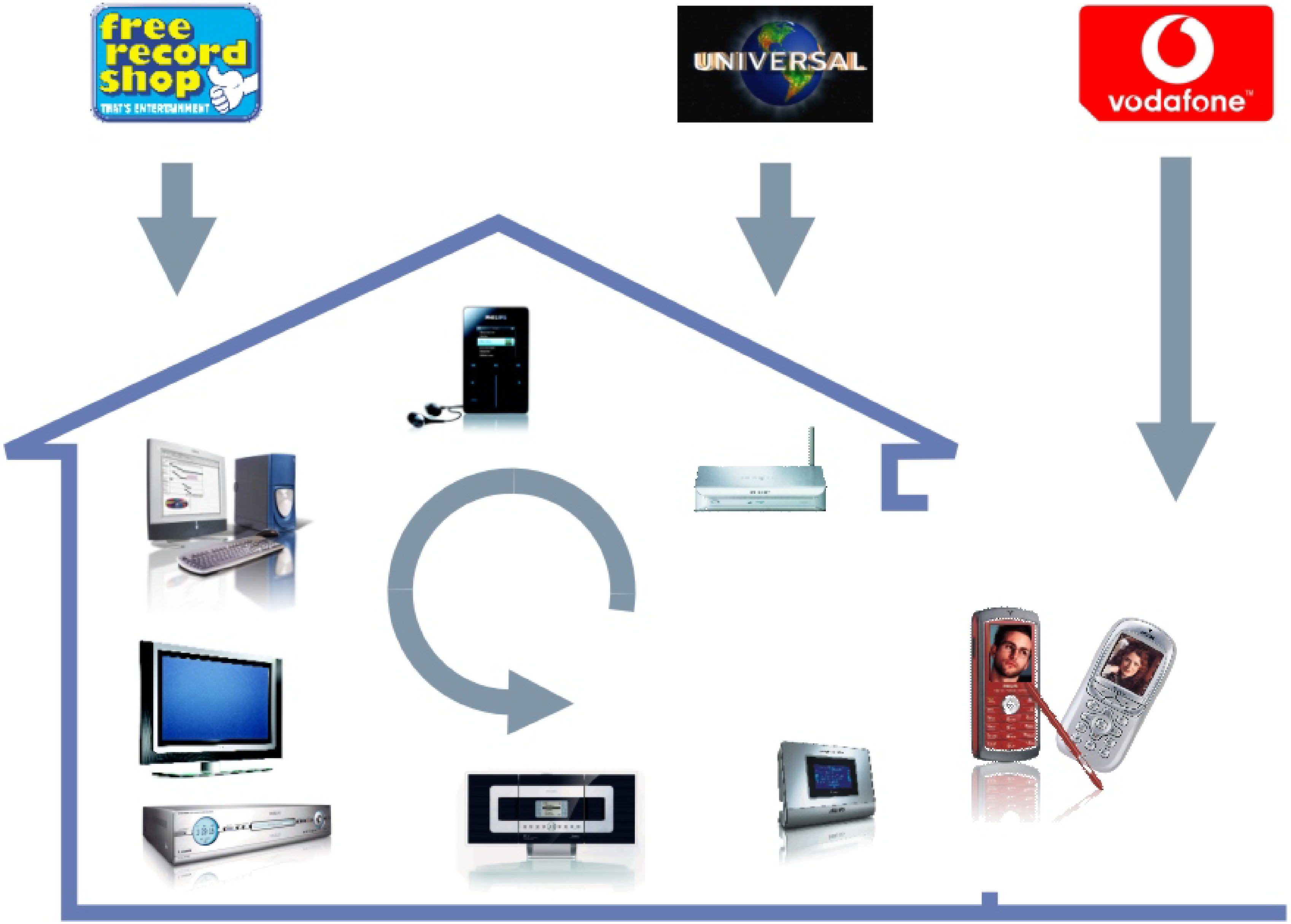
Introduction of the Domain Issuer in OMA DRM

DRM workshop CCNC 2007

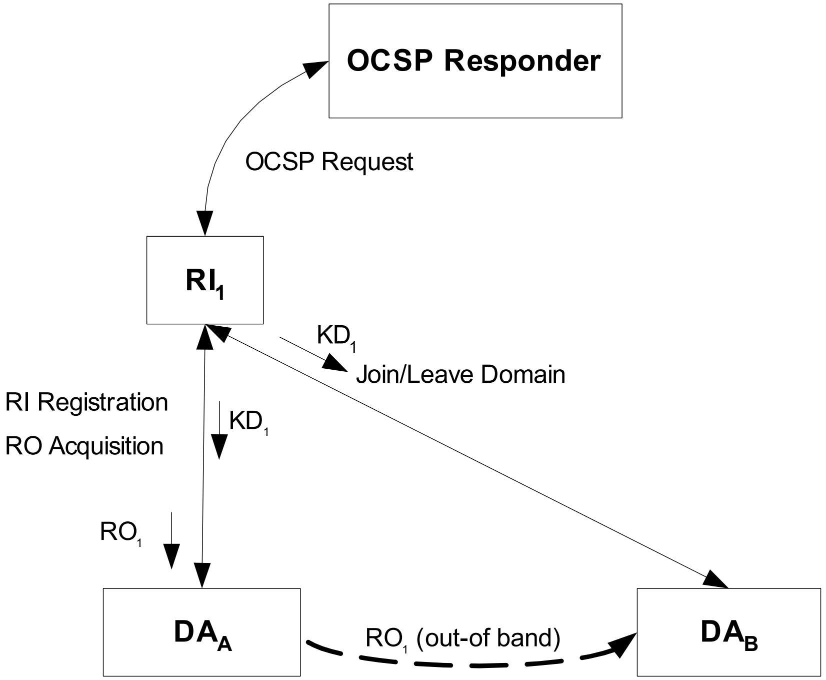
Paul Koster, Javier Montaner, Sorin Iacob, Najib Koraichi
Philips Research, Vodafone R&D .NL, Telematica Instituut
Mobile Enabled Secure Exchange of Content
January 11, 2007


free record shop
THAT'S ENTERTAINMENT
UNIVERSAL
vodafone™

OMA DRM 2.0 Domain Architecture

- Rights Issuers define Domains consisting of DRM Agents
- Rights Issuers issue Rights Objects bound to Domains
- DRM Agents exchange Rights Objects (and Content) out-of-band

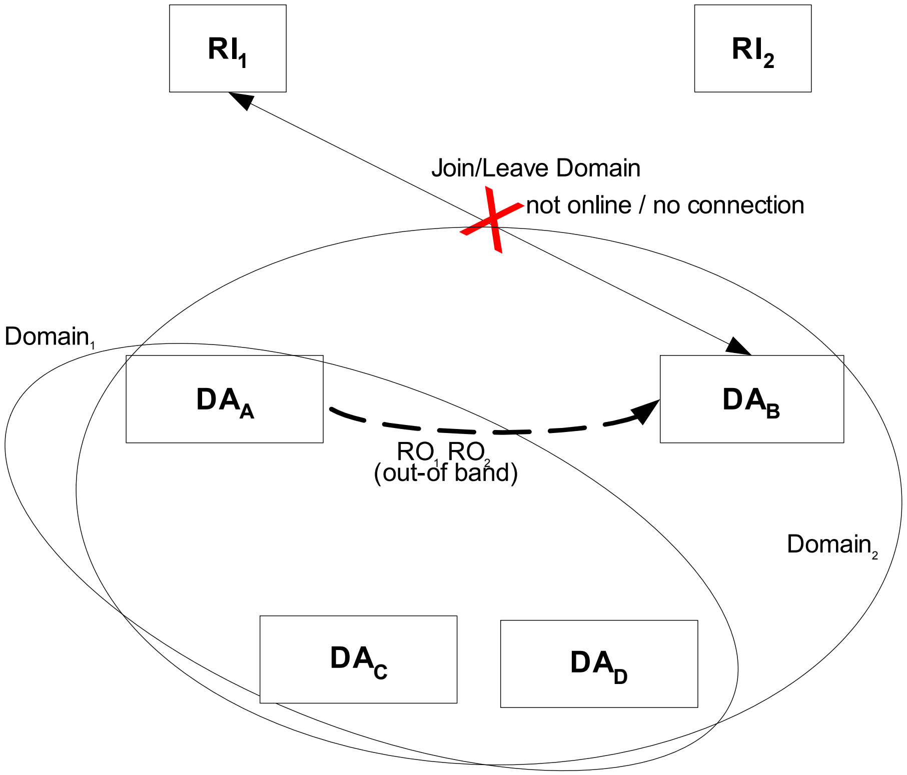
➔People can use their content on all their (domain) devices



Multiple Rights Issuers cause confusion

- People buy their OMA DRM content at multiple shops.

- No uniform behavior on all devices
  - Some content plays on all
  - Other content first requires online Join Domain
    - inconvenient and confusing for offline cases, e.g. mobile music players or memory cards

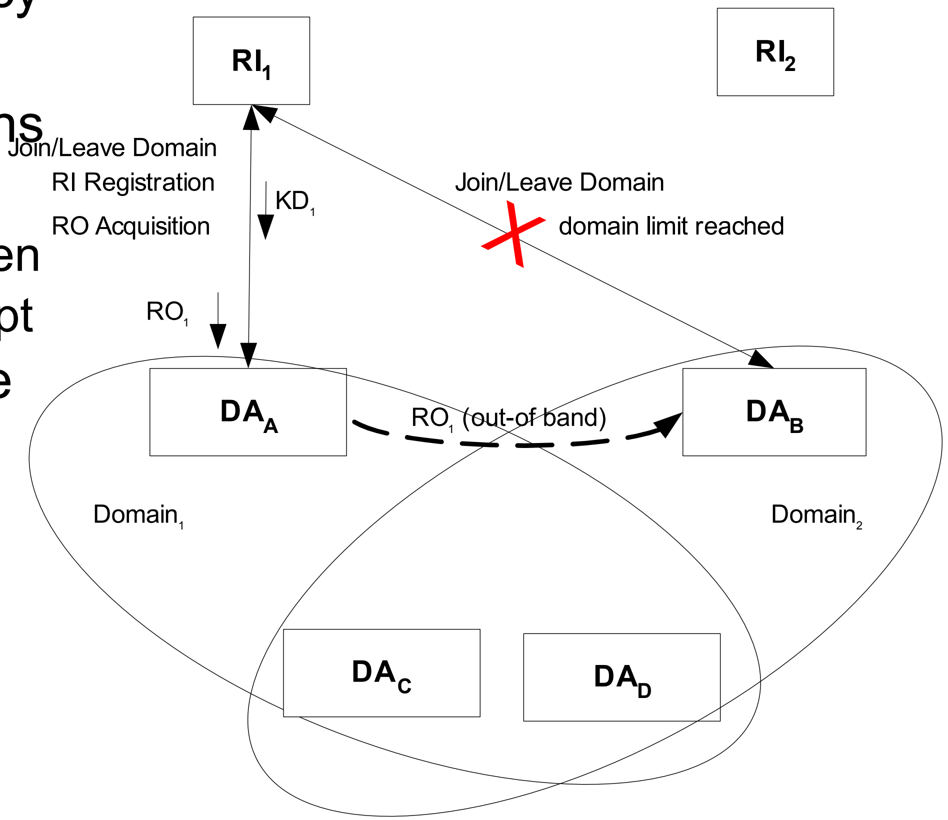


Multiple Rights Issuers cause inconvenience

- Rights Issuers have a domain policy

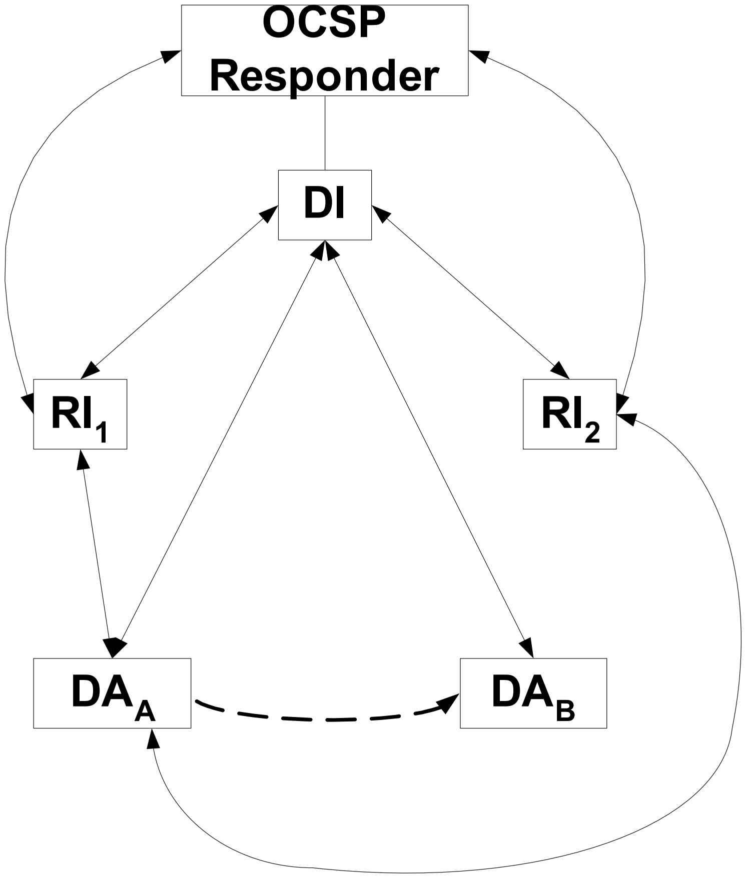
- User manually synchronize domains
  - Requires work
    - Although process is easy when done on first rendering attempt
  - Impossible in cases where one domain reached the maximum
    - Non-overlapping set of DAs

- Consistency expected



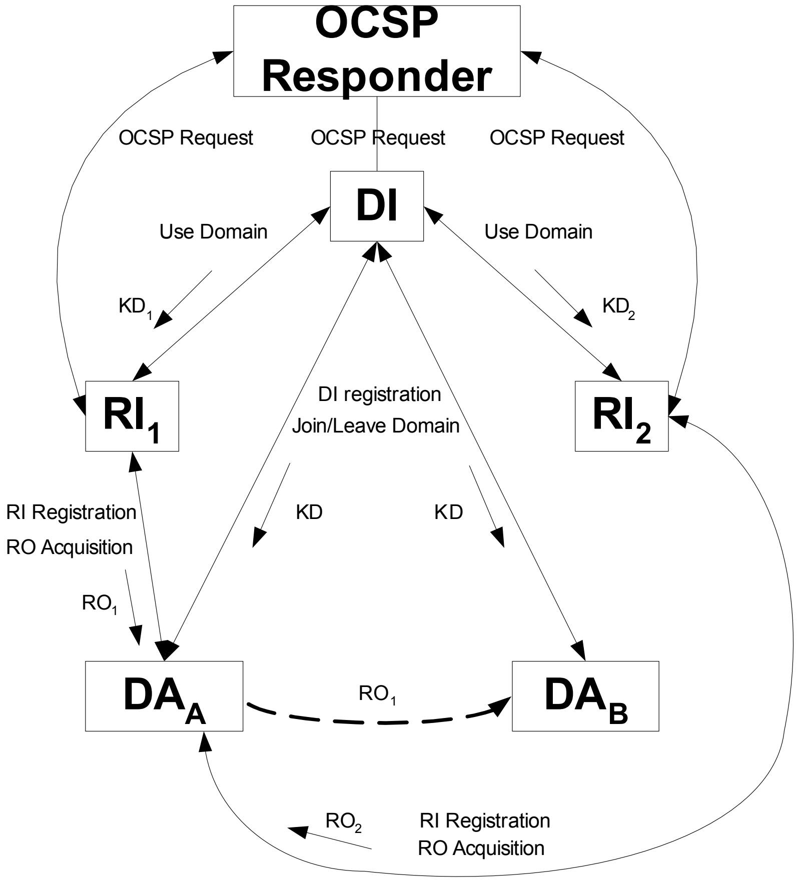
Introduction of the Domain Issuer in OMA DRM

- Single shared Domain Issuer improves user convenience
  - Enables user to have one domain.
  - One Join Domain between DA and DI ensures that DA can render all content issued by participating RIs.

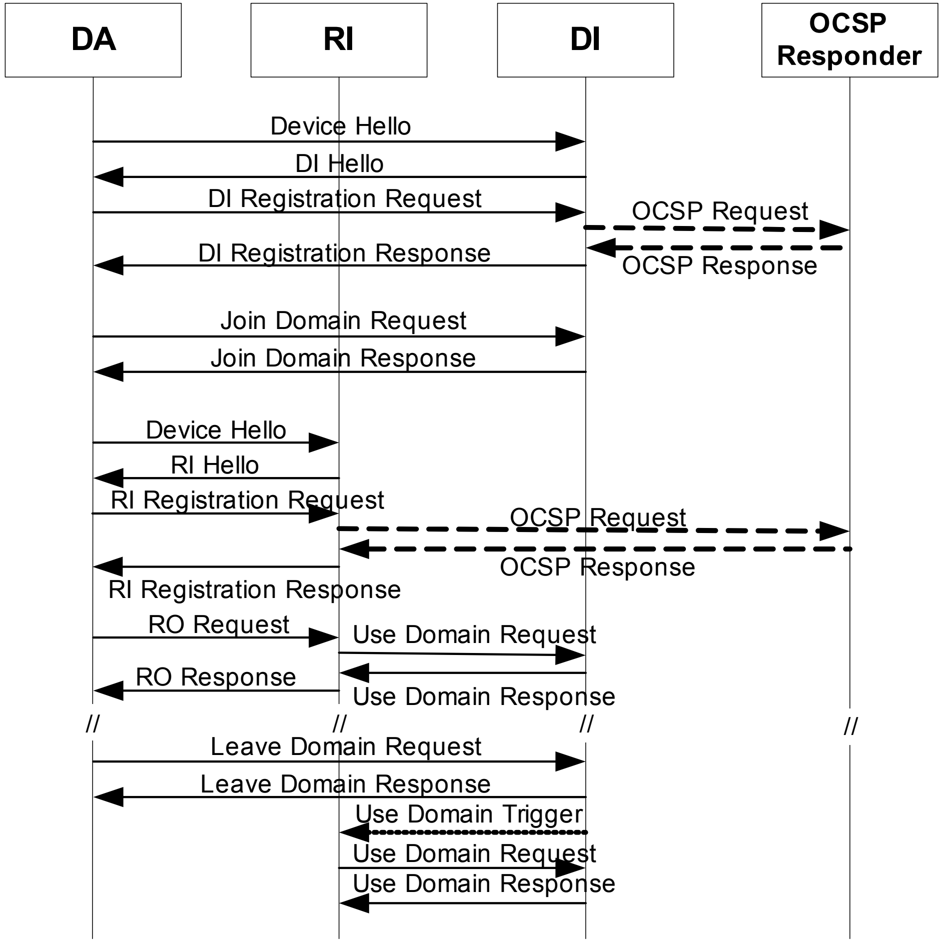


Architecture

- One or more DIs
  - One: practical, clearer √
  - More: confusing, inconvenient
- Domain key management
  - DK per DI: DI control, practical √
  - DK per RI: No efficient DK distribution
- DI, RI and DA communication
  - Protocols limited to 2 parties: operational independence, robust √
  - Proxy requests, etc.: less robust



Example interaction



Requirements

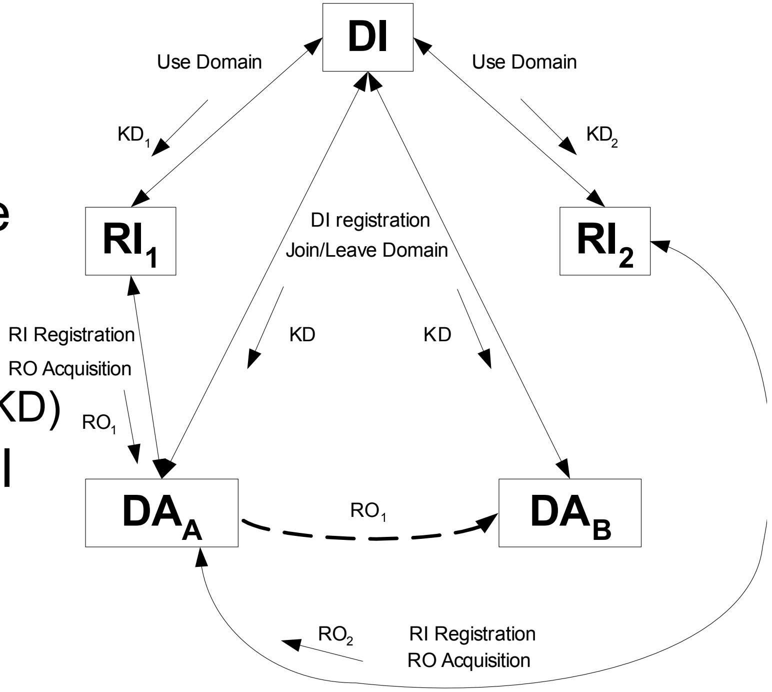
Prevent negative effects on RI and protect DI interests:

- The DI should play an essential role in key management for his domains so that it cannot be bypassed.
- The DI should be able to stop the use of domain functionality when the business relationship with RI ends.
- The RI shall trust the DI but should not need to trust other RIs that issue content for the same domain.
- Non-trusted devices should be revocable from a domain in order to secure future domain content.
- Content issued by other RIs should not be affected when a RI is revoked.

Domain key diversification

- Diversified Domain Keys (KD_i) per RI_i
  - DI control
  - RI independence

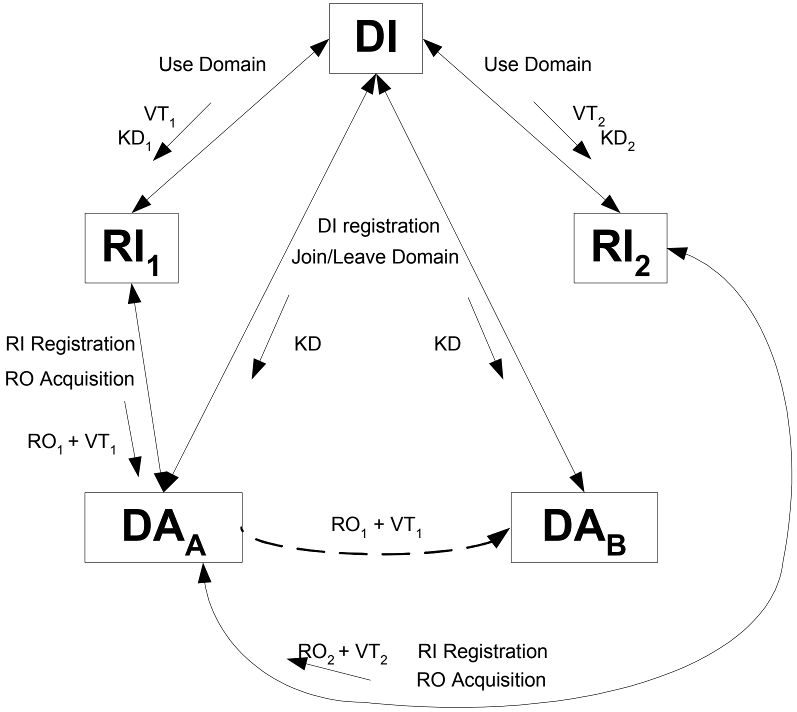
- KD_i derived from Master Domain Key (KD). KD shared by DI and DAs. KD not available to RIs.
  - DI and DA calculate KD_i using
    KD_i = first 128 bits of HMAC-SHA1(PubKeyRI, KD)
  - RI_i obtains KD_i via Use Domain protocol
  - RI_i encrypts RO with KD_i



ValidationToken

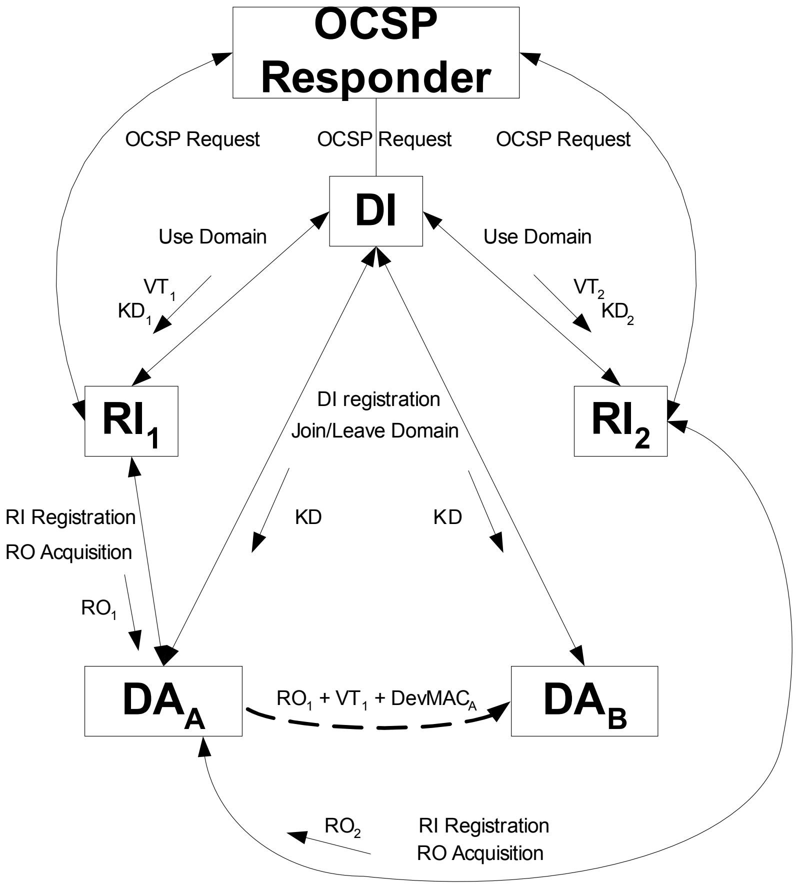
- Diversified domain keys do not confine a KD_i to one RI and have limited revocation options
- Validation Tokens (VT) entitle RIs to issue ROs to DAs belonging to domains of a DI.
  - DI control
- Operation
  - DI (periodically) creates VT_i

    VT_i = {ExpiresAfter, RI_i PublicKey}$_{\text{signedDIPrivateKey}}$
  - RI_i obtains VT_i via Use Domain protocol
  - RI_i embeds VT_i in RO
  - DA verifies VT_i using DI context



DeviceMAC

- ValidationTokens do not prevent RI to issue ROs out-of-band
  - Using old VT
  - DAs cannot verify compliance of RI
- DeviceMAC asserts that RI had a valid non-expired VT and was non-revoked at RO acquisition
  - DI control
  - Proof RI compliance to DA
- Operation
  - DA obtains RO and VT from RI
  - DA computes DeviceMAC: DeviceMAC = HMAC-SHA1(RO, KD)
  - DA embeds DeviceMAC in RO
  - DAs validate DeviceMAC for ROs received out of band.



Evaluation

- Requirements met
  - Solution addresses business requirements of both DI and RI
  - However strong dependence on DI

- Security is comparable with OMA DRM 2.0
  - Domain keys protect content keys
  - Domain key updates protect future content
  - Compliance / revocation supported
  - However, DI has master domain keys

Conclusions

- Separate Domain Issuer increases user friendliness.
- Limited changes to OMA DRM 2.0.
- Security mechanism to support independent roles of DI and RIs.
- Future work
  - transfer of domain (keys) from one DI to another
  - rights/domain management local to devices

Q&A

PHILIPS