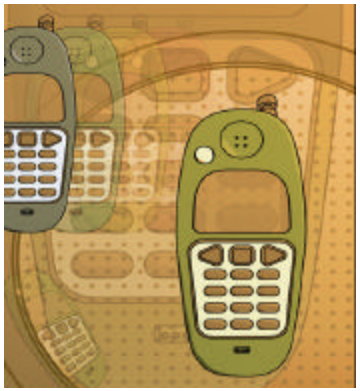
Security Issues in OTA Reconfigurabiltiy



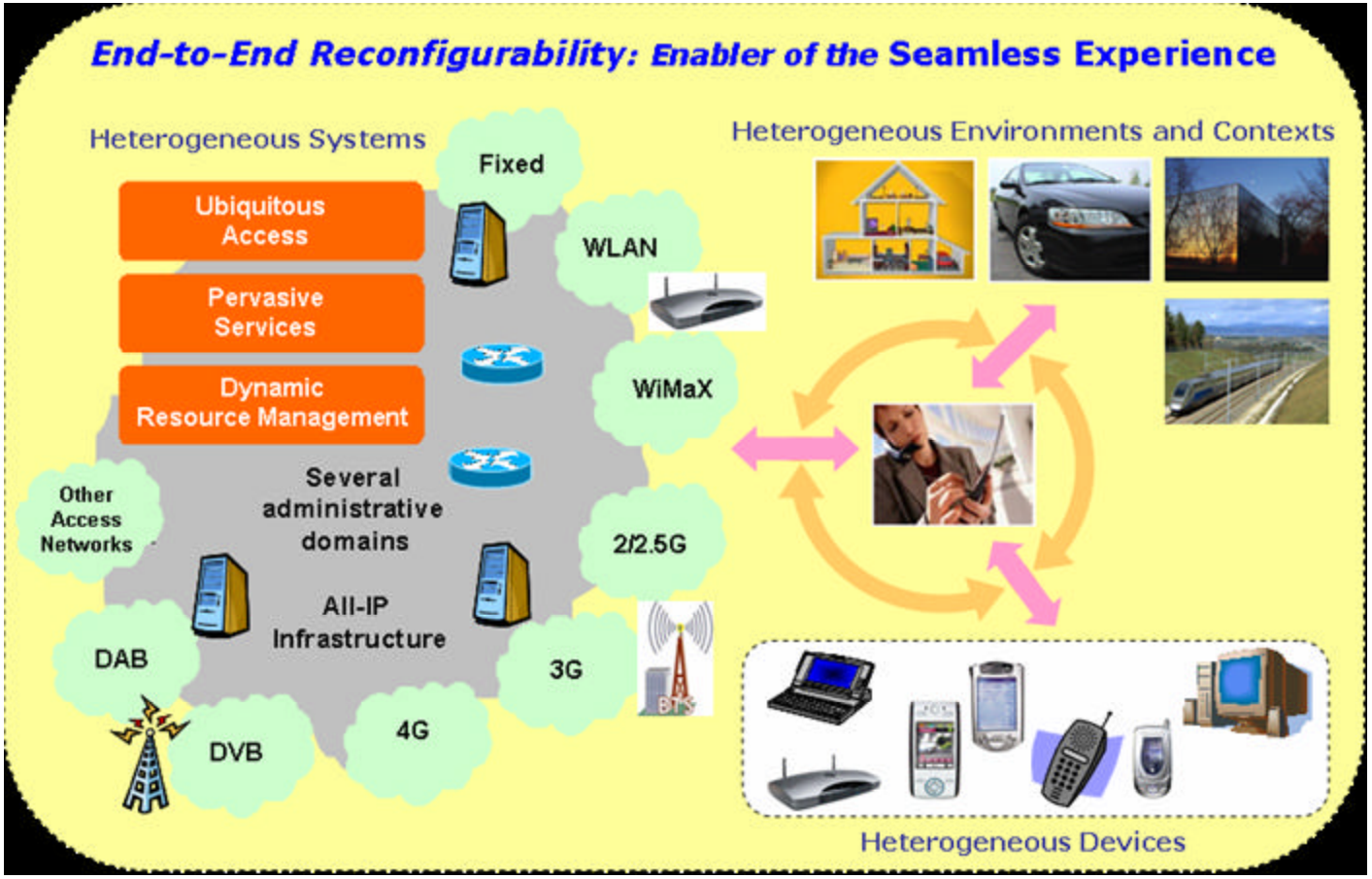
Karim El-Khazen
Rainer Falk
François Haettel
Ulf Lücking

E²R Project Objective

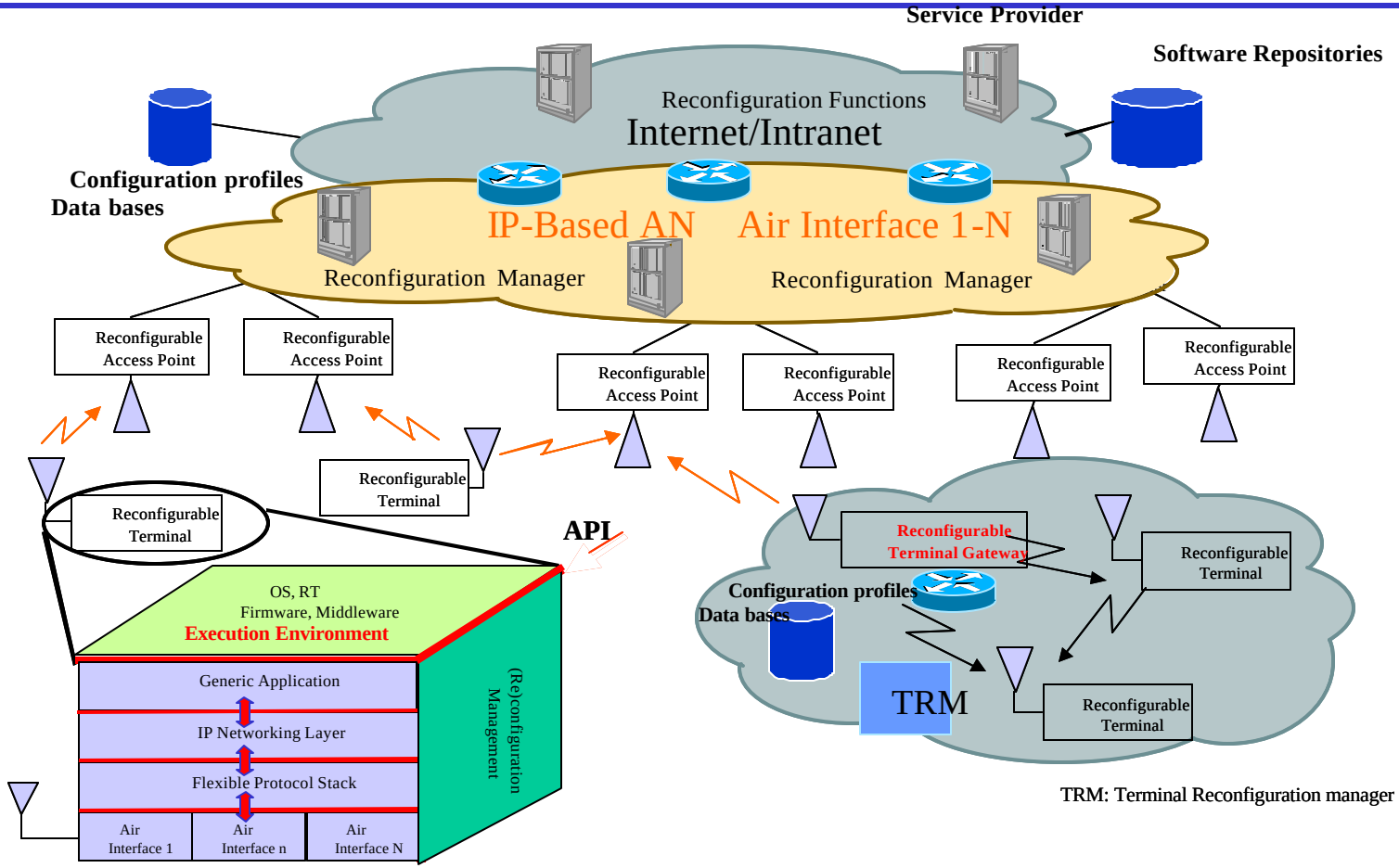
- ✓ The key objective of the E²R project is to devise, develop and trial architectural design of reconfigurable devices and supporting system functions to offer an expanded set of operational choices to the users, application and service providers, operators, regulators in the context of heterogeneous mobile radio systems
- ✓ Innovative research, development and proof of concept will be sought in an end-to-end aspect, stretching from user device all the way up to Internet protocol, and services, and in reconfigurability support, intrinsic functionalities such as management and control, download support, spectrum, regulatory framework and business models

E²R Project Scope

Beyond 3G (B3G) Systems



E²R Architectural Perspective

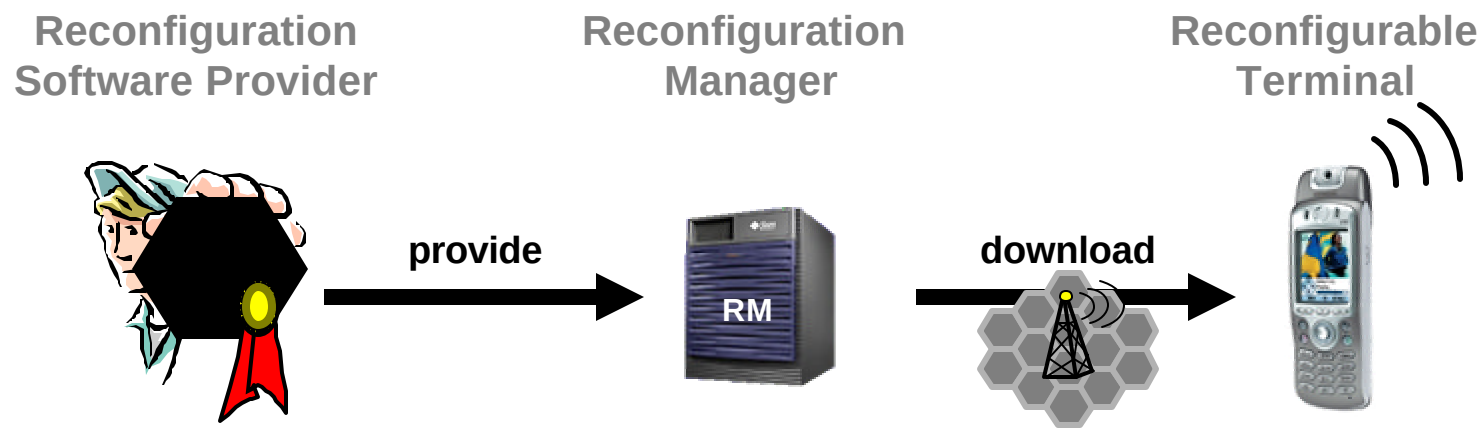


E²R Project Architectural Vision of the Beyond 3G System

Security Requirements System Perspective

- Authentication of the User
- Authentication of the Network
- Authentication of the Equipment
- Identification of all Involved Parties
- Reconfiguration Authorization
- Privacy of Exchanged Data (personal data, user profile and equipment profile stored in the reconfigurable equipment)
- Regulator Approval (for critical types of software)
- Software Certification (verify origin)
- Software Integrity
- Correct Operation of the Software (test and verify correct behaviour)
- Security of the Detection-control Mechanism

Secure OTA Reconfiguration



Radio Software Authorisation

Reconfiguration Control

Conformance

reliable, correct operation

Reconfiguration Classes

Different authorization policies depending on affected functionality

- Regulatory conformance: e.g. transmission frequency, emission power
- Network operator: e.g. monitoring and selection of most suitable radio technology, handover decisions, medium access algorithms
- Manufacturer: e.g. bugfixing, terminal upgrading
- Service provider: e.g. “branding” of user interface, software needed for service-provider specific services
- Value added Services provider: e.g. third party software services/applications
- End user: e.g. applications, user interface themes, background images, ring tones

Authorization Framework

- what needs to be signed: what to include in meta information, e.g. authorised target device(s), software identifier or approval number, region where may be used; further conditions that have to be met for activation of software module
- who is authorised (trusted) to sign a download software module and thereby authorise/approve its use.
- requires public key infrastructure with certificate management (what kind of certificate management?)

Security Issues - Reconfig. Equipment Perspective

- Access control
  - To the resources by authorized entities only (depending on trust levels)
  - To grant privilege rights to "only" concerned entities/parties
- Authorization
  - To avail services
  - To enforce flexible authorization policies over resources distributed within the equipment
- Secure Configuration Channel
  - To provide secure transport of re-configuration data and sensitive information
- Error Recovery and Rollback Mechanisms
  - To provide reliable operation of the equipment after installation of SW
  - New SW modules introduced into the protocol stack should not harm the system
- Secure OS Environment
  - To keep security related reconfiguration information protected inside a terminal, using dedicated modes, bootstrap methods and kernel functions
  - use of component-based kernel approach
    - allows the implementation of flexible access control strategies to provide hardened RTOS with respect to security

Security Issues - Reconfig. Equipment Perspective

- Authentication
  - Of the user/equipment to the network and vice-versa
    - during connection establishment
    - during vertical handover or horizontal handover to a different security domain
    - support of several methods of user and network authentication (e.g. WLAN, 3GPP) and enhancements to support (future) IP-based communication networks
- Confidentiality
  - Of sensitive data (e.g. security policies enforcement, reconfiguration information, mobile banking data etc.)
  - Of the entities relevant privacy data
- Secure management
  - Of large number of devices to guarantee privacy from a user/device and also from the different stakeholders (operators, manufacturers and service providers)
  - Useful for mass deployment of a service/upgrade
- Integrity
  - To avoid intervention of unsolicited parties to corrupt/modify/exchange the data

SW Activation Control

Restrictions concerning the conditions under which a radio software may be activated

- different regulations depending on the region/location
  - a radio software module may be activated only in a certain region: encode as meta information
  - different radio software authorization policies in different regions: switch and enforce the currently valid authorization policy (e.g. software authorization by manufacturer or by regulatory body)
- possibly a radio software module requires even a dynamic authorization by the currently used network
- when the same radio hardware model is marketed in different market segments (e.g. commercial wireless, public safety), only the corresponding software modules should be accepted (prevent that a user of a commercial device can download the software for police or air traffic control)

Summary

- Main Objective: ensure reliable, correct operation despite flexibility and openness introduced by reconfigurability
- Reconfiguration-Specific Security Requirements
  - protected reconfiguration environment local to equipment
    - provision of privilege modes for access control, authorization...
    - secure bootstrap methods
  - software authorisation (certification, approval)
    - horizontal vs. vertical market model
    - independent or combined approval of HW-SW-combinations
  - secure reconfiguration process
    - protected reconfiguration communication channel
    - authentication (robust certificate model)
    - authorisation (central, decentralised reconfiguration control)
    - access control (assigning privilege levels to entities)
    - correctness, privacy of profile and context data
    - network-based configuration validation
  - recovery, fault management
    - monitoring (watch-dog), recovery and/or rollback
- Mobile Security Requirements not Specific to Reconfiguration

Backup

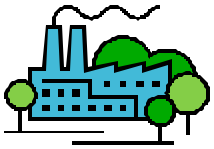
Actors

Trusted 3rd Party/
Security Entity

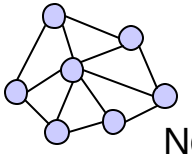
Spectrum manager

Regulator

Certification
Entity

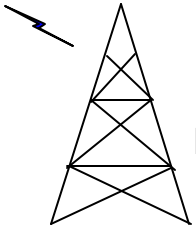


Equipment
Manufacturer

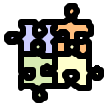


Network
Operator

Reconfiguration
Manager



Access
Network



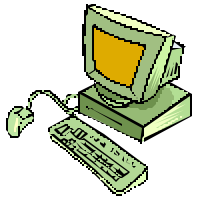
Service
Aggregator

Reconfigurable
Equipment

User/
Subscriber

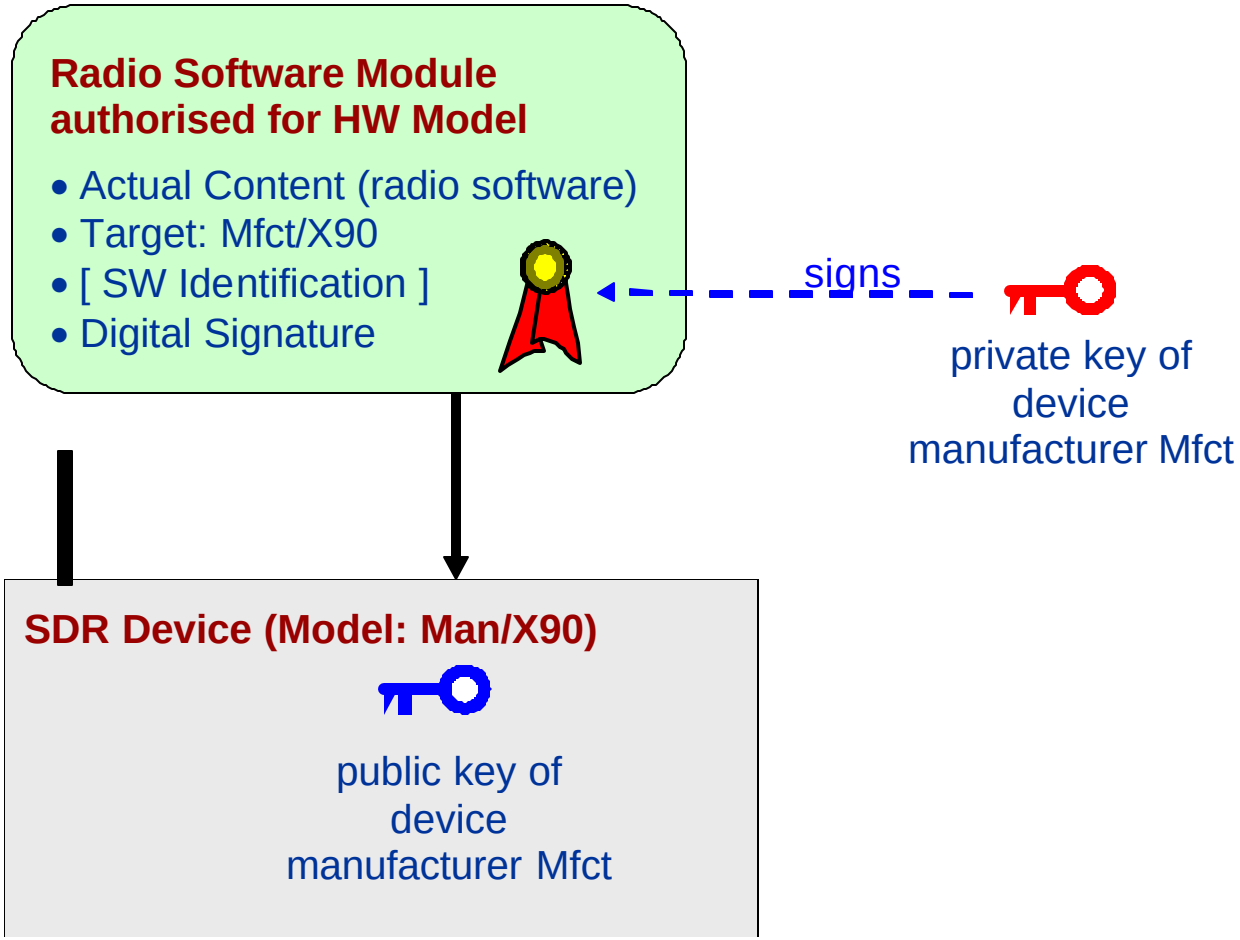
Software
provider

Content
provider

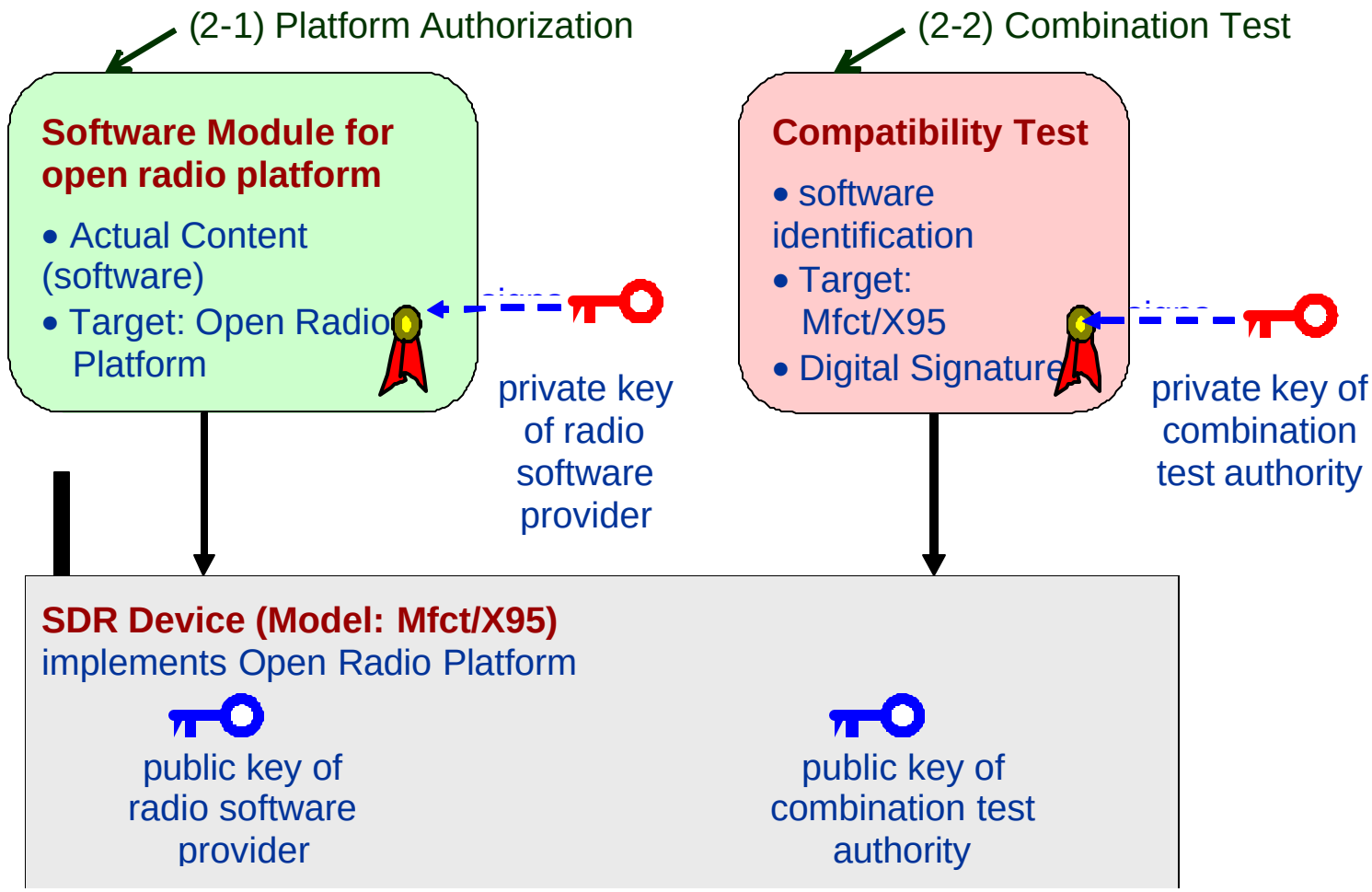


Value Added Service
provider (VASP)

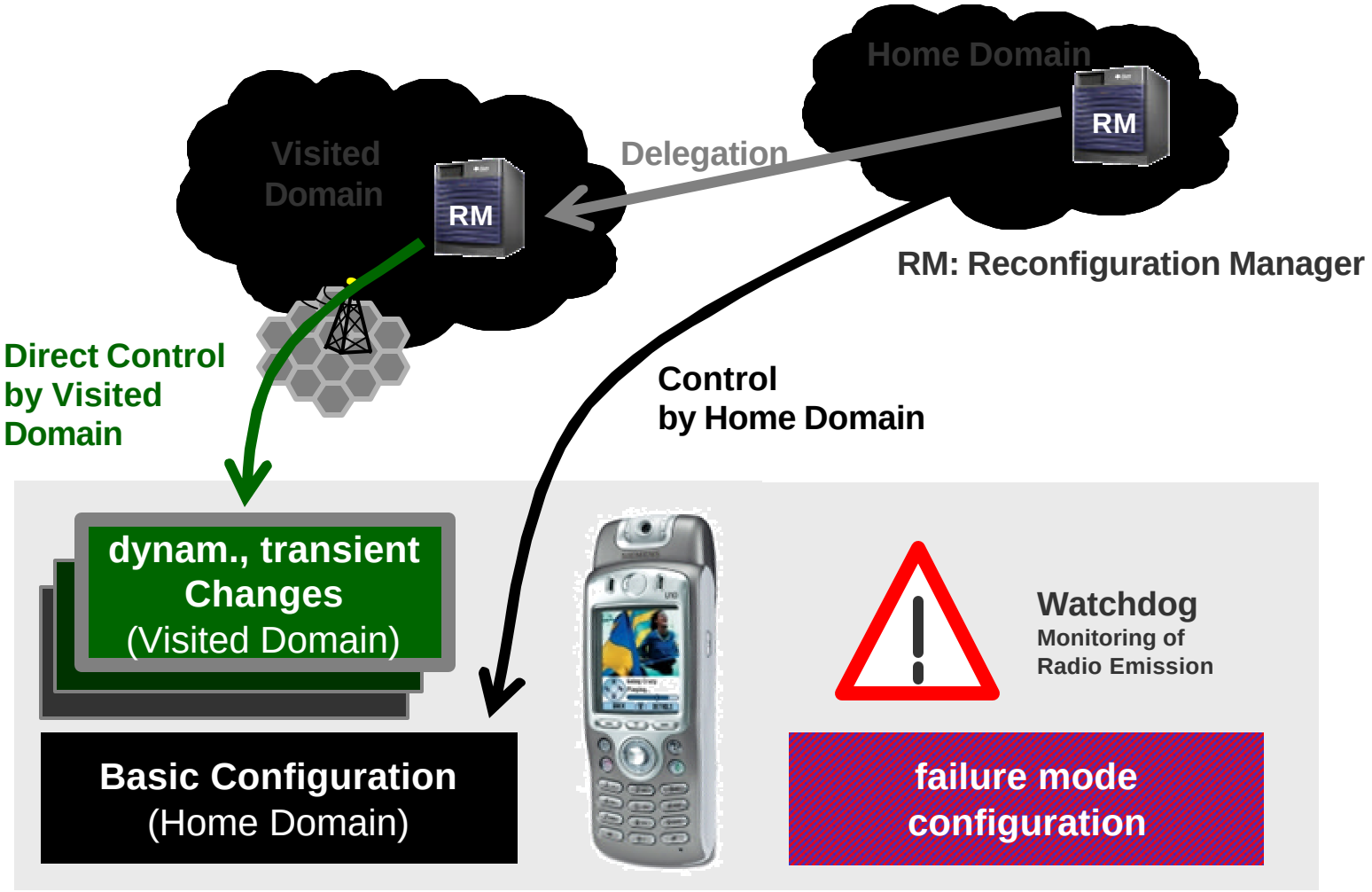
Software Authorisation by Device Manufacturer



Authorisation for Open Radio Platform with Additional Compatibility Test



Decentralize Reconfiguration Control



Security Issues - Support Functions Perspective

- Secure Reconfiguration Process
  - Authorization of Entities Triggering or Performing a Reconfiguration
  - Protected Reconfiguration Signalling
  - Protection of Reconfiguration Support Functions
  - Integrity, Authenticity and Confidentiality of Information Used in the Configuration Process (Preferences, context)
  - Ensure privilege modes of operation
- Reconfiguration Software Download
  - Protection against Malicious or Malfunctioning Reconfiguration Software
  - Secure Storage and Management of Cryptographic Material (e.g. keys, root certificates)
  - Prevent Illegitimate Use of Reconfiguration Software
- Control of Radio Emission (Compliance)

Availability & Integrity

- Availability (of systems and data for intended use only)
  - Availability is a requirement intended to assure that systems work promptly and service is not denied to authorized users. This objective protects against:
    - Intentional or accidental attempts to either:
      - Perform unauthorized deletion of data or
      - Otherwise cause a denial of service or data
      - Attempts to use system or data for unauthorized purposes
- Integrity (of system and data)
  - Integrity has two facets:
    - Data integrity (the property that data has not been altered in an unauthorized manner while in storage, during processing, or while in transit) or
    - System integrity (the quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation