
(Mobile) Applications of Trusted Identities

by Andreas U. Schmidt

Fraunhofer SIT, Darmstadt

Darmstadt, 20th September 2006



Fraunhofer Institut
Sichere Informations-
Technologie

Why is the mobile domain particularly interesting for advanced IDM and TC?

The future role of MNOs

From a recent study of KPMG Germany*:

„Throwing subsidised handsets on the market is not a sustainable strategy for success. It makes more sense to build a stable and loyal customer base with attractive and convergent services“

MNOs are **privileged players** as they already have a **stable and huge customer base**

MNOs are advised to consider new business models from the **Web 2.0 environment**

It is necessary to explain the new convergent services to the customer

Opportunities:

Mobile entertainment; **mobile network games** are enabled by 3G and convergent technologies;

Live TV and Video downloads are attractive **to commit customers to a service provider**

A majority of customers wishes a **single service provider**

for accessing the various services and coordinating charging and payment, making the various service providers transparent with respect to the user recognition

Accounting and charging competence is going to be a key ability

And we may add: Trust and IDM are crucial

Why is the mobile domain particularly interesting for advanced IDM TC?

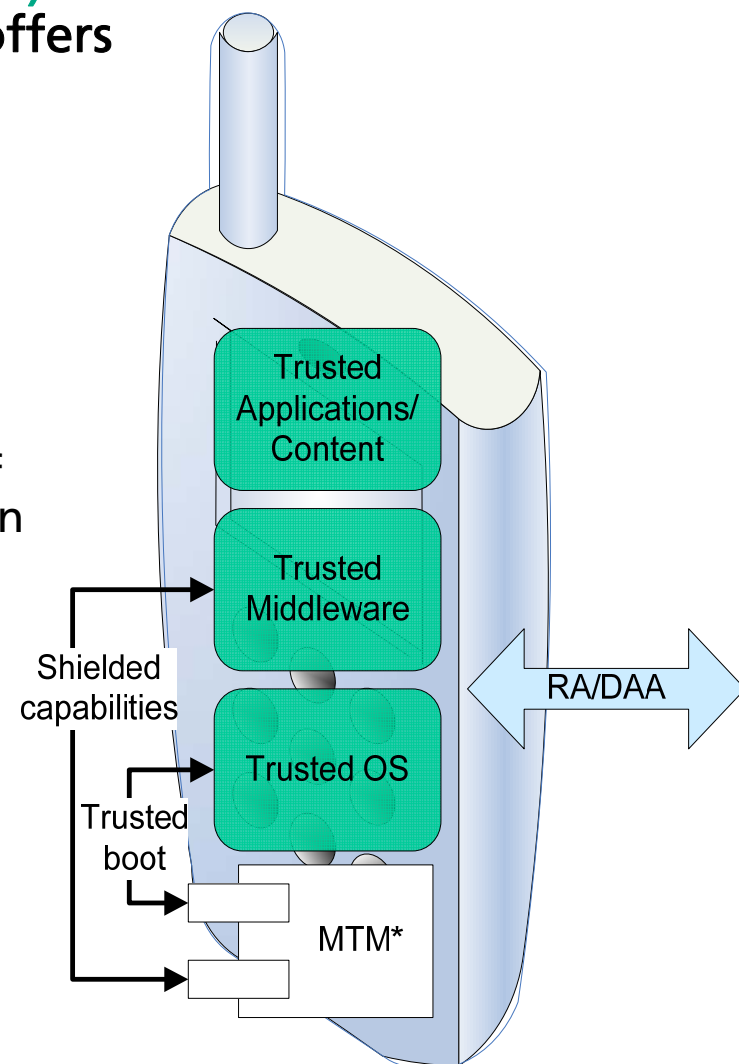
Convergent, trusted devices as a base for novel services

- **Mobile access to applications & content is becoming network-agnostic**
 - Customers attracted by attractive applications & content
 - Diversity of technologies (2G, 3G, WLAN, WiMAX, MobileIP)
 - Customers interested in optimizing price/performance ratio
- **Mobile devices are becoming very smart, multi-purpose devices**
 - More than voice comm., both consuming and providing applications, data and media
 - Network access is a commodity, customers expect additional features
 - Next step for MNOs (business models): providing customised/customisable services
- **Novel requirements for trust across domains – even technological boundaries**
- **Trusted computing (TC) can become the enabler for service provisioning**
 - Enables network- and device-agnostic trust relations on application-level
 - Uniform trusted platform for service provisioning
- **Credentials from various domains of trust, carried, managed and transmitted by TC-enabled devices can yield trusted, application-level, identities**

Mobile trusted platforms

A system equipped with a **trusted platform module (TPM)** as specified by TCG, is called a **trusted platform (TP)**. It offers **protected capabilities and shielded locations**

- TPM provides (RSA) key management, i.e., methods for generation, storage, and usage of keys
- Trust measurements on the system environment exerted at boot- and run-time allow for trustworthy assertions about the current system state and a re-tracing of how it was reached
- The system state, and a measurement log (order matters) of how it was reached is securely stored in platform configuration registers (PCR) tamper-resistently located inside the TPM.
- Memory curtaining, sealed storage, and secure I/O are enabled by pertinent TPM base functions.
- Trustworthy system and application software can build on this to establish authenticated communication with the exterior and transmit data protecting integrity and confidentiality.
- **The timeline:** Stable Spec for the Mobile Trusted Module (MTM) is out! MTM-equipped devices will be available within 12 to 18 months



*mobile TPM profile, currently under spec by the pertinent TCG WG

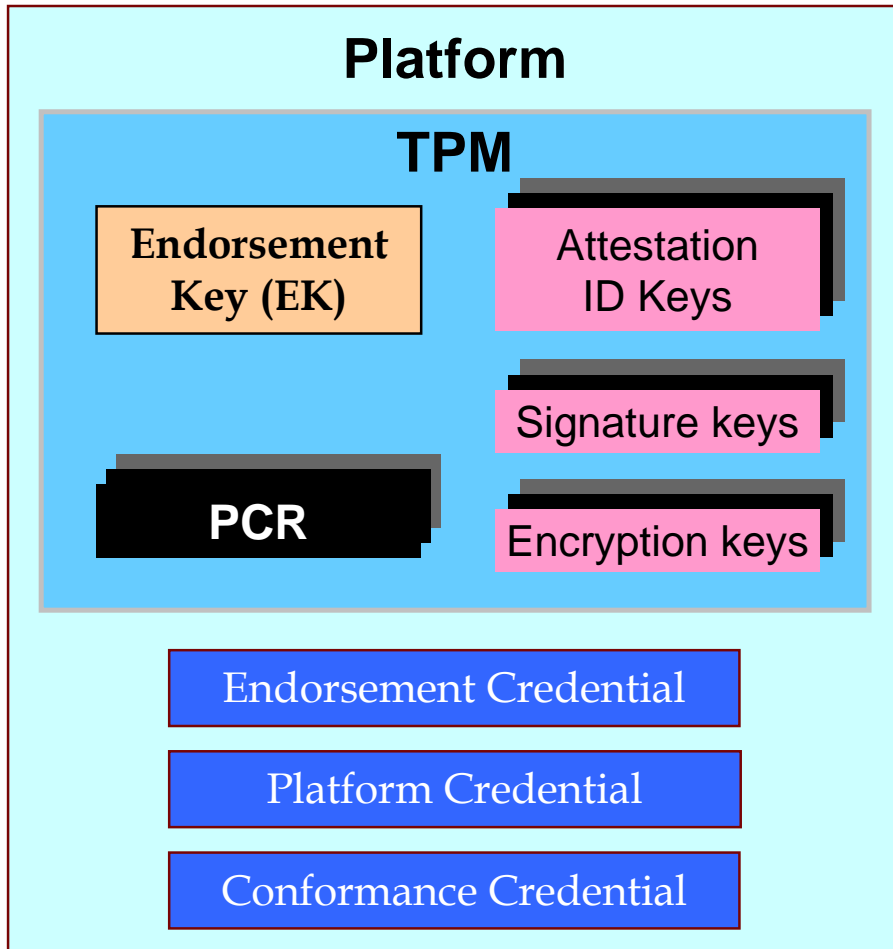
Terminology

- Trust
 - An entity can be trusted if it always behaves in the expected manner for the intended purpose



It does NOT mean that the device as such,
let alone its user,
is trustworthy in unspecified,
or arbitrary contexts

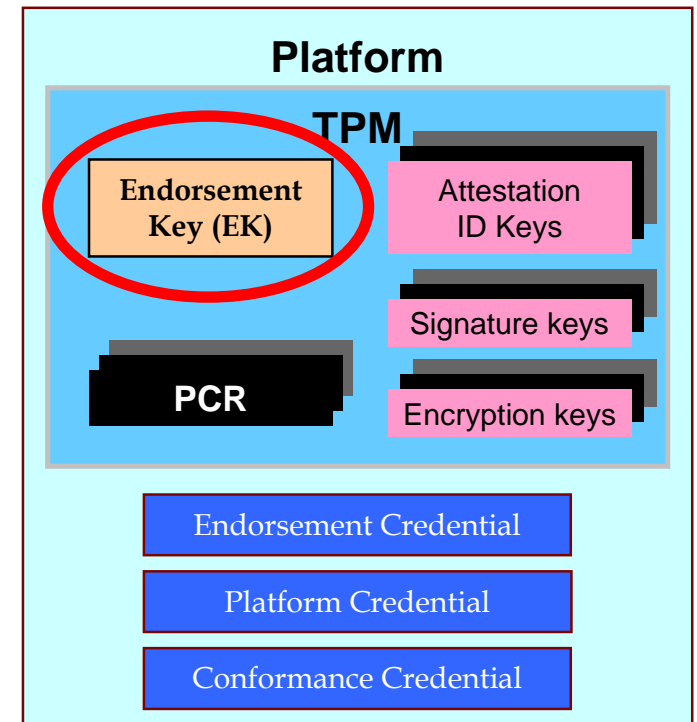
Generic Architecture



- TPM attached to platform
- Credentials held outside TPM
 - Endorsement credential normally provided by TPM manufacturer
 - Platform credential normally provided by platform manufacturer
 - Conformance credential provided by lab
- TPM can load and use a virtually unlimited number of AIK, signature and encryption keys

Endorsement Key (EK) Details

- Each TPM has a unique EK
- The EK is a 2048-bit RSA key
- The EK is generated:
 - When the entity that issues the EK credential has control and is willing to certify the creation of the EK
- There are mechanisms to change the EK
- The EK only participates in two operations
 - Taking TPM ownership
 - Creation of Attestation Identity Keys



Persistent Keys

Platform

TPM

EK

Attestation
ID Keys

SRK

Signature keys

PCR

Encryption keys

Endorsement Credential

Platform Credential

Conformance Credential

- Endorsement Key (EK)
 - Not part of the key hierarchy
- Storage Root Key (SRK)
 - All keys are protected by this key
 - Root of Key Hierarchy
 - Changed on new owner

Key Hierarchy

Protected by the TPM

Storage Root Key (SRK)

Endorsement Key

Protected by the RTS

Migratable Storage Key

Non-Migratable Storage Key

Attestation ID Keys

Migratable Storage Key

Migratable Signing Key

Non-Migratable Storage Key

Non-Migratable Signing Key

Migratable Signing Key

Migratable Signing or Storage Key

Migratable Signing or Storage Key

Key Types and Classes

- **Storage Keys**
 - Protects keys or external data
- **Signing Keys**
 - Digital signatures
- **Attestation Identity Keys (AIKs)**
 - Special Signing keys
 - Provides attestation
- **Non-Migratable Keys**
 - Permanently bound specific TPM, i.e., platform
- **Migratable Keys**
 - Can be migrated to other platforms
- **Certified Migratable Keys**
 - Can be migrated to only “certified” authorities

Remote attestation

The TPM is a hardware (or virtualised) **root of trust** on which the two essential **attestation protocols** rest:

- **Remote attestation (RA)**, yielding, conventional privacy using an ID provider, and
- **Direct anonymous attestation (DAA)**, employing zero-knowledge proofs

RA enables an exterior entity to determine if the requesting agent is altered or not:

- The TP presents the value of a certain PCR *and* the log how this value was created
- This data block is signed using an **Attestation identity key (AIK)**

Privacy: AIKs are generated by the TPM, and certified by a **privacy CA (PCA)** (the TP identifies itself towards the PCA using the **endorsement key [EK]**)

Based on this data two attributes can be attested to the external verifier:

- The data was produced by a genuine TP
by verifying the AIK-signature of the data with the corresponding PCA certificate.
- The integrity, i.e., unalteredness of the TP
by comparing the integrity values of the measurement log.
A compromised system can tamper the log but cannot change the PCR values as these are protected by the TPM.

The verifier has to know a reference value for the reported values in the transmitted measurement log and PCR value

This reference base is rather large and hard to maintain in the PC domain:

There are many
hard- and software versions
admissible boot and runtime parameters
frequent updates

A remedy might be **virtualisation**, implementing small trusted compartments managed by a **hypervisor** and **virtual TPMs** (currently under specification)

The mobile domain is distinct

the number of hardware combinations is rather small
updates of the used software are also rare

RA therefore seems to have higher practical feasibility in the mobile domain

The MTM has special features which are enabling, in particular

A built-in verifier (practically a PCA) allowing for offline attestation

Application scenarios for trusted mobile identities

We deal with authentication and credentials

By transmitting authentication data or exerting authentication protocols, **agents** enter the **domain of trust of a principal**

The authentication process **attests to the trustworthiness** of the agent, i.e., makes implicit or explicit assertions to the principal about the identity of an agent and/or its being in a secure/trustworthy state

the token/data for authentication and the embodied attestation is subsumed under the term **credential**

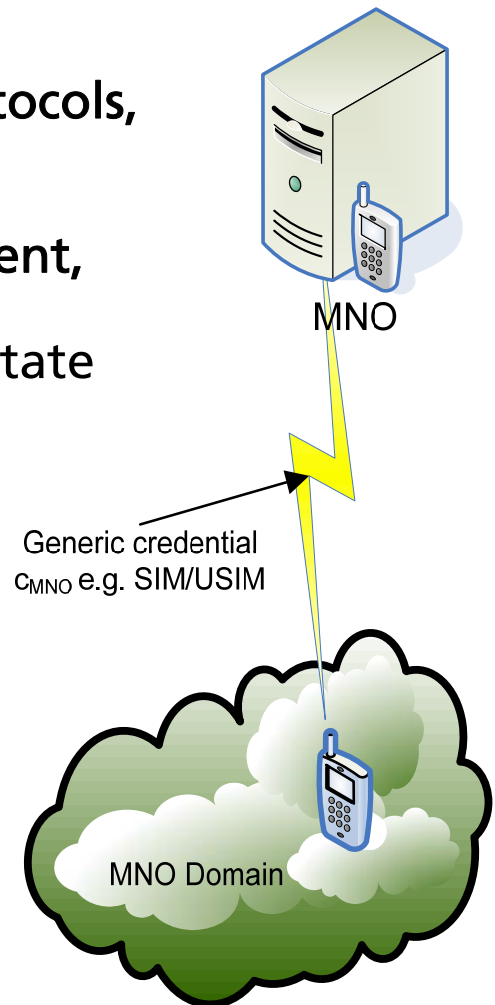
SIM/USIM, cryptographic certificates, shared secrets, PIN/TAN, (smart card-based) biometry, ...

Our aim: Complement **generic domain credentials c** by **trust credentials t** obtained somehow by use of TC, to enable **referral trust** and **transitivity**

Main focus lies in the use or abuse of AIKs, since

they can be generated inside the device in arbitrary amounts

embody a unique identity for it

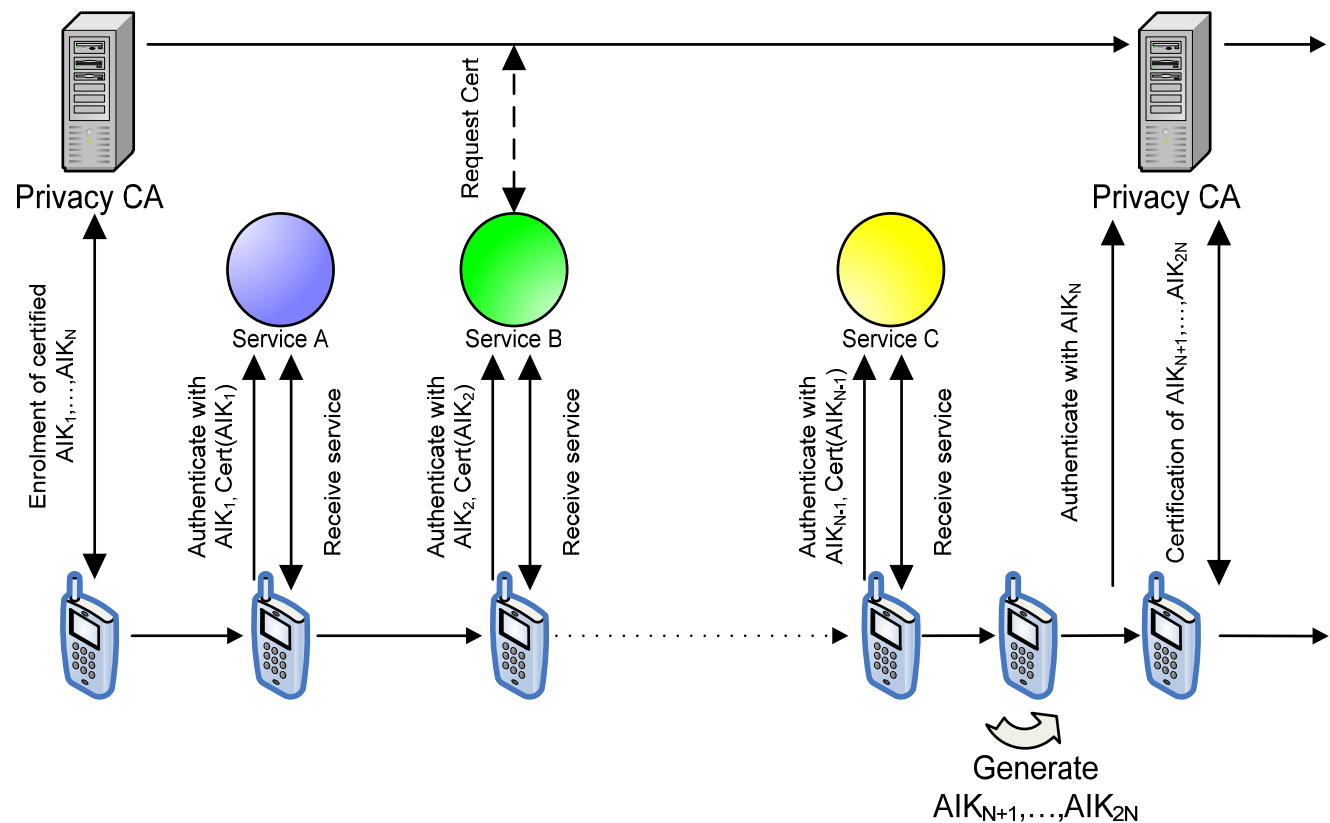


Pseudonymous service access using PCA, RA, AIKs - A bit of privacy

Assume AIKs are used for AA to service access

Then principals can annul the pseudonym and identify users, by 1to1 association of genuine credentials to TPs (SIM)

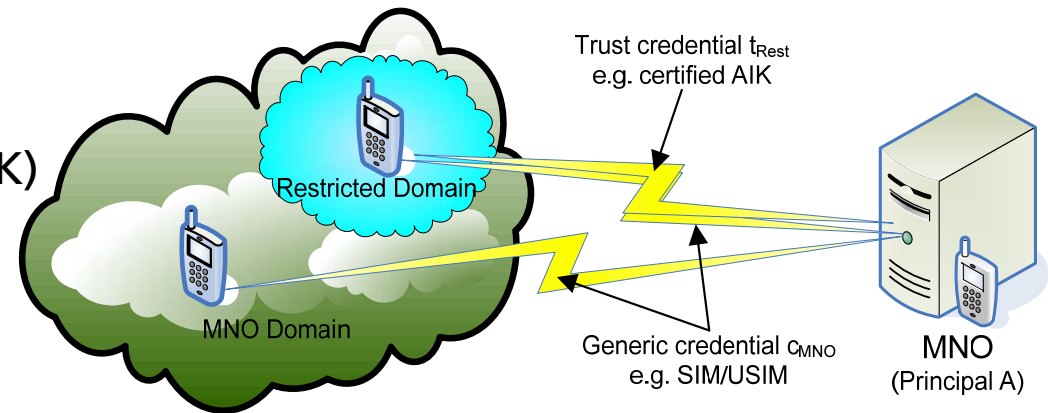
Improvement: Use One-time AIKs (like one-time PIN/TANs or tickets) to prevent accumulation of profiles by principals and/or service providers



- Better: use DAA, created by IBM Zurich (based on idemix), HP, and Intel
- DAA enables to prove the same assertions as RA, without revealing the platform identity at all
- Needs initial enrolment with a trust domain and principal
- DAA is not used yet
- It provides *anonymity rather than pseudonymity* – not applicable in all use cases

Restriction to a sub-identity

Restriction places agents a in a **subgroup $a' < a$** , by dual authentication, with generic credential $c_{a,A}$ and trust credential $t_{a'}$ (e.g. by RA + extra AIK)



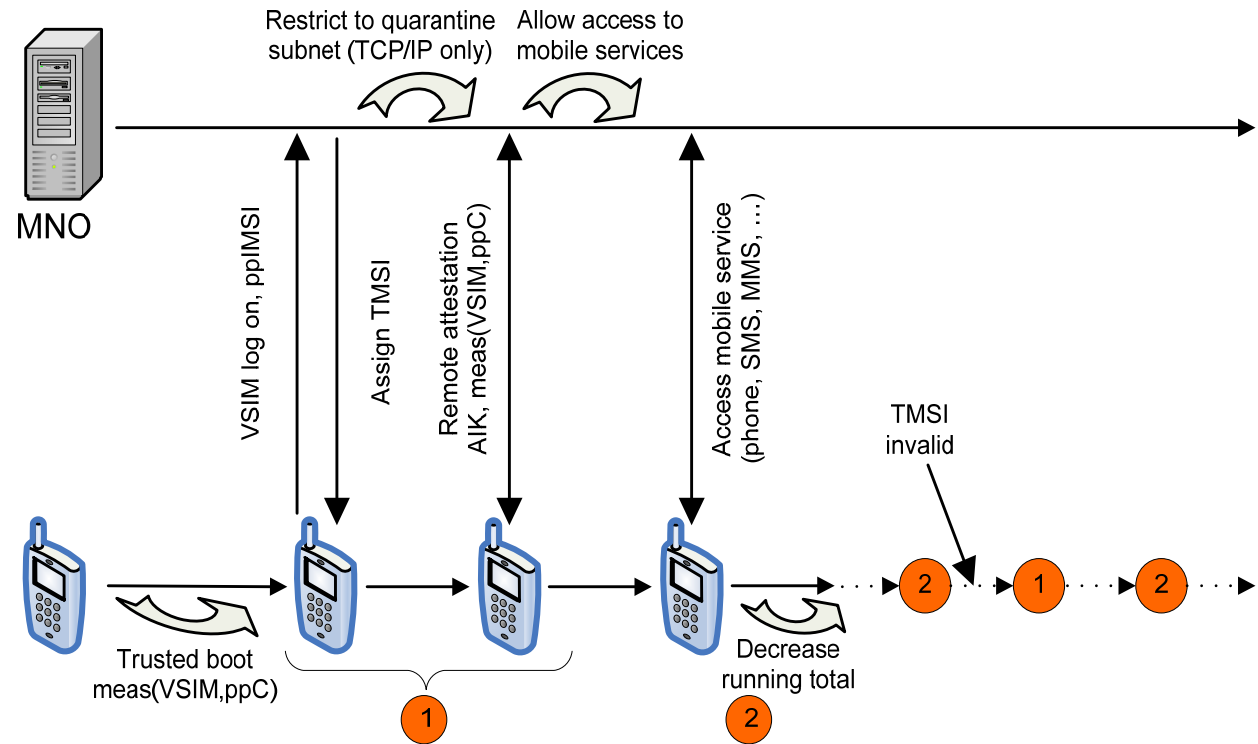
Restriction can be implemented in many ways:
AIKs, ACLs, shared secrets or individual credentials residing in trusted storage space,...

Security in restriction:

- $t_{a'}$ may be stronger than $c_{a,A}$, but basic **network access usually still requires $c_{a,A}$**
- Stronger authentication makes a' -agents **privy to special services and/or content**
- Combination of credentials raises **resilience against cloning** (by checking consistency of creds)
- **Enrolment** is key, highest security (against cloning) is only achieved if both $c_{a,A}$ and $t_{a'}$ are individualised and impressed under control of A – balance with privacy

Application of restriction: 'Anonymous' prepaid device

- A prepaid mobile device:
- Running total managed on device – no central accounting
- User can remain anonymous (not legal in the EU)
- Uses virtual SIM (VSIM) and a trusted prepaid client (ppC)



- Modified network log on 1. attests to the integrity of VSIM and ppC, after which access to network services is granted (2.), as usual using only a TMSI
- MNO can demand frequent re-attestation (e.g. by invalidating TMSI)
- Cheap one-way devices or recharging via third party SP

Restriction is a general concept with manifold applications, a major instance of which is, from an MNO's viewpoint, and in accordance with statements from the industry

➤ Functional restriction

- Finer-grained than **SIM-lock**
- enables the production of single device with **many appearances** (cost-efficient)
- Model appearance can be determined **at roll-out or even at the POS** (e.g. by user activation)
- **Dynamic, seamless up- and downgrading** according to customer SLAs
- High enforcement level. (This is as well the basis for **DRM proper**)
- Location-based restriction, e.g. to counter industrial espionage
- On-device management & transfer of sensitive user data (photos, messages,...)
- ...

Establishing identities across domain boundaries by referral trust

Transposition

Transposition can make sense if b cannot connect directly to principal B

Mobile device a and machine b mutually authenticate using trust credentials

They thus establish a secure channel to convey b's generic credential to principal B

RA. proves that the trust credential of b is unaltered

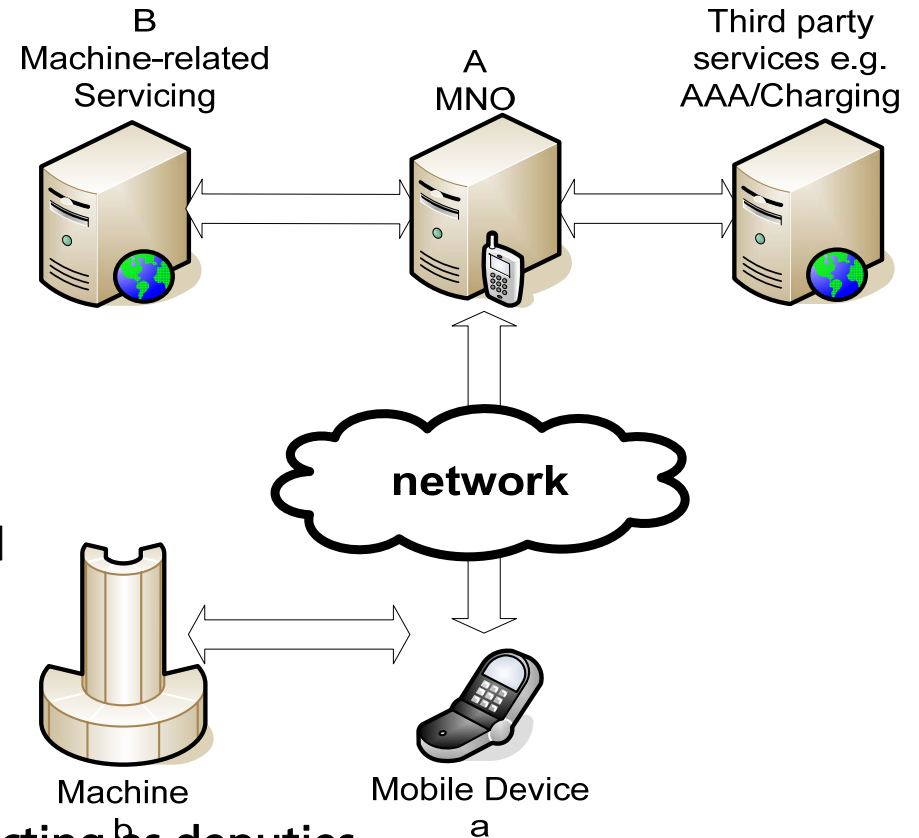
Variants of authentication of b toward B can involve A, depending on trust (e.g. contractual relationships)

AA can even be decentralised, i.e., left to agents a, acting as deputies

Balance gains by outsourcing with secrecy

Third party services, e.g., for accounting and charging can be included

Central scenarios: Point of sales (POS), remote machine maintenance and telemetry



Minimal need to know principle in transposition

The POS owner wants to hide his business secrets from the MNO, e.g.

- the location and number of its POS endpoints, sales volumes, and price structure

The MNO likes to protect the privacy of customers w.r.t. the POS owner

(and maybe even the charging provider)

Individual identities of POS and device need not be revealed in the purchase process

- Using the TC concept of a privacy CA and AIKs
- The AIK can be used in combination with the PCA certificate as a pseudonym of the platform, e.g., one per purchase
- POS and device can change their identity after a certain time

Fine **separation of duties** (POS owner / MNO / charging provider) is helpful

- e2e encryption protects individual communications

Price lists need only be exchanged between POS and mobile device

- Established trust assures that they won't leave the device

Advanced scenarios may employ DAA

Integrated scenario: Facility management

MNO offers services to fac. Managers

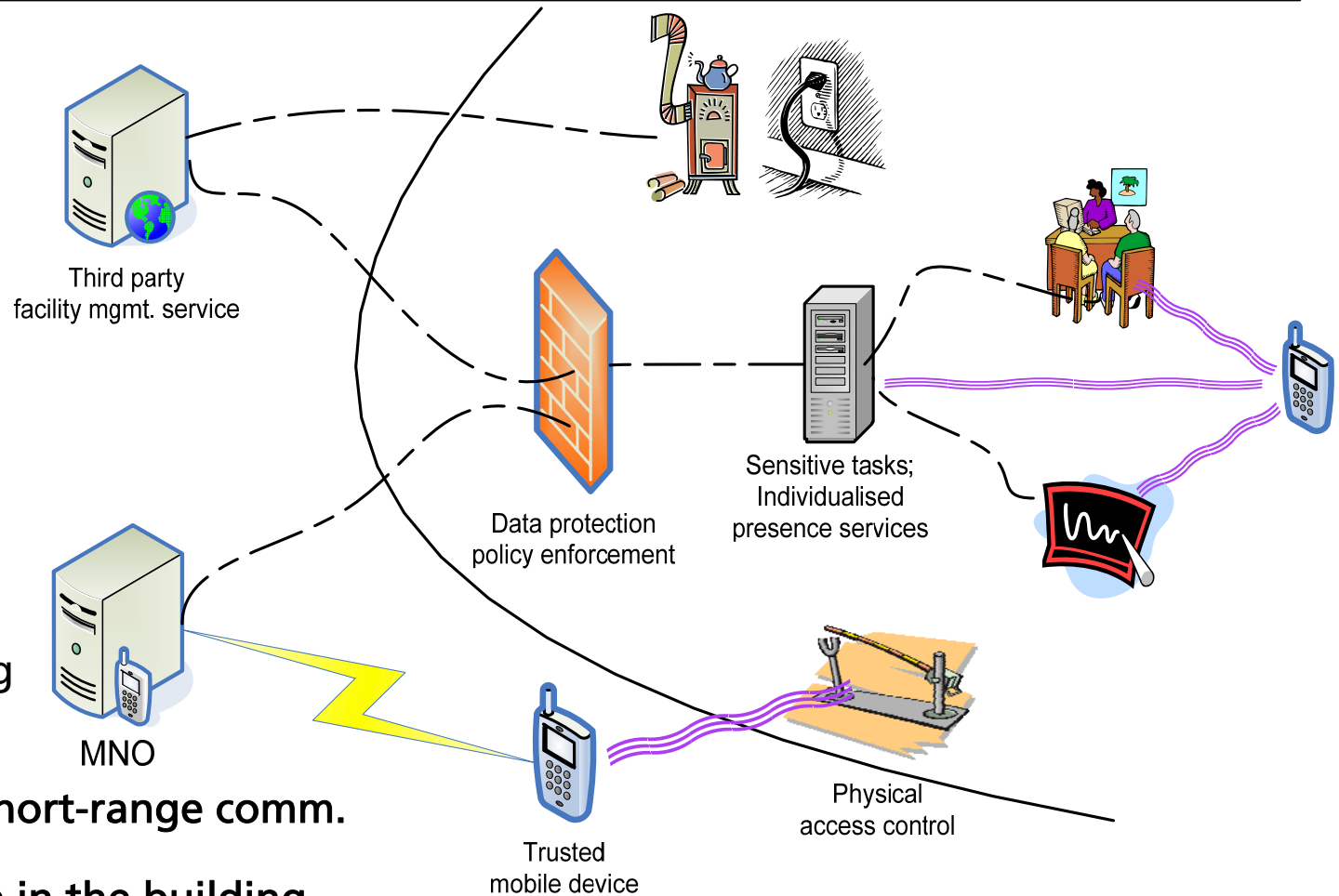
No more specialised tokens to access a building – standard mobile devices can be used

Authentication at gates is essentially transposition

Functional restriction to, e.g., disable cameras and suppress MMS within building

Tasks within the building can be fulfilled using mobile's short-range comm.

Can save network infrastructure in the building



Trusted Computing research and application potential

- TC supports two emerging and ongoing trends in ICT
 - horizontal integration of access technologies
 - movement from closed to open systems in business environments

- TC can provide a de-centralised trust infrastructure,
transgressing technical boundaries between, eg., authentication domains and methods – research on a fundamental and applied level is needed

- TC has great potential *in combination* with other technologies
like RFID, mobile devices, PKI

- TC has a potential to partially complement or co-operate with IDM

- TC can be an enabler for new business models and market mechanisms, e.g.
 - de-centralisation of trust transactions, recommender systems, ...),
 - integrated multi-VAS (provider) businesses
 - peer-to-peer, and superdistribution-based markets
 - Web 2.0+ business