Trusted Computing: Introduction & Applications

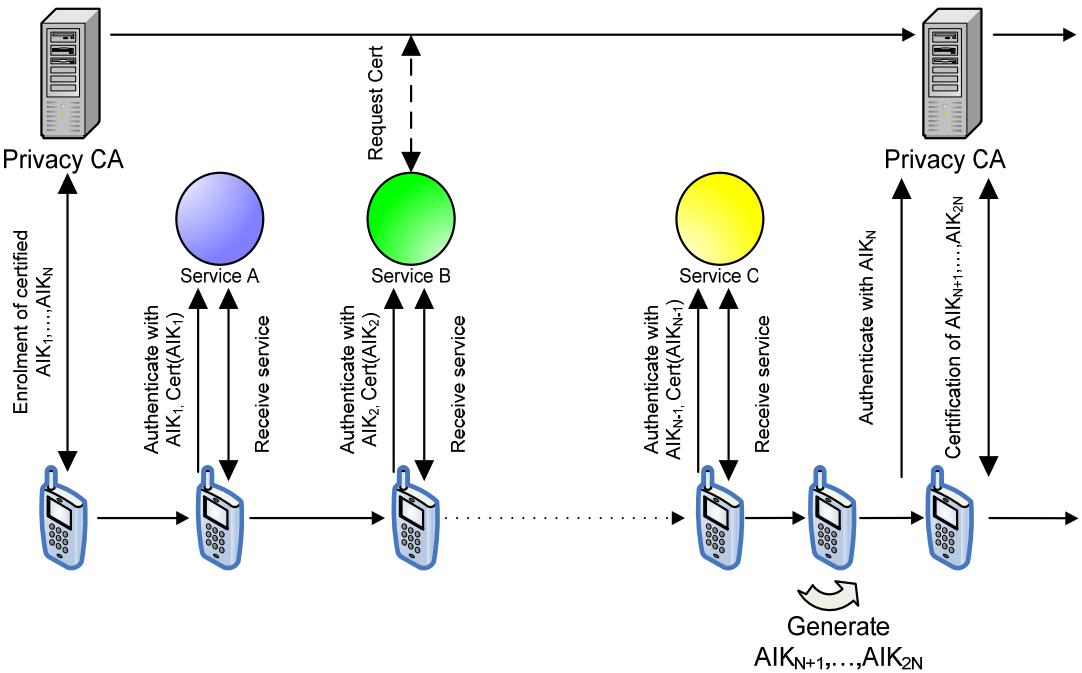
Lecture 9: Mobile Applications

Dr. Andreas U. Schmidt

Fraunhofer Institute for Secure Information Technology SIT, Darmstadt, Germany

A bit of privacy in service access by RA and AIKs

- Assume AIKs are used for AA to service access
- Then principals can annul the pseudonym annd identify users, by 1to1 association of genuine credentials to TPs (SIM)
- Improvement: Use One-time AIKs (like one-time PIN/TANs) to prevent accumulation of profiles by principals and/or service providers



- Better: use DAA, 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

Trust credentials

- **By RA (or DAA), a an agent a which is a TP can establish a trust credential t_a, embodying three fundamental assertions**
  1. **The presence of a live and unaltered TPM.**
  2. **The integrity of the system and its components**.
  3. **That an existing credential $c_{a,A}$ is unaltered.** (Established by trusted system software and components to access it)

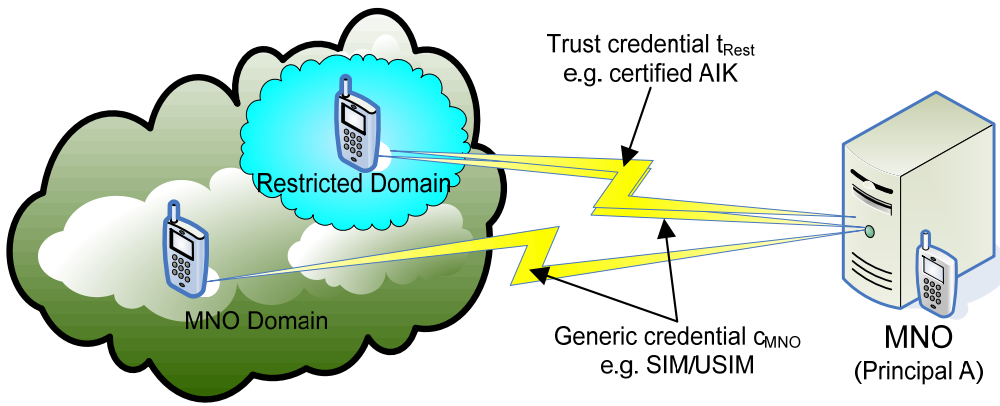
- **3. builds on 1. and 2.**

Applied categories of transitive trust

- **Restriction**
  An agent a in the domain of principal A is put in a subclass a‘, e.g. privy to special services or content
- **Subordination**
  An agent b (previously not in A‘s domain) is incorporated in it by referral through an agent a in that domain who vouches for him
- **Transposition**
  authentication of agent b w.r.t. her own principal B is mediated through agent a in domain A
- **Categories centred on agents a in principal A‘s (the MNO‘s) domain and involve increasing number (0,1,2) of other subjects**
- **Mind: Applied categories, *not orthogonal* (e.g. transposition can sometimes be decomposed in twice subordination). Theoretical refinement seems possible**

Restriction

- **Restriction places agents a in a subgroup a‘<a, by two-factor authentication**, with generic credential $c_{a,A}$ and trust credential $t_{a‘}$.
- **$c_{a,A}$ and $t_{a‘}$ are used independently, thus needs only assertions 1.&2.**
- **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

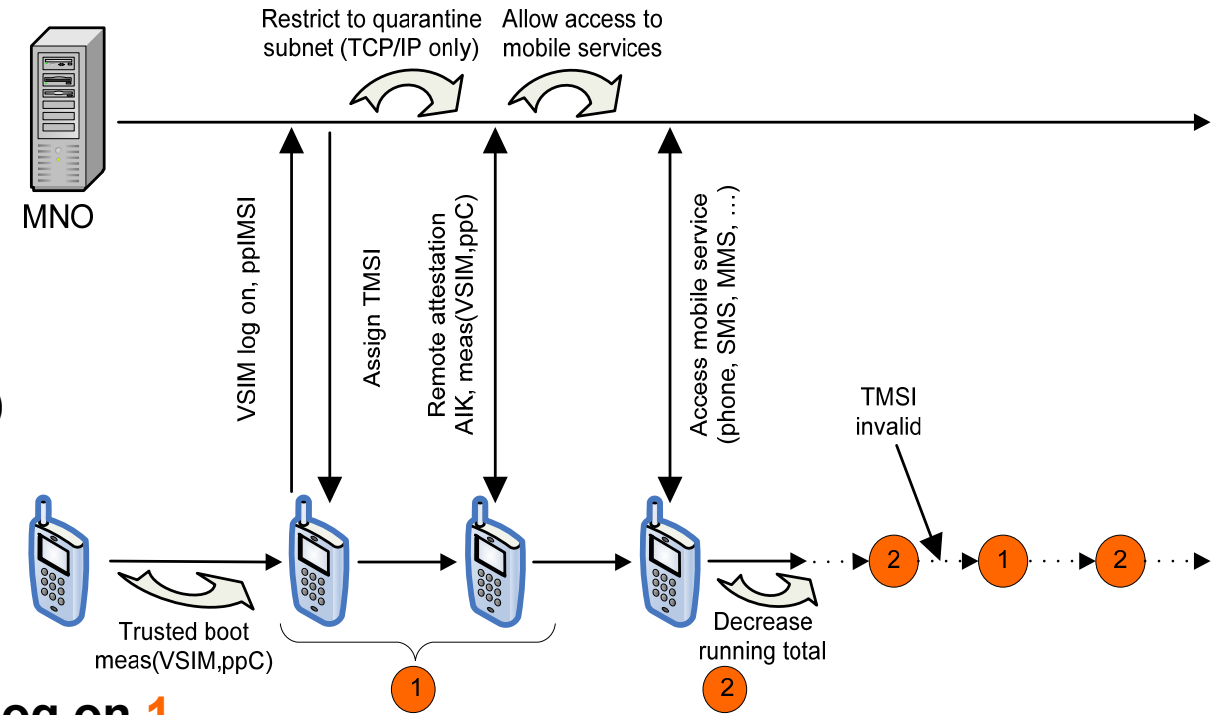


Restriction applications

- **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,…)
  - …

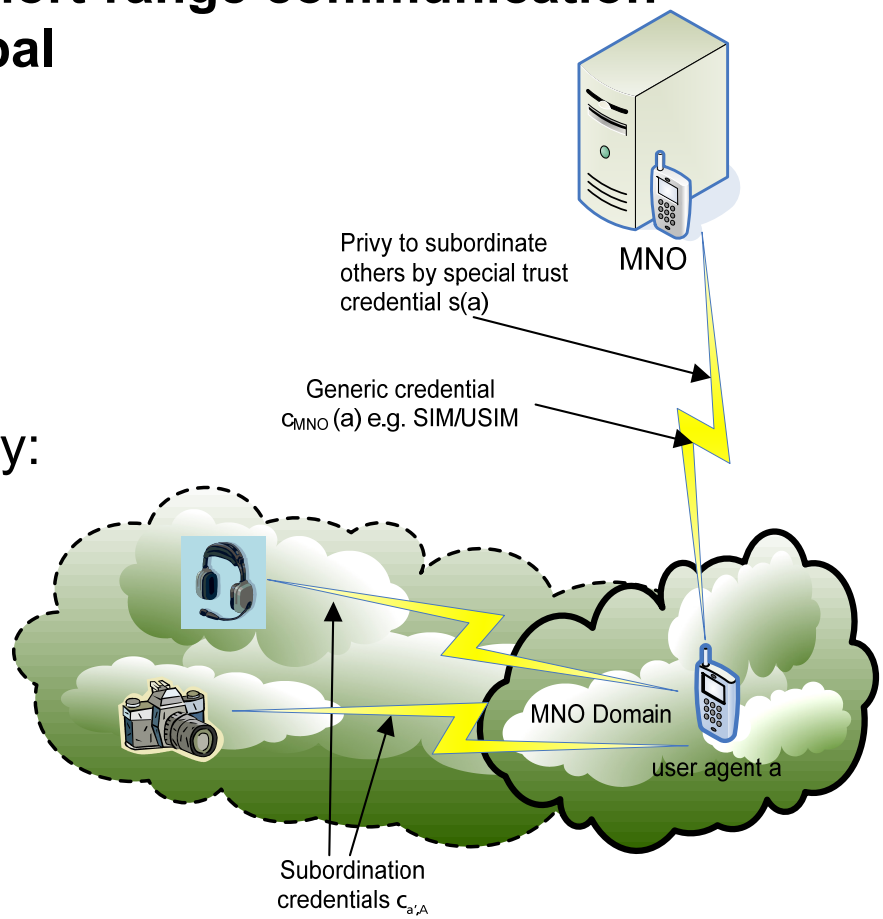
Application of restriction: 'Anonymous' prepaid device

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



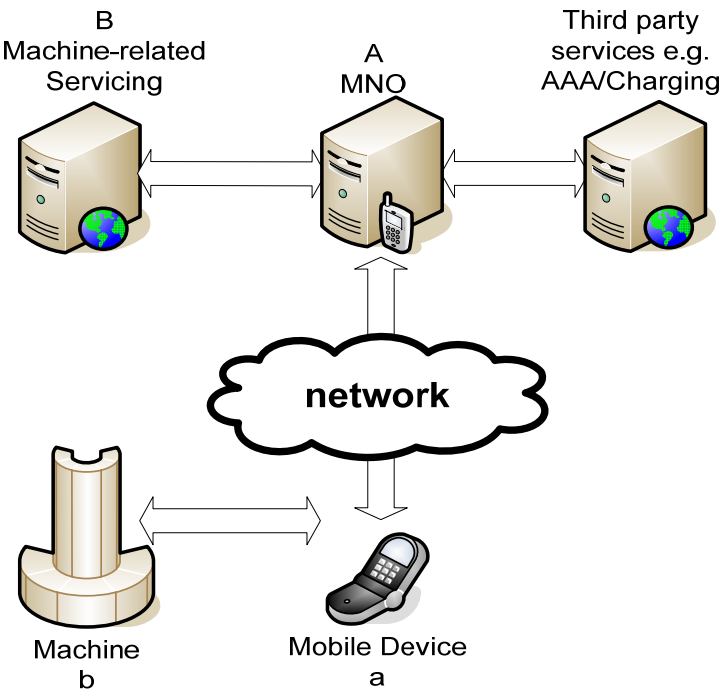
- **Modified network log on 1.** attests to the integrity of VSIM and ppC, after which access to network services is granted (2.), as usual using only a TMSI
- **MNO can demand frequent re-attestation** (e.g. by invalidating TMSI)
- **Cheap one-way devices or recharging via third party SP**

- **Subordination introduces new agents to A‘s domain, mediated by existing agents**
- **Subordinated agents can use short-range communication**
- **Direct communication to principal not required**
- **A can but need not partake in authentication**
- **Many possible variants**
  - If a dedicated credential $c_{a',A}$ is used for sub-devs, trusted assertion 3. is necessary:
  - an existing credential $c_{a',A}$ is unaltered.
- **Prime example: Bonding of accessories to mobile devices**
- **Extends range of SIM-lock – ‚customer retention‘**



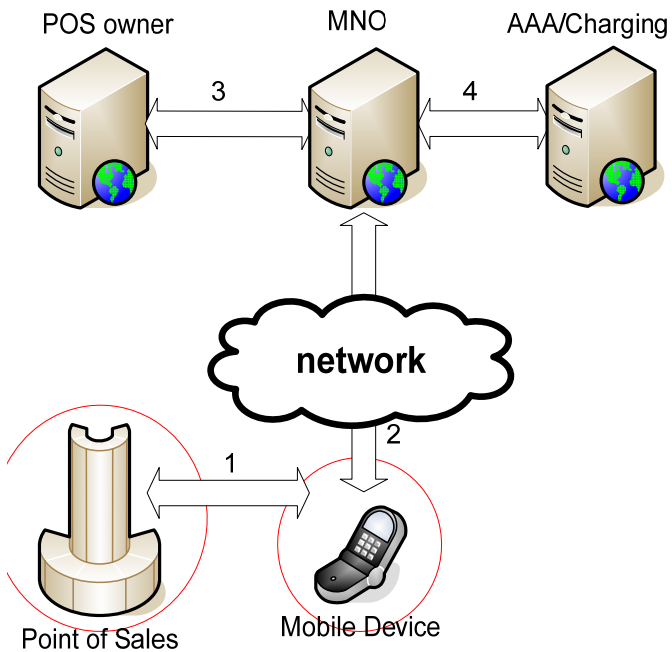
Transposition

- **Transposition can make sense if b cannot connect directly to principal B**
- **Mobile device a and machine b mutually authenticate using trust credentials t_a, t_b**
- **They thus establish a secure channel to convey b's generic credential $c_{b,B}$ to principal B**
- **Assertion 3. proves that $c_{b,B}$ 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**

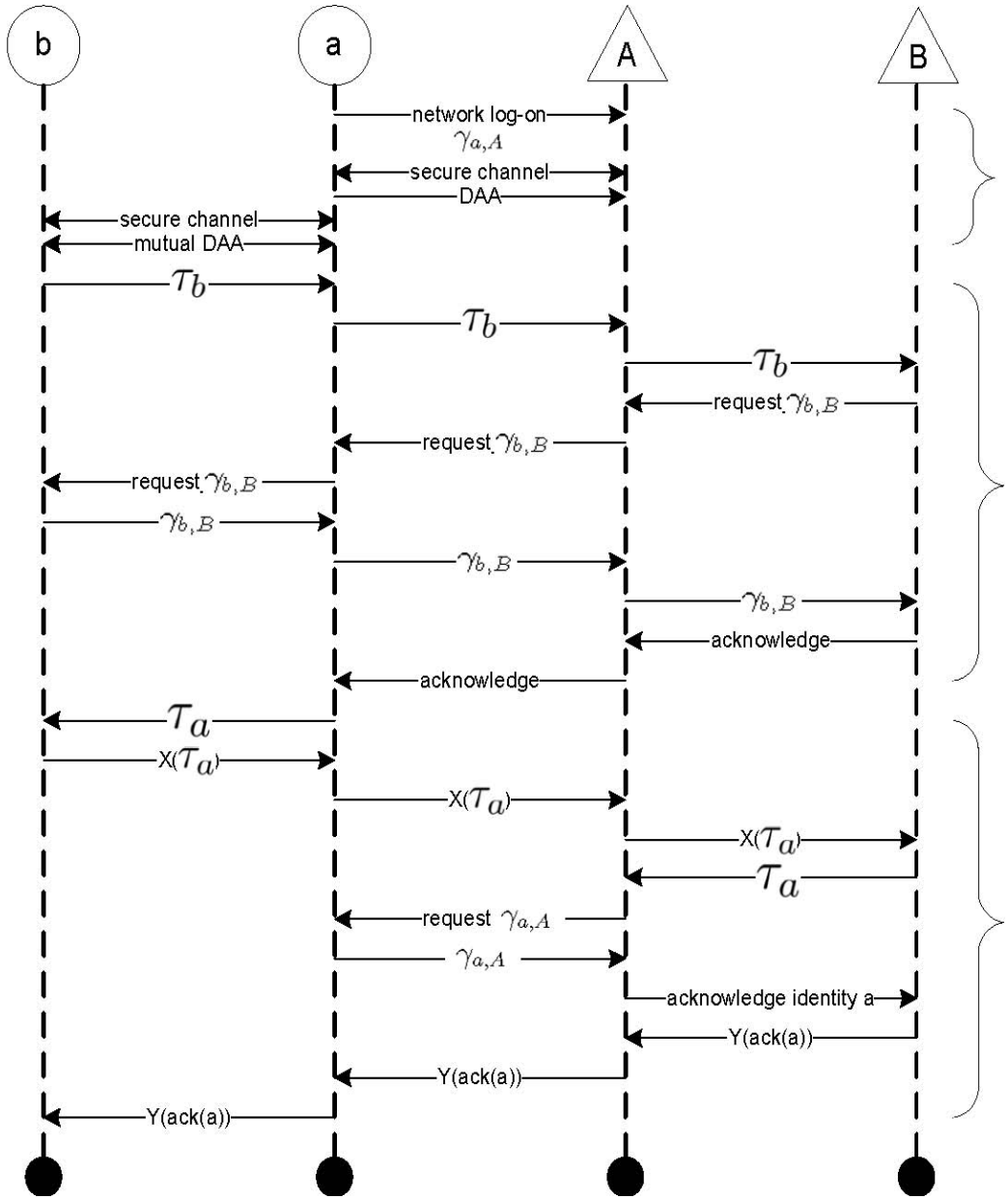


Point of Sales

- (1) Mutual proof of integrity between POS and mobile device as trust base of the purchase operation device and POS exchange price lists and payment modalities
- POS has to verify the device's authentication by connecting the POS owner infrastructure (via the mobile device). Alternatively POS connects the charging provider
- (2) Signed price and payment processing info is transferred to the MNO
- (3+4) The charging data is transferred to the POS owner where a special data package for the charging provider is generated
- After the confirmation of the charging the POS owner (or the MNO) acknowledges the purchase and the POS vending machine delivers the good.



Transposition realisation



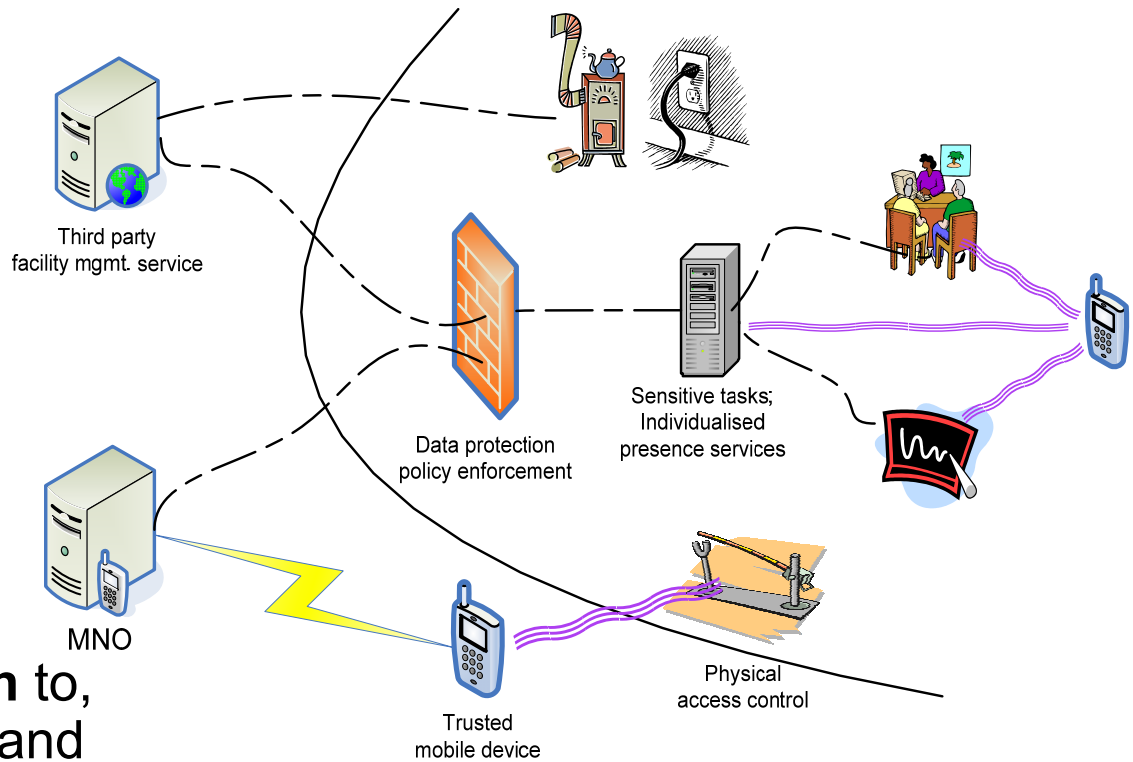
- **The sequence shows a realisation variant**
- **It establishes maximal mutual trust:**
  Both principals A and B can trust the involved agent of the other domain, resp. b, and a
- **It is equivalent to two subordinations, with exchanged roles**
- **Many other variants are possible**

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**

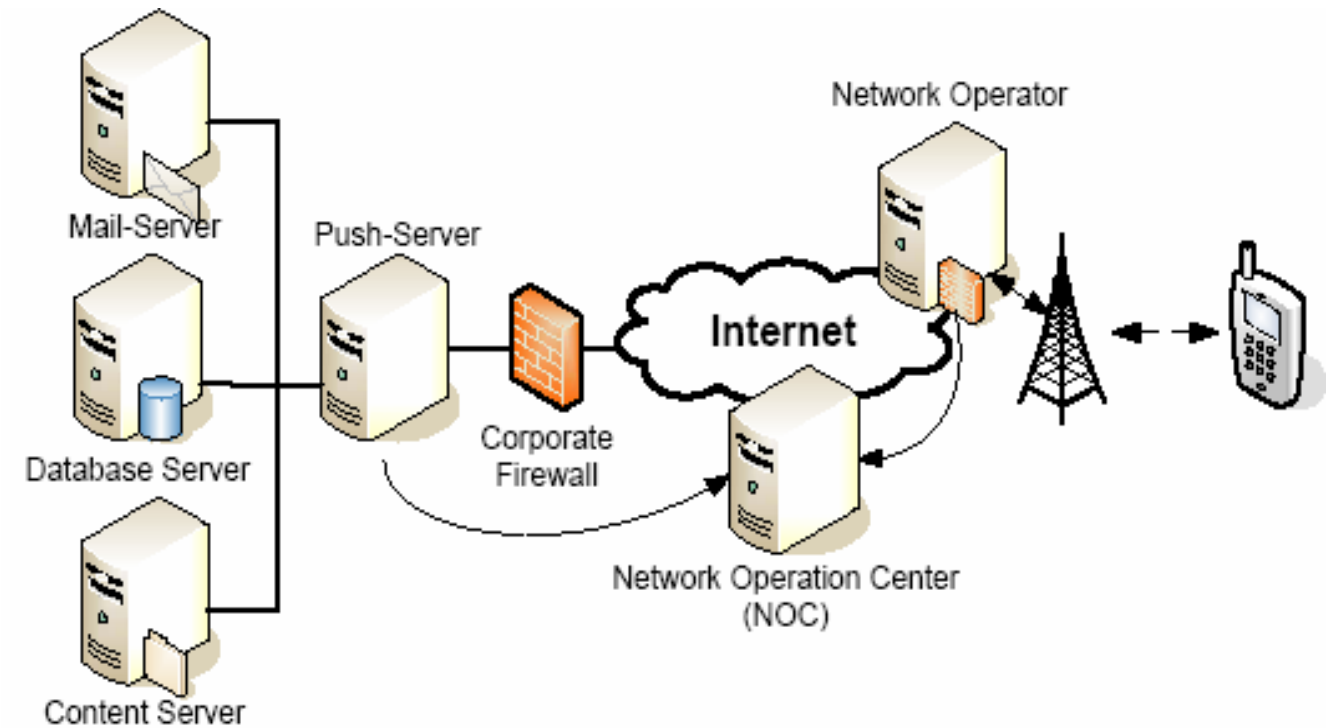
Integrated scenario: Facility management

- **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**

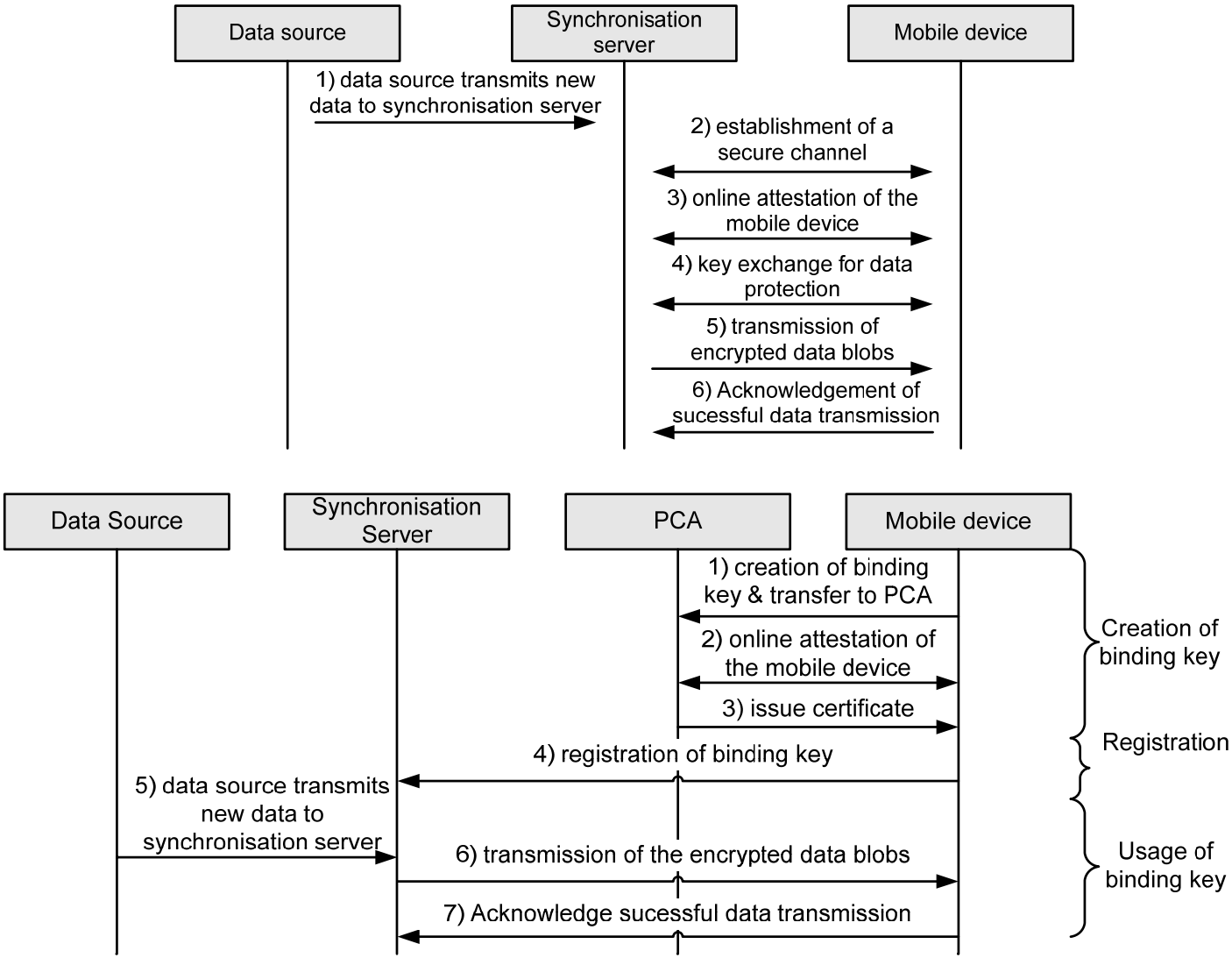


Content protection in Push services

- In a centralised architecture, push services pose various security risks to transported content



Content protection in Push services



Trusted Computing research and application potential – traits of the technology and research perspectives

- **The public's negative impression of TC is gradually changing**, e.g., data-protection agencies note TC's potential for privacy-protection. TC has been functionally and organisationally separated from DRM
- Mobile devices and laptop PCs will soon provide a broad base of TC-equipped user agents
- The **relationship between privacy, data protection, and TC** should be further examined:
  privacy is not in opposition to TC, but rather privacy protection can benefit from TC (by, e.g, separation of duties, implementation of ‚minimal need to know' principles)
- **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, idenitity management (IDM)
- **TC has a potential to partially replace resp. complement or co-operate with PKI and IDM**

Trusted Computing research and application potential – application and economic perspectives

- **TC supports two emerging and ongoing trends in ICT**
  - horizontal integration of access technology
  - movement from closed to open systems in business environments
- **TC application should be explored in various (economic) sectors such as**
  - Mobile (broad user base, established AAA infrastructure)
  - E-Government (e-procurement, government rights management, controlled publication of data)
  - E-commerce (user-to-user transactions, commercial grade signatures)
- **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