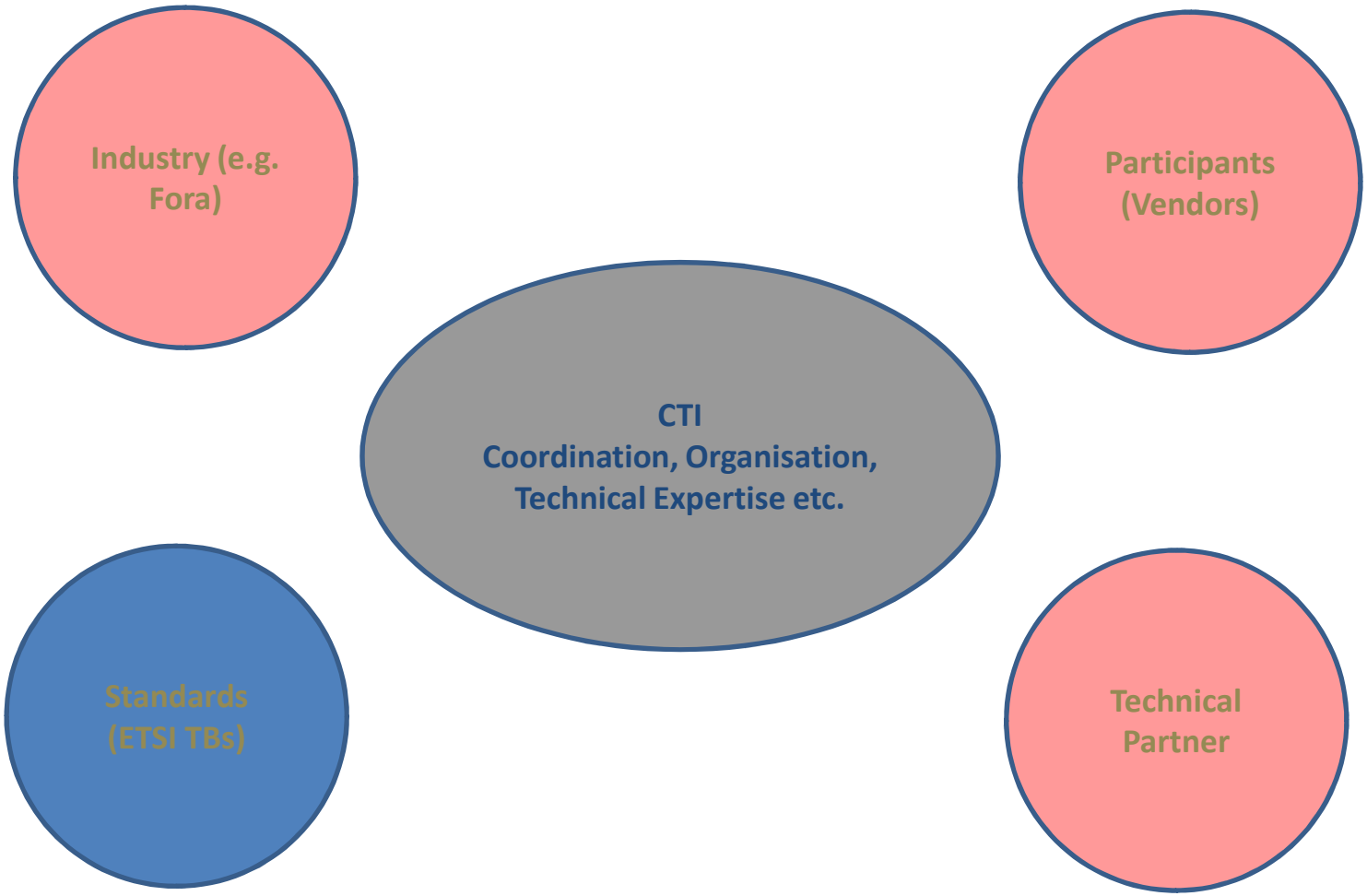
- IMS
- Bluetooth
- IPv6
- Triple Play over xDSL
- SIM/Handset
- WLAN IRAP
- RFID
- STQ (Speech Quality)
- WiMAX
- SIGTRAN
- Femtocell
- OSA/ParlayX
- SMS / MMS
- B2B (Business-to-Business)
- SIPiT
- J2ME – Mobile Apps
- HDMI
- VoIP for Air Traffic Management (EUROCAE)
- Electronic Signature (XadES, CadES)
- Lawful Interception
- Optical Fibre (GPON)
- Power Line (PLT)
- Intelligent Transport Systems (ITS – C2C)
- Fixed Mobile Convergence (FMCA)
- GRID/Cloud Computing
- ENUM

Events in 2010

- Security barcamp
- EUROCAE#4 (Air Traffic Management)
- Femtocell#1
- CONNECTATHON (eHealth)
- DECT CAT-IQ 2.0#1
- TTCN-3 User Conference (China)
- USIM Cards (Late cancellation, maybe 2011)
- DECT CAT-IQ 2.0#2
- GPON#5 (Gigabit Optical Networks)
- Electronic Signature XaDES
- Electronic Signature CaDES
- SIPit#27 (Taiwan)
- IMS Testing, Interoperability and Best Practices Workshop
- Femtocell#2 (Two events planned December 2010 moved to Jan. 2011)
- In the pipe 2011: Femtocell#3, IMS#4, Eurocae#5, SIPit#28, DLNA, CONNECTATHON, xGPON, IPv6

MZ2

Making it Happen

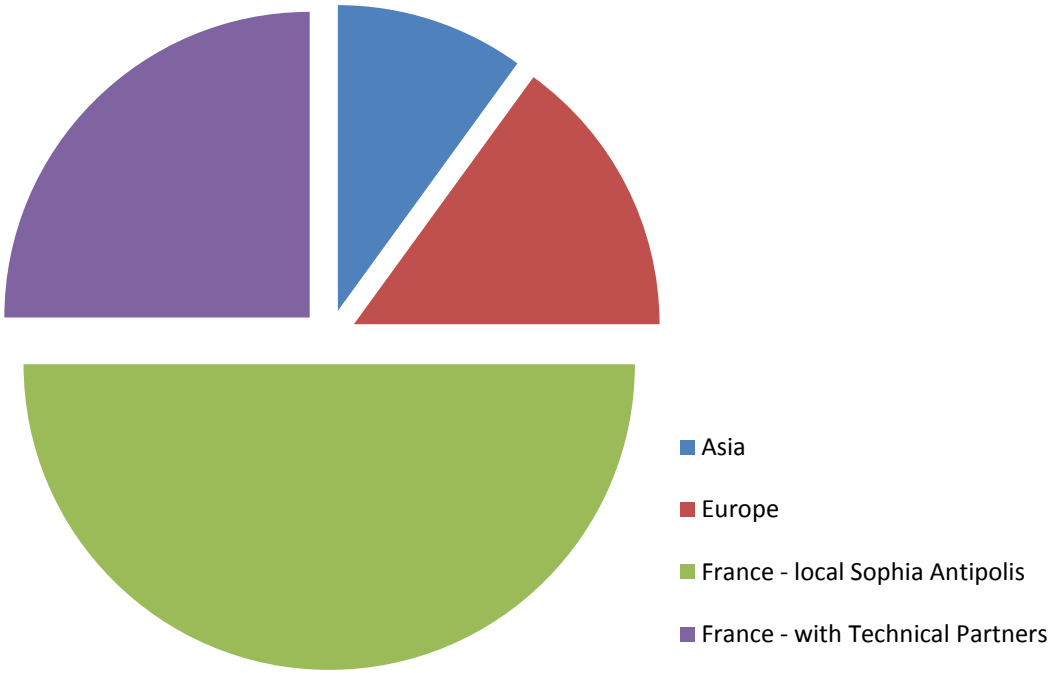


Slide 14

MZ2 Consider showing CTI with it's organizational and techical sides as key player. Maybe techical partner could be shown as optional?
Milan Zoric; 06/07/2010

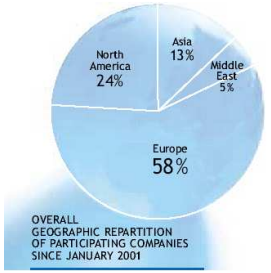
Where

- Hotels
- Test labs
- Technical partners
- …



Who attends Plugtests™ events?

- Plugtests are for ETSI TBs but
  - Participants do **not** have to be ETSI members
  - Events are open to any company/organisation bringing a product to the event
  - Vendors, operators, content or application providers, test tools etc.
  - Other Standardization Bodies, Fora or other interest groups may also attend
  - Universities and Research Institutes are also welcomed



- Prerequisite: **must** bring equipment to the event for testing
- Observers may be present but **only** at the request (agreement) of the community

Funding Sources

- EC grant
  - New contract on yearly basis (> 12 events)
  - Requires imagination to persuade DG enterprise to continue funding this activity (> 10 yrs now)
  - This funding is critical – but high admin overhead
- Fees
  - Usually a company fee and a participant fee
- Sponsors
  - Not common
- Target is to break-even over the year

Trends

- Events require more technical involvement
  - Building on an already good reputation
- Events becoming more complex
  - Femtocell, IMS …
  - Can require double effort (time)
  - Infrastructure costs (e.g., access to core networks)
- Move towards remote events
  - ETSI HIVE (Hub for Interoperability and Validation at ETSI)
  - ESI events (XAdES, CAdES, TSL)

Trends

- Events require more technical involvement
  - Building on an already good reputation
- Events becoming more complex
  - Femtocell, IMS …
  - Can require double effort (time)
  - Infrastructure costs (e.g., access to core networks)
- Move towards remote events
  - ETSI HIVE (Hub for Interoperability and Validation at ETSI)
  - ESI events (XAdES, CAdES, TSL)

XADES/CADES 2010 PLUGTESTS

Remote Interoperability Event

25th Oct – 5th Nov 2010

XAdES/CAdES 2010 Plugtests

- The XAdES event aimed at conducting interoperability test cases on XAdES and CAdES signatures

- This included an extension to the XAdES v1.3.2 and CAdES v1.7.4 with respect to previous Plugtests events. This extended test provided test coverage of the specification including testing signatures evolution, simulating real life situations.

- A new set of specific test cases was also provided to cover the extensions defined in the new XAdES v1.4.1 and CAdES v1.8.1

3 Types of tests

- Generation and cross-verification tests.

  Each participant is invited to generate a certain set of valid XAdES/CAdES signatures with certain characteristics (generation). The rest of participants are invited afterwards to verify these signatures (cross-verification).

- Only-verification tests.

  ETSI has generated a number of invalid XAdES/CAdES signatures by different reasons. Each participant tries to verify these signatures, checking in this way that the corresponding tool actually detects that the signature is not valid.

- Signatures Upgrade and Arbitration tests.

  A simple form of XAdES/CAdES is generated by one participant A (acting as signer). A different participant B (acting as verifier/archival system) verifies the aforementioned signature and upgrades it to a more evolved form. Finally, the participant A (acting now as arbitrator) takes the upgraded signature and verifies it as an arbitrator would do.

General information

- Event duration:
  - 25th Oct - 5th Nov 2010 (extended until 22 Nov due to the number of participants)
  - 4th XAdES and 2nd CAdES Remote interoperability event
- Server name: http://xades-portal.etsi.org
- Protected area
  - Username and password were needed to access to this testing portal

  ❑ The portal included PKI-related ONLINE services, needed to perform the tests (CA server, Time-stamp server, OCSP responders)

Participation

- 27 Companies were registered to the plugtests event
  - 27 companies performed XAdES interop
  - 17 companies also performed CAdES Interop
- 66 Participants registered from 18 countries among Europe, but also Turkey, Israel, USA and Japan.
- At the end of the Plugtest, a report has been produced that included recommendations for future XAdES/CAdES standardization activities, which has been submitted to ETSI TC ESI

THANK YOU!

Centre for Testing and Interoperability (CTI)
plugtests@etsi.org