Deployment of Mobile Trusted Modules

Trusted Location Triggers

Andreas U. Schmidt

Together with Nicolai Kuntze, Michael Kasper, and Jörg Abendroth (Nokia Siemens Networks)

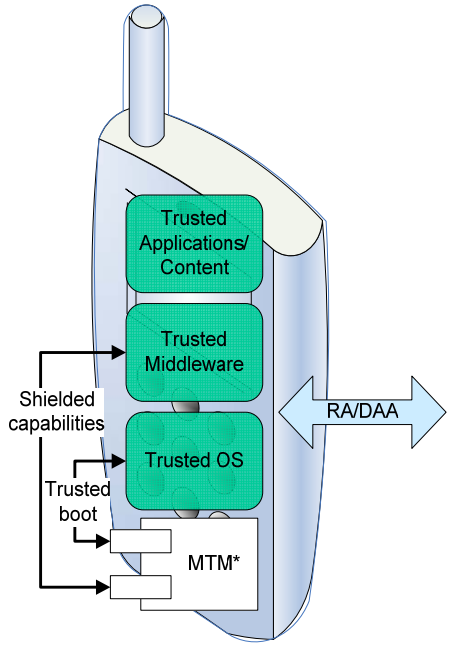
Fraunhofer Institute for Secure Information Technology SIT, Darmstadt, Germany

Part I

On the deployment of Mobile Trusted Modules

TCG MPWG

- **Mobile Phone Work Group (TCG MPWG)**
  - Subgroup of the TCG
  - Specifies the TCG MPWG Reference Architecture and TCG MPWG Specification
  - Members: Nokia Corp., Wave Systems, Infineon,Gemalto, Samsung Electronics Co., France Telecom SA or Ericsson, HP Labs, Nokia Siemens Networks, …
- Document History
  - MPWG Use cases – 09/2005
  - MPWG Requirements – 03/2006 (internal doc)
  - MPWG Reference Architecture – 06/2007
  - MTM Specification – 06/2007
  - … Use case Analysis



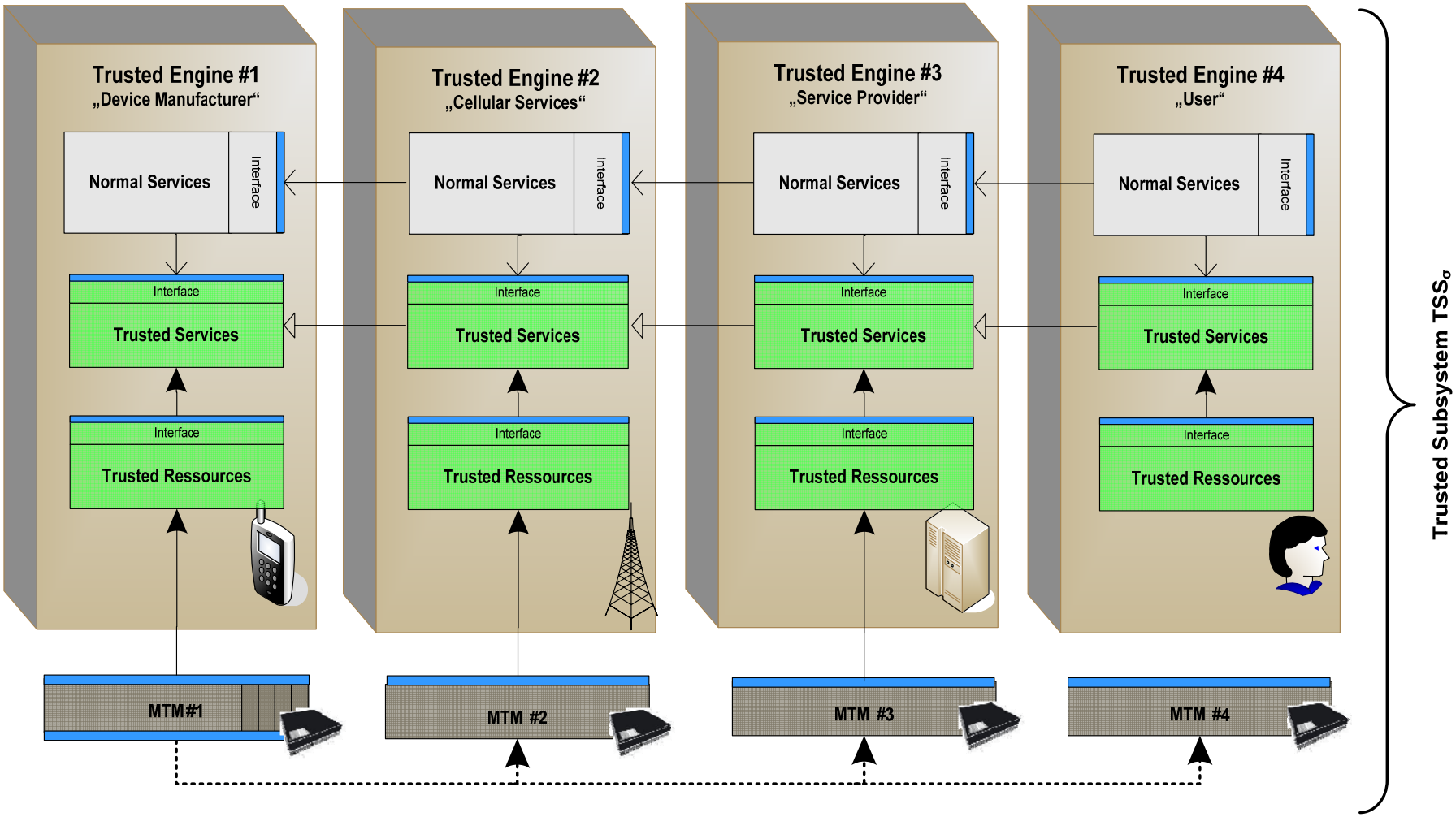
Specification Backgrounds

- Baseline was TCG TPM v1.2 specifications
  - Optimized for PC platform
- Standard HW, Standard Boot Cycle (BIOS, EFI), Standard OS
  - Rich feature set
- Basically unlimited by size/power constraints
- TCG MPWG set out with two tasks
  - Enable implementation in a mobile phone
  - Enable implementation of published use cases
- Enabling implementation in mobile phones
  - Heterogenous hardware and OS environment
  - Proprietary boot cycle
  - Suitable for implementation inside a SoC
  - Enable implementation as SW in a separate trusted on-chip execution environment
- Enable implementation of published use cases
  - Local Verification
  - e.g. Platform Integrity, IMEI protection

MPWG Platform Highlights

- Introduces RTV as a root verification agent under the control of a secured Root Verification Authority identity
- Controlled mutability PKI public key RVAI
- Elaborates
  - An abstract architecture for platform/device description
  - A verified and controlled transitive trust verified boot mechanism
  - A reference integrity framework to validate platform integrity
- Reference Integrity Metrics - RIMs
  - An authentication mechanism to assure the validity of all integrity control information
- RIM Certificates
  - An authorisation mechanism to validate the authority of all authorisers traceable to two kinds of Mobile Trusted Modules
    - MRTM – Mobile Remote Owner TM
      - For remotely configured security policy
      - Allows for local verification
    - MLTM – Mobile Local Owner TM
      - For locally configured security policy

Trusted Mobile Platforms



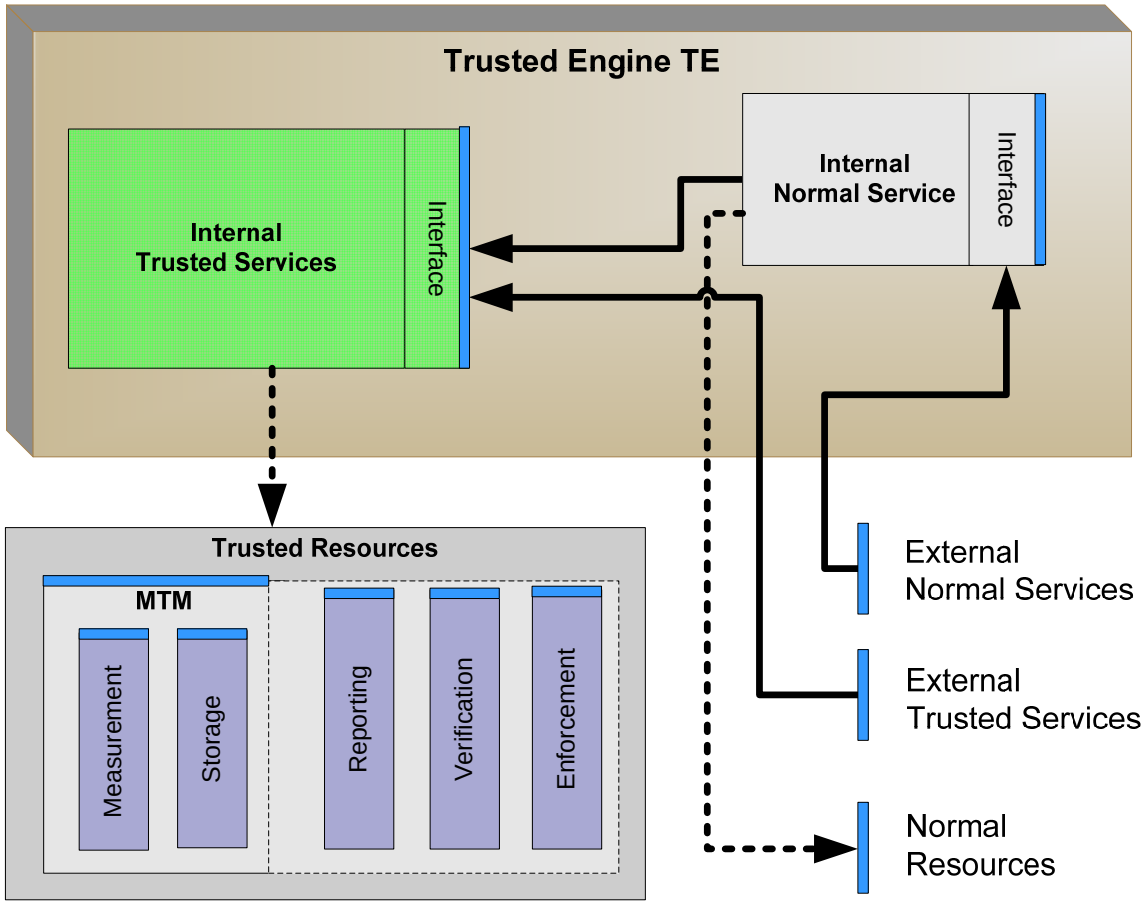
Trusted Subsystems

- A subsystem with designated TBB, acting on behalf of a single stakeholder
- Consists of
  - Trusted Engines (TE)
  - Trusted Services (TS)
  - Trusted Resources (TR)
  - Measured Services
  - Normal Services
  - Normal Resources
  - Security Policies (SP) [foundation for trust]
  - System Configurations (SC)
- Supported by one or more dedicated MTM / vMTM's
- Principal entities (MPWG spec):
  - local stakeholders Device Owner (DO) and User (U); and the
  - remote stakeholders Device Manufacturer (DM), and more general Remote Owners (RO) (e.g. Communication Carrier, Service Provider).

Trusted engines

The TCG MPWG abstracts a trusted mobile platform as a set of tamper-resistant trusted engines.

Each Trusted Engine is able to
- implement arbitrary software functionalities as trusted and/or normal services provide evidence for its trustworthiness, and report its current state,
- access a set of trusted resources, and
- import and/or export services, shielded capabilities and protected functionality.



Trusted engines functionality

Minimal capabilities

- implement arbitrary software functionalities as trusted and/or normal services,
- provide the evidence for its trustworthiness,
- report the evidence of its current state,
- obtaining and using Endorsement Keys (EK) and/or Attestation Identity Keys (AIK),
- access a set of trusted resources, and
- import and/or export services, shielded capabilities and protected functionality.

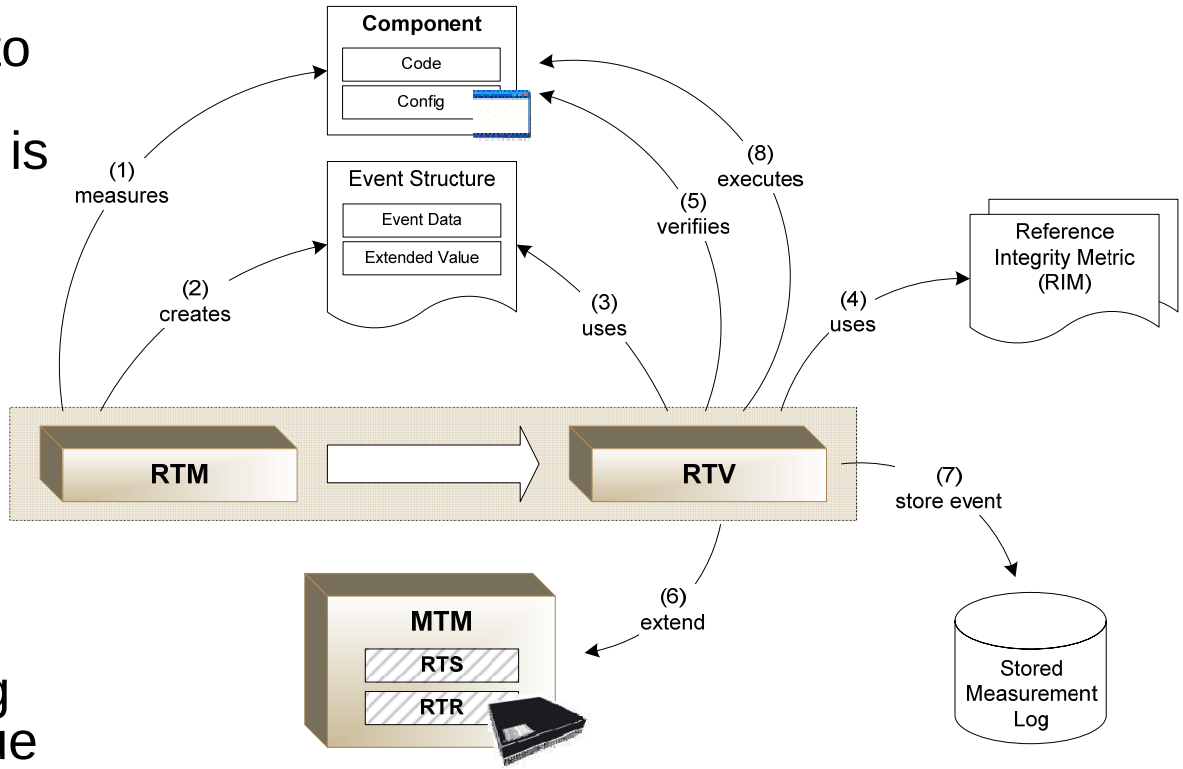
RoTs as Trusted Resources

- The TCG MPWG defines Roots-of-Trust (RoT) as Trusted Resources
  - Root-of-Trust-for-Reporting (RTR)
  - Root-of-Trust-for-Storage (RTS)
  - Root-of-Trust-for-Measurement (RTM)
  - Root-of-Trust-for-Verification (RTV)
  - Root-of-Trust-for-Enforcement (RTE)

- Typically, a Mobile Trusted Module (MTM) consists of a RTR & RTS (with a subset of TPM v1.2 functionality plus a set of new Mobile-specific commands)
- Each RoT vouches its trustworthiness either directly by supplied secrets (EK, AIK) and associated credentials, which are only accessible by authenticated subjects of the stakeholder, or indirectly by measurements of other trusted resources.

Local verification

- **Local verification Process**
  In the mobile domain, to avoid communication costs, this functionality is extended by a local verifier, which checks the measurements against a given Reference Integrity Metrics (RIM).
- Device-side verifier offers assertions to the integrity values.
- verifier receives the log and a signed PCR value as well as the certicates to verify the signature



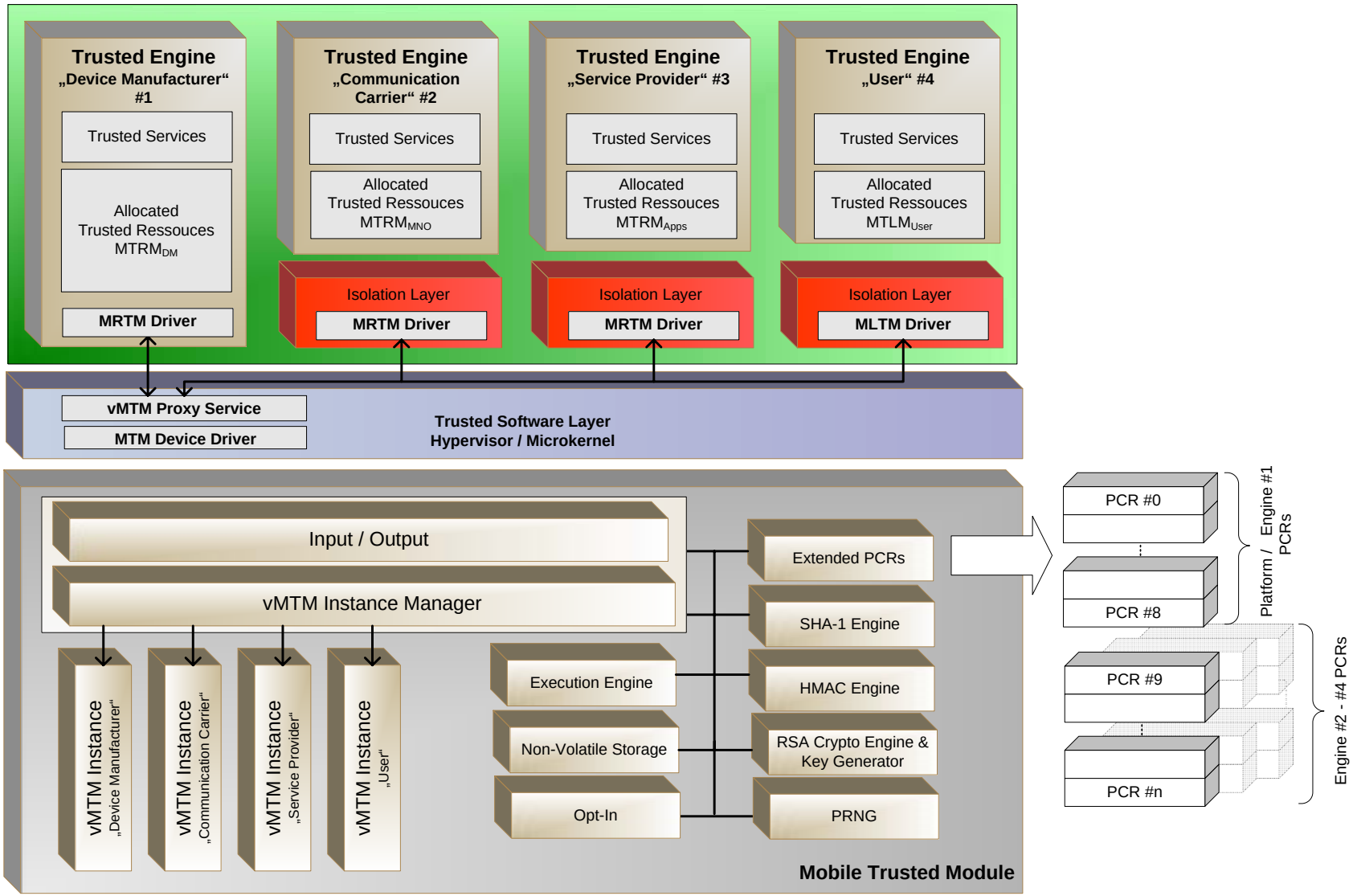
Architecture variants for MTM & TSSys

- Standard TPM based
  - uses a non-modied standard TPM to build the TCB of this system.
  - The secret keys are stored into a single key-hierarchy on behalf of *DO*
  - an adversary or malicious local owner may be able to access the secret keys of a remote stakeholder and take control of a remote owner compartment
  - The user can disable the MTM or corrupt engines of remote stakeholders
- Software-based MTM-Emulation Model
  - Software-based allocated *MTM*-emulation with an isolated key-hierarchy per vMTM instance
  - Security critical data, e.g. *EK* or *SRK*, are only protected by software mechanisms outside the tamper-resistant env.
  - Advantage high performance – good for simulation and testing
- Generic MTM-based Model supporting multiple Stakeholders and virtual MTMs

Multiple-stakeholder model

- Adaption of secure coprocessor architecture for virtual TPMs proposed in [7]
- Single genuine hardware MTM and several virtual software MTMs
- One MTM for each trusted engine
- A Trusted Software Layer oers a vMTM Proxy Service to all embedded trusted engines *TE*
  - routes MTM commands from a *TE* to its dedicated instance *vMTM*
- Requires some additional functionality to separate vMTM instances

Multiple stakeholders in virtual TEs



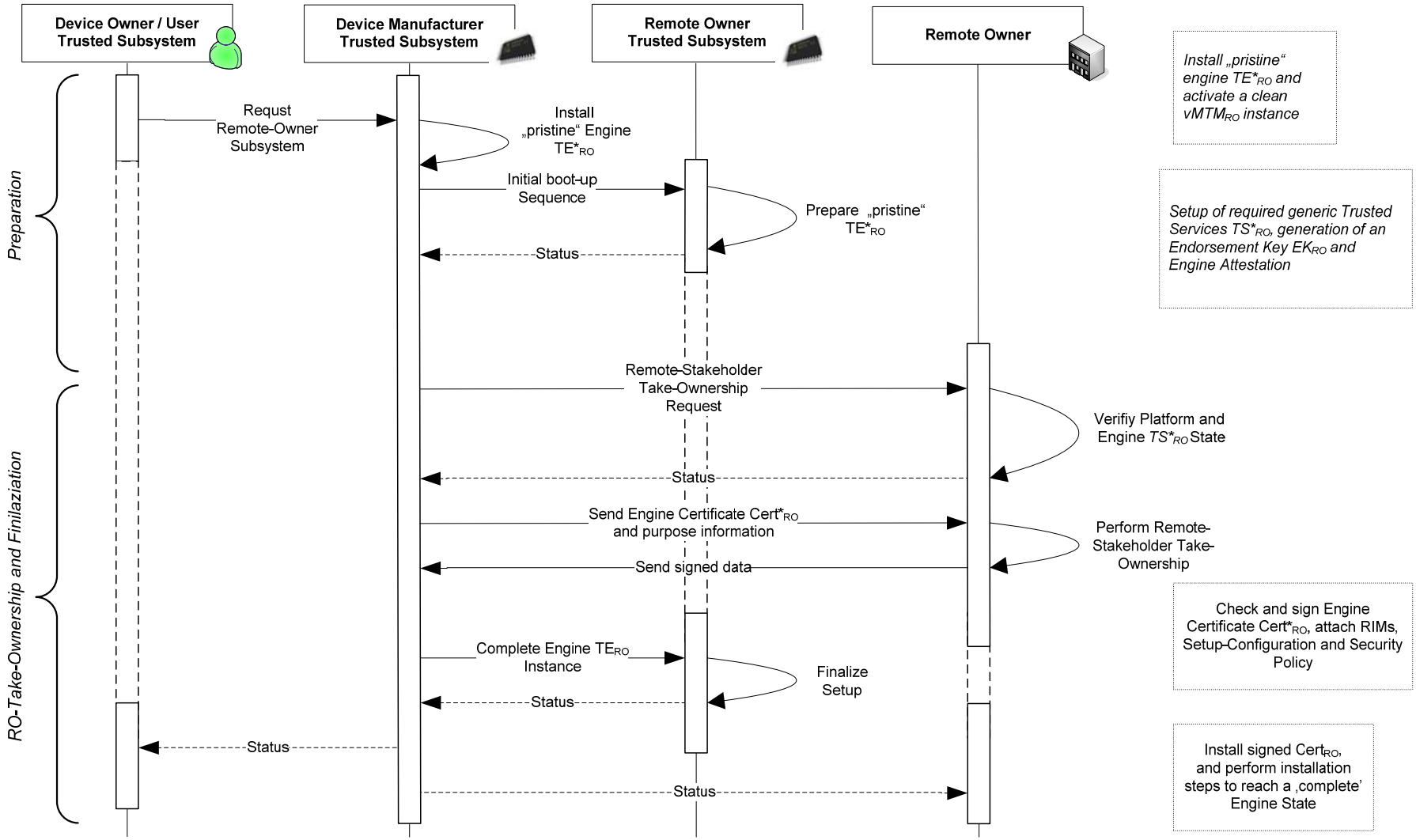
Remote owner take ownership

- Unspecified in MPWG reference architecture
- Minimal requirements
  - the remote owner MUST be protected from a User attempting to remove the remote owners ownership of the engine, or attempting to disable or de-activate the engine's MRTM
  - (eninge might be removed entirely, however, if on a DO-conrolled list in the discretionary domain)
  - remotely owned engine MUST therefore support secure boot, to ensure that the engine loads the way the remote owner is expecting.
- a general model is that the engine's MRTM is already enabled and activated, and already has an owner set when the User takes possession of the device.
  - This MUST be true of the Device Manufacturer's Engine, for example.
  - However, a remote owner MAY be able to take ownership at a later date if not already set

Remote take ownership proposal

- Idea
  - install and instantiate a ’blank’ trusted subsystem containing
    - a pristine engine
    - a set of generic trusted services (such as a trusted boot agent)
  - Certify it by the remote owner on condition that
    - the platform is able to provide evidence of the TSS’ pristine configuration and policy conformance with respect to the RO’s policy

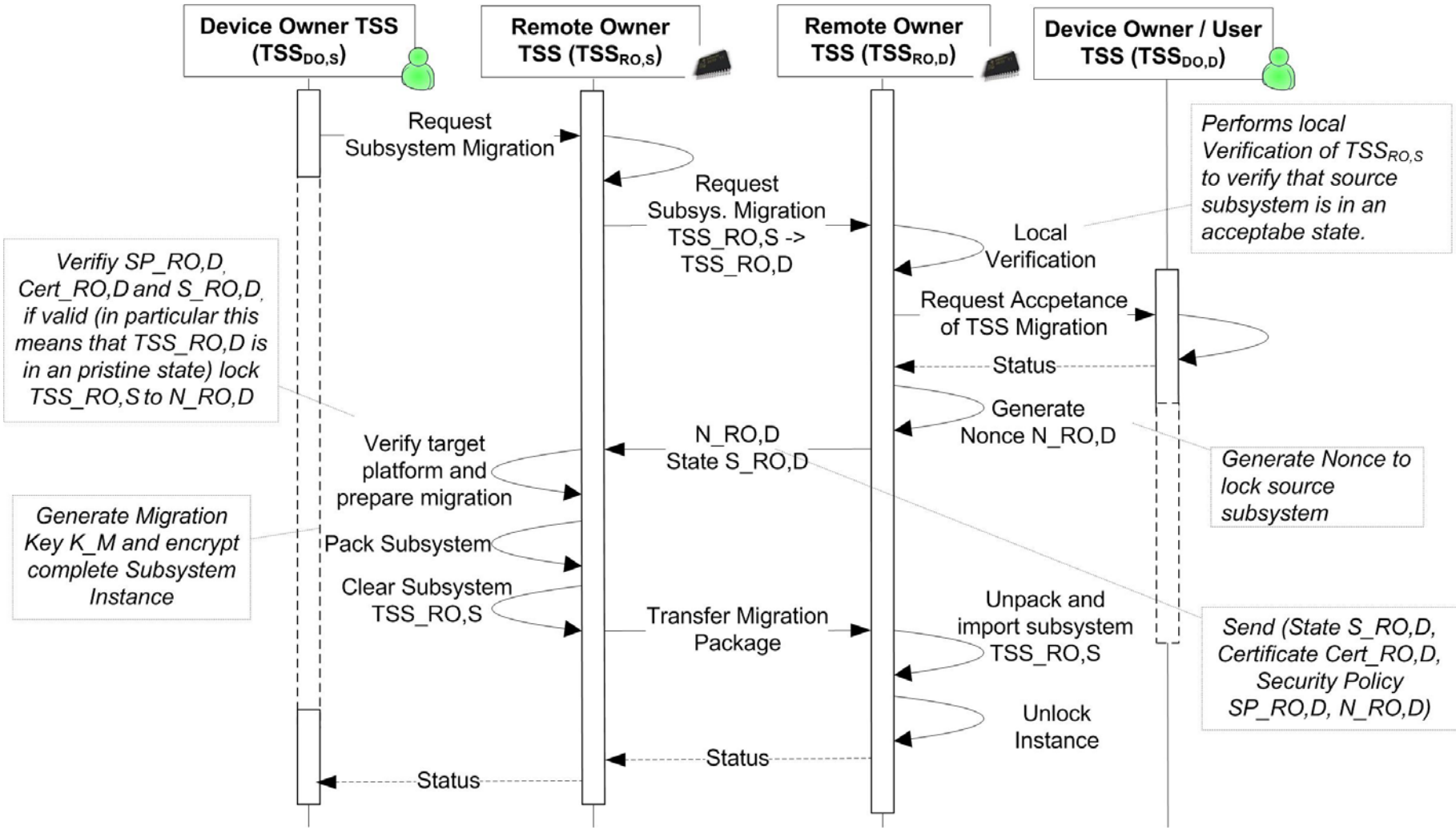
Remote take ownership protocol (proposed)



Remote take ownership protocol (proposed)

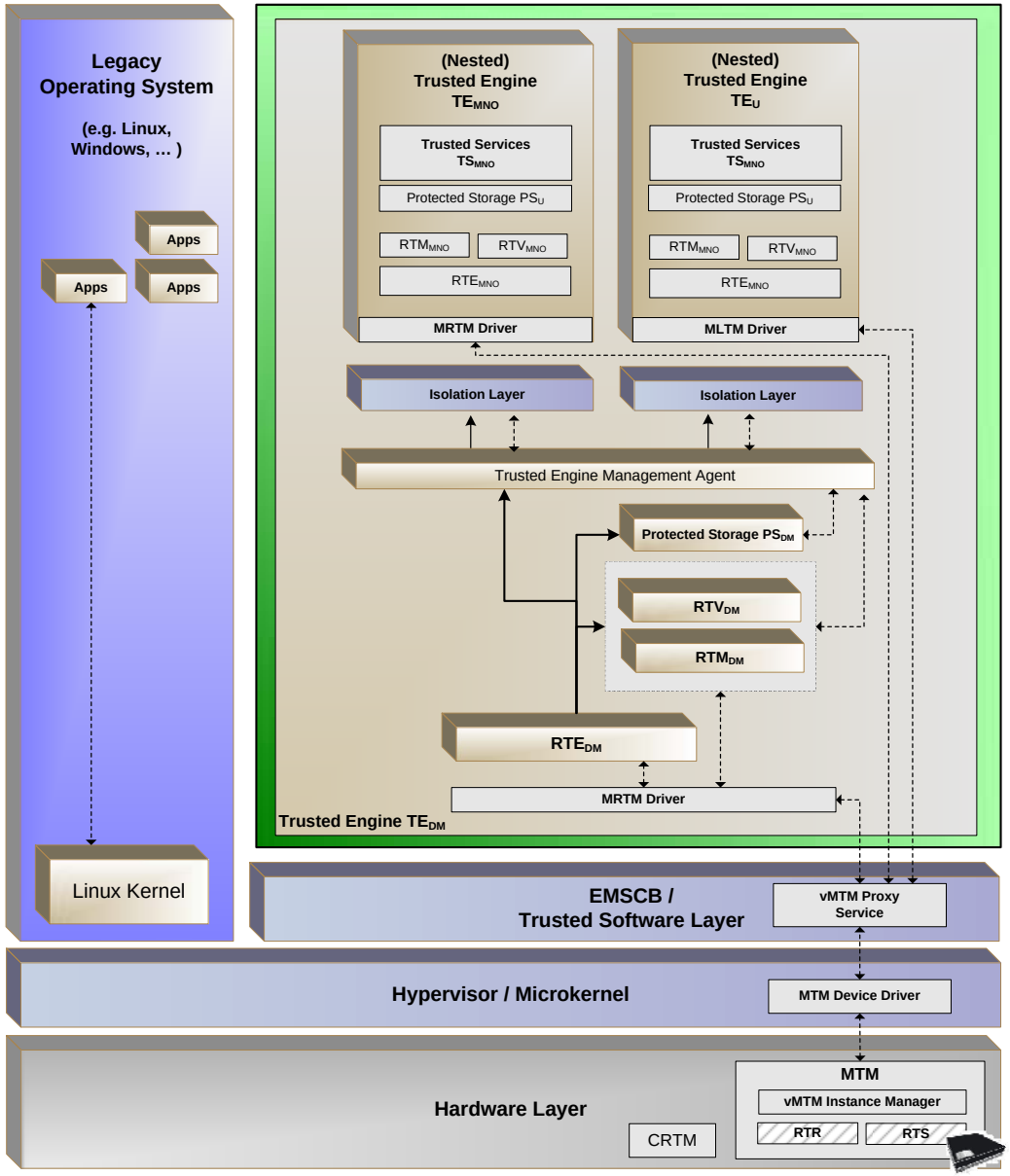
- Precondition: DM engine started in trusted boot, containing ability to install pristine engine
- Protocol:
- Platform preparation
  - Install pristine engine e.g. from dedicated ROM
  - Booted under control of RTE_DM
  - Instantiate vMTM_RO in this engine
  - Create EK pair locally in this engine, and according certificate
  - Local or remote attestation of the pristine engine
  - Using RIM Cert of RO
- Take ownership execution
  - Platform requests RO take ownership by sending generated EK, certificate, and attestation data – *encrypted channel!*
  - RO checks attestation data and validity of intended purpose of the engine on that particular platform
  - Signs the engine‘s certificate
  - Creates RIM certificates for local verification
  - Sends it to the platform, encrypted with EKpub_RO to TSS_DM
  - TSS_DM triggers completion of TSS_RO instance, i.e.
    - Installation of signed EK certificate
    - Installation of RIM certificates
  - Completion is confirmed to RO

Migration of a TSS (proposed)



Prototype

- A prototypical implementation of a Trusted mobile platform based on EMSCB/Turaya
- Work in progress



Part II

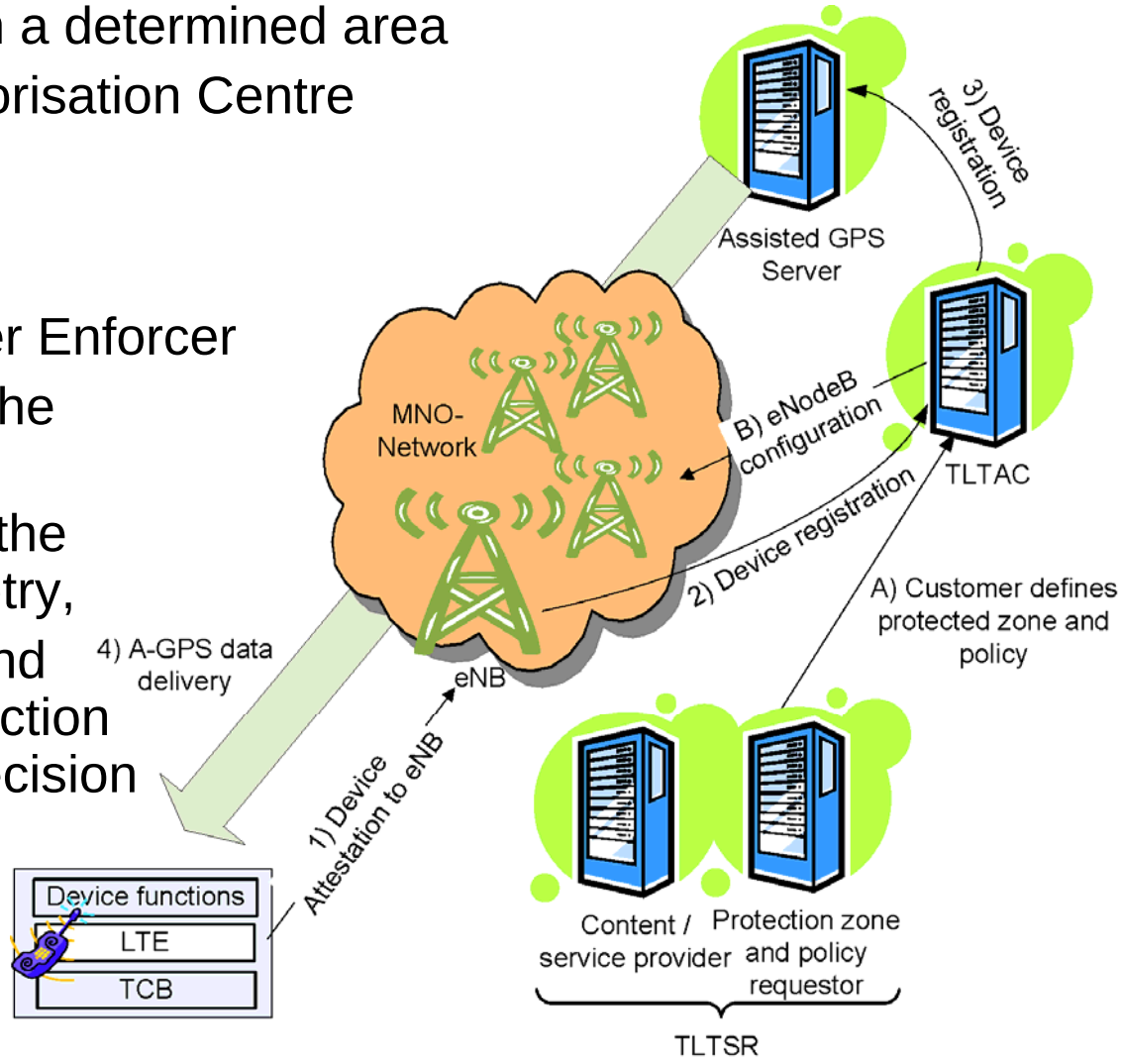
Trust for Location-based Authorisation, or
Trusted Location Triggers

Motivation and main idea

- Various methods for location detemination exist (triangulation, [A]-GPS, round-trip times, hybrids, …
- Some people have looked at LB-authorisation,
- But no device-side enforcement mechanisms exist which scale with security requirements
- Core idea: Tursted Location Trigger Authorisation (TLTA) Architecture, combining
- Net (cell) –based coarse localisation
- Device side enforcement engine supported by Trusted Computing, serving
- Device-side authorisation decisions, and
- Device or hybrid fine-granular location determination

Entities of TLTA in 3GPP SAE Framework

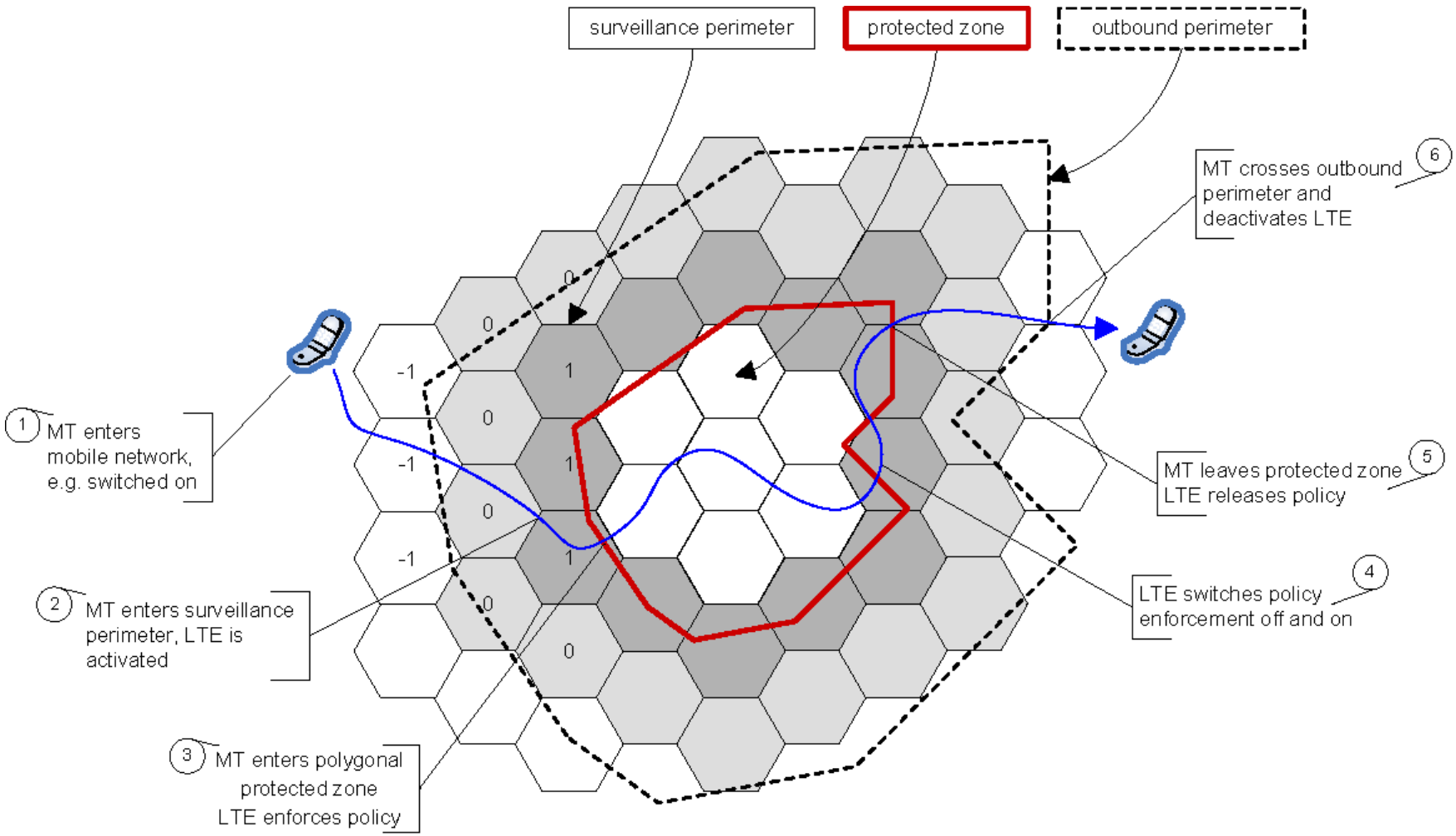
- TLTSR – the Service Requestor of TLTA wants a policy enforced in a determined area
- TLTAC – The TLTA Authorisation Centre establishes protection by configuring certain eNodeBs
- LTE – the Location Trigger Enforcer
  - (i) receives and holds the policies from TLTAC,
  - (ii) receives and holds the protection zone geometry,
  - (iii) determines entry and exit events to the protection zone by some high-precision location mechanism, e.g., A-GPS, and
  - (iv) enforces the policies on the device.



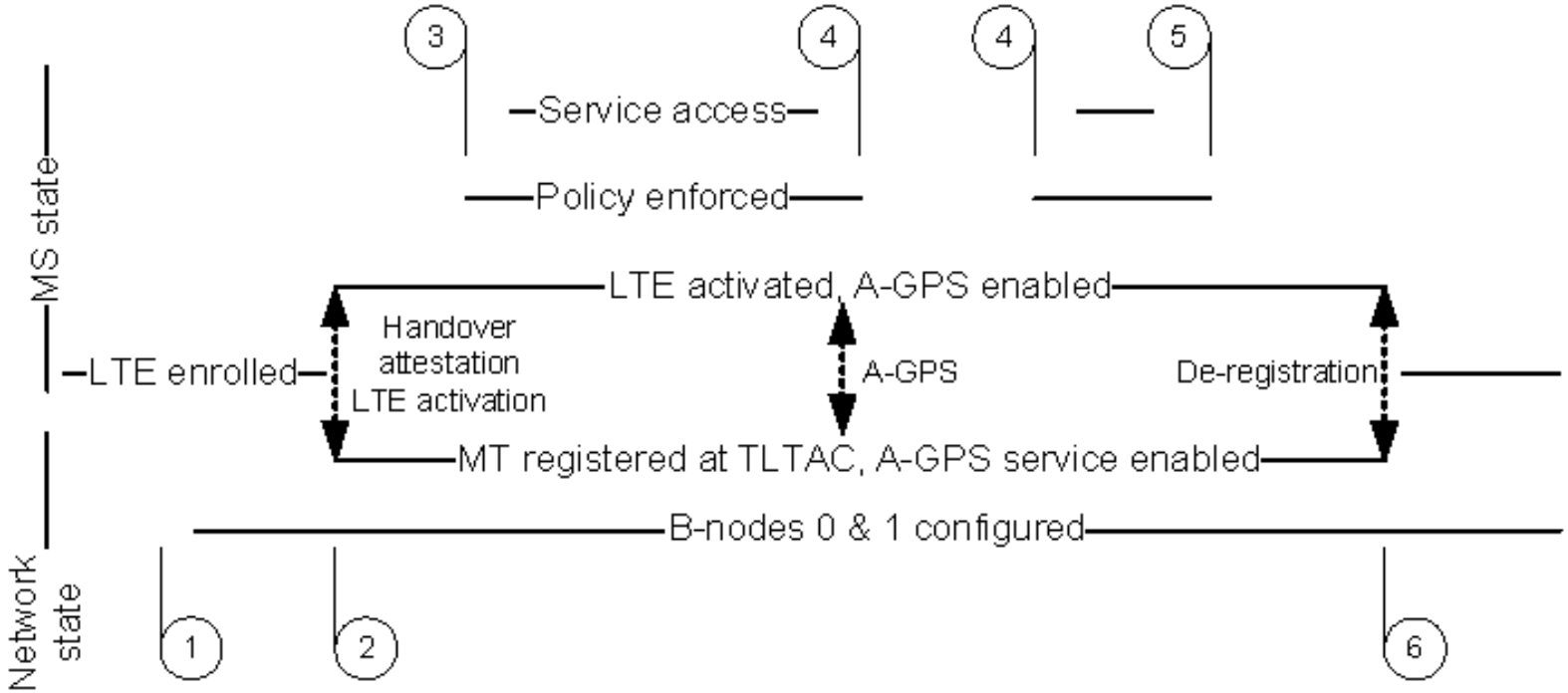
LTE Trust

- LTE rests on a Trusted Computing Base, in particular in a Trusted Subsystem
- Its presence and activity on the device is ensured by secure boot
- And can be verified by an outside entity – here the TLTAC and/or the pre-configured eNodeBs by *remote attestation*

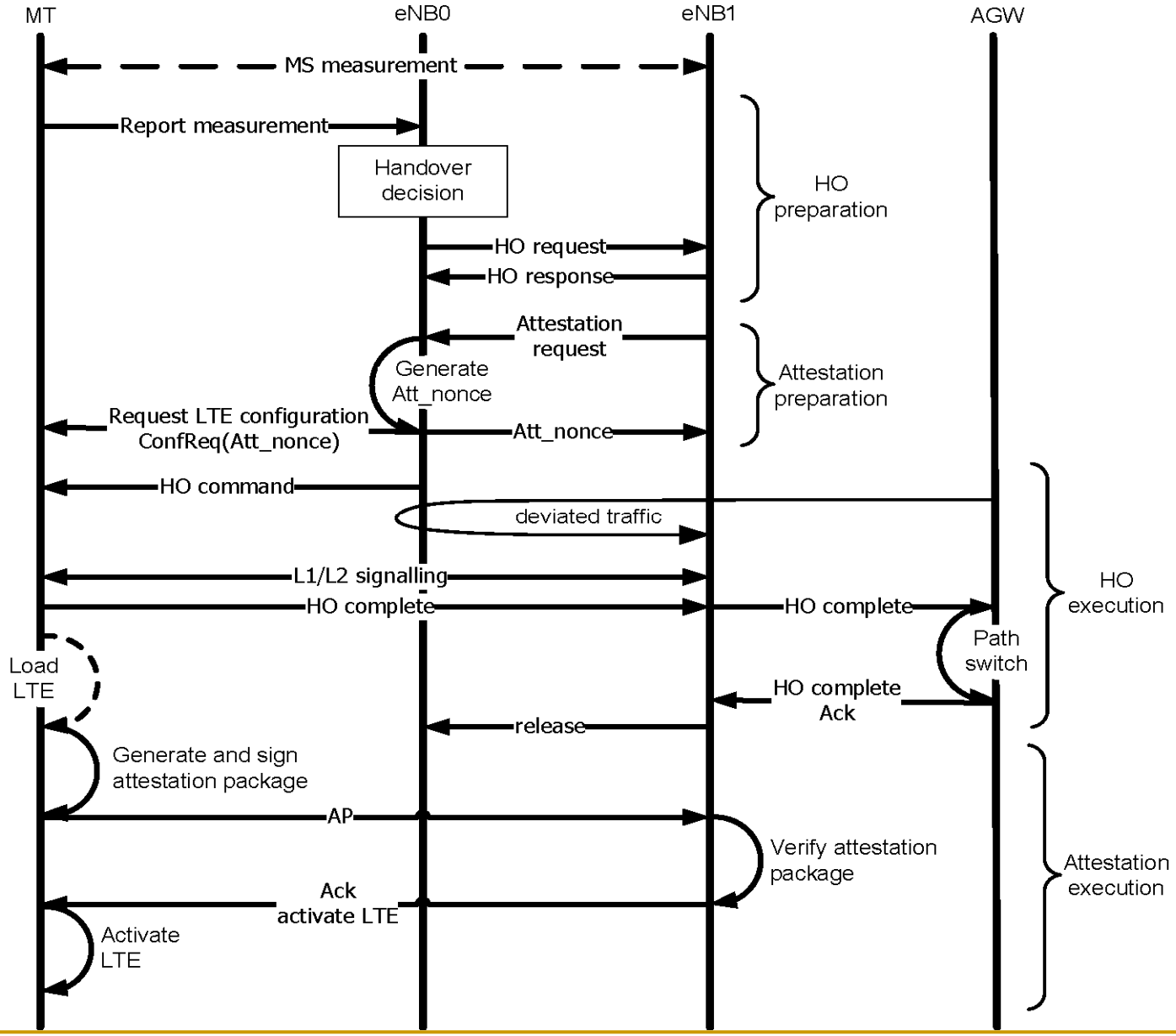
Mobile station travelling through TLTA-protected area



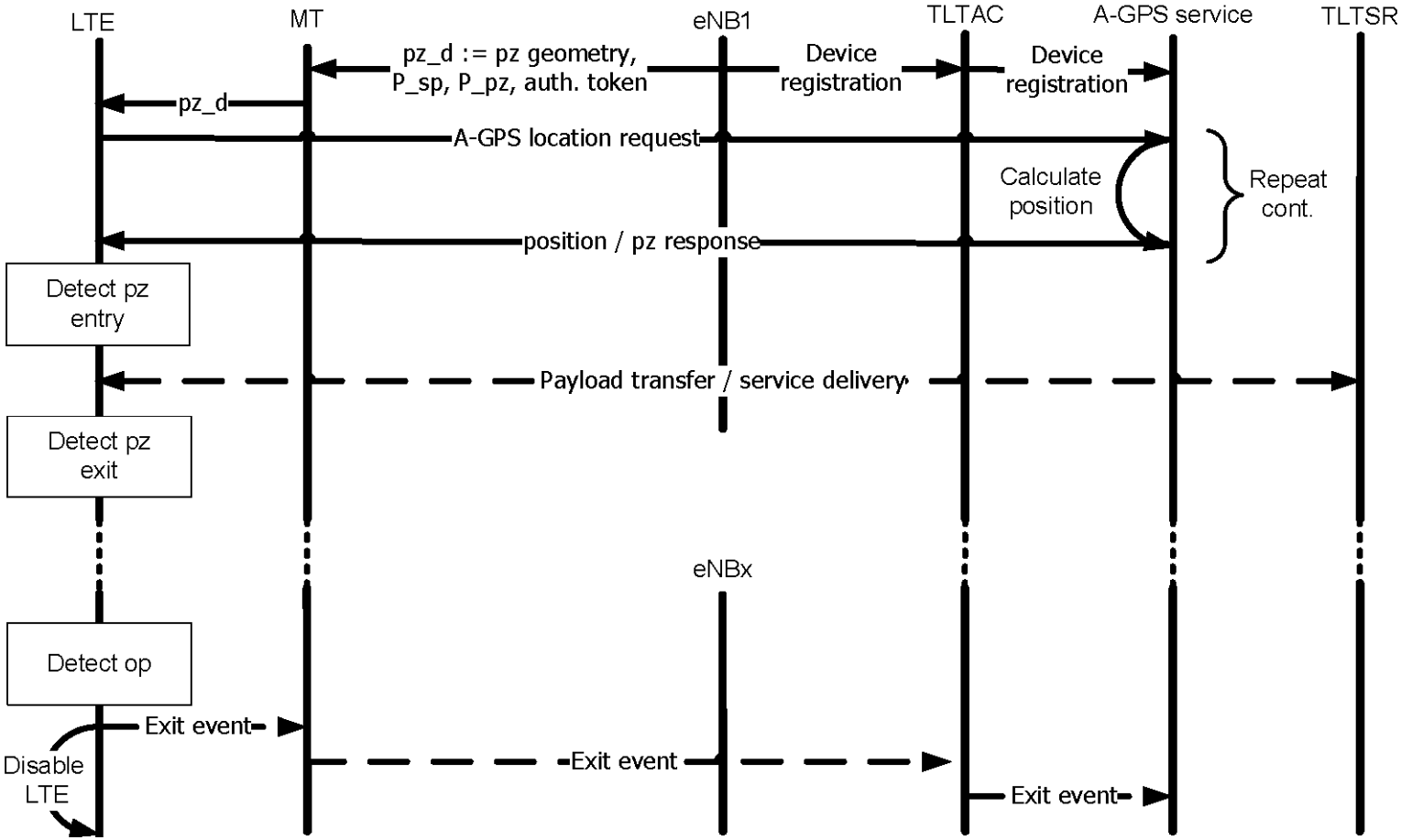
Network and device states during travel



Modified Handover at the surveillance perimeter



LTE Operations and Release



Security and Efficiency Considerations

Security

- Differs for
  - Functional enforcement
    - Functions on ***all*** devices in pz must be enforced
    - Needs out-of-band processes (gate controls) for untrusted devices
    - Susceptible to attacks to subvert pz (e.g., directional antennas to prevent perimeter handover)
  - Access Control
    - Service or data only to registered (with TLTAC) devices
- Generally: While LTE is protected by MTM (hardware), handled data in transit is susceptible to side-channel attacks or direct memory eavesdropping

Efficiency

- TLTA is designed to distribute workload to devices
- Choice of geometry

Application Scenarios

- **High-tech trade fair**: Functional restriction policies can be enforced with exemptions. Consider a high-tech trade fair. pz is determined by the fair's host so as to coincide with the physical entry barriers of the fair area. sp is a larger area so that visitors with TLTAC-enabled MTs will already be registered with TLTAC when passing the entry control. Ppz stipulates that cameras and sound recording facilities of devices are to be switched off by LTE. They then can freely pass through, while unprotected (or non-networked devices, e.g., cameras) are detected at the entry barrier and are confiscated. **Countering industrial espionage** is another use case. A company may use TLTA to disable MT cameras within the borders of their campus, while keeping the MTs of visiting executives operative for communication purposes.
- **Sports stadium and concert hall**: The voice commentary on a sports event is broadcast encrypted to mobile devices in a stadium, which is the pz. Only TLTA-enabled devices receive the decryption keys with the Ppz data managed securely by LTE. The TLTSR and service provider can simply broadcast the content and has no need to operate own access control facilities. In a concert hall, the live audio broadcast should add to the experience of the audience, and can be personalised in terms of language and otherwise. Not received outside of the concert hall, to avoid bootlegging.
- **Mission critical communication**: MTs in a disaster area can be configured to receive emergency and alarming messages. This can be used to inform the public or emergency action forces but also to locate them within the danger zone. Standard mobile devices can co-operate with the special ones of action forces and inter-work over network boundaries, e.g., with TETRA networks.
- **Mobile gaming:** A game spread out over the area of a city requires to adjust the device side policies based on narrow location, e.g., when the user has reached a certain waypoint. These scenarios have in common that they could in principle also be realised by authorisation not based on location, e.g., organisational processes, yet with varying methods to reach the desired enforcement level. The benefit of TLTA is a unified authorisation method scaling with security requirements.