



A DRM Security Architecture for Home Networks

Bogdan C. Popescu - Vrije Universiteit

Frank L.A.J. Kamperman - Philips Research

Bruno Crispo - Vrije Universiteit

Andrew S. Tanenbaum - Vrije Universiteit



Outline

- Application scenario
- Authorized Domains framework
- Authorized Domains security architecture
- Conclusions



Application Scenario

- Distributing digital home-entertainment content
 - music
 - digital television
- Requirements
 - providers - prevent illegal copy and re-distribution
 - consumers - “content anytime, anywhere”



Protecting Content

- Content always associated with usage rules
- Content only released to **compliant devices**
 - built by licensed manufacturers
 - by construction always enforce usage rules
 - tamper-resistant to prevent circumvention
 - can prove they are compliant - using crypto keys incorporated in the device when manufactured

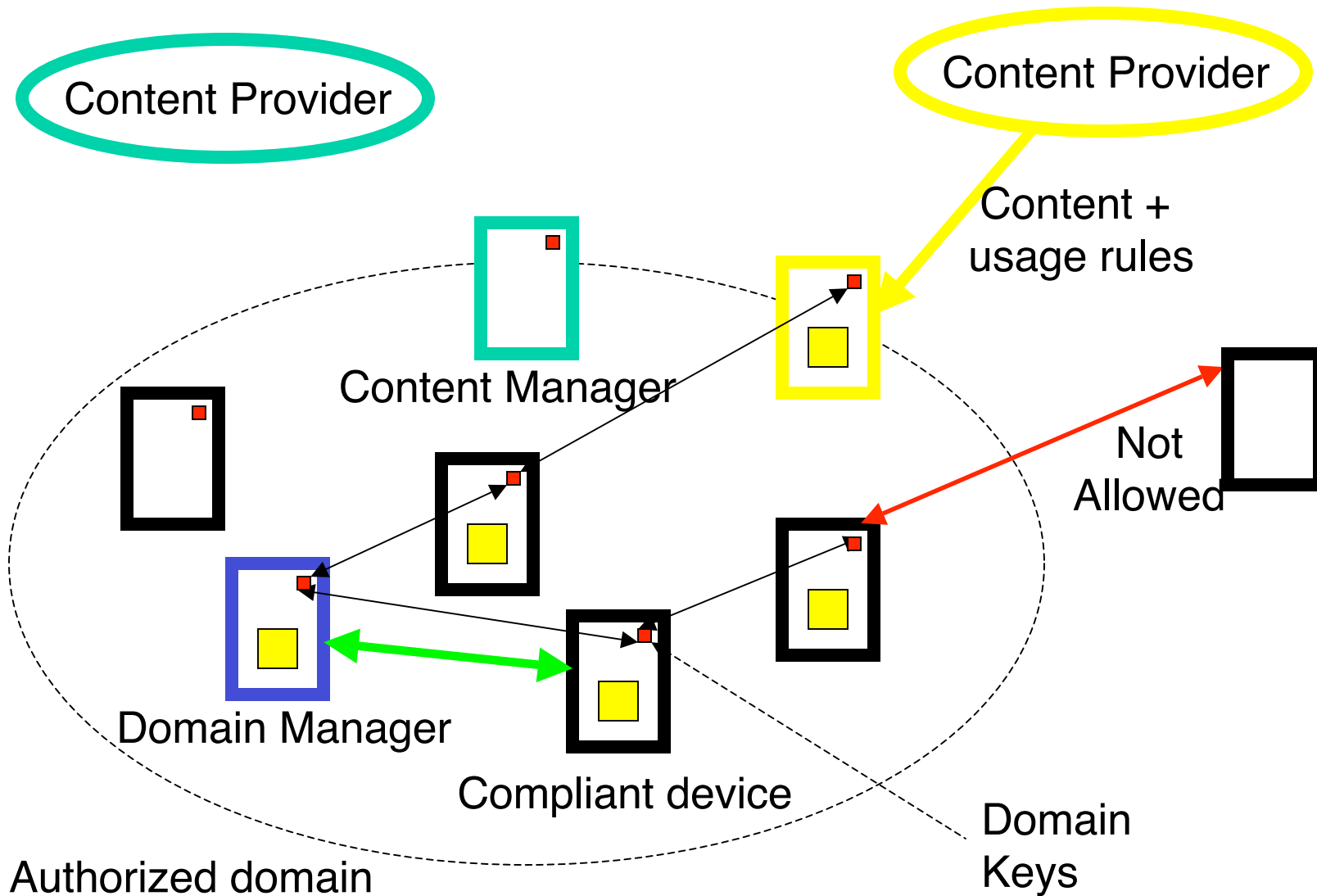


“Content Anytime, Anywhere”

- Consumer allowed to link **limited** number of compliant devices into a home network
- Content can move freely inside home network, subject to usage rules
- Tight controls applied at network boundaries



“Authorized Domains” Framework





Implementation Requirements

- No continuous network connectivity
 - AD may be disconnected from Internet
 - individual devices may be disconnected from AD
- Simple management operations
 - adding new device should only affect that device
- Limit manufacture costs
 - preferably not use crypto accelerators
 - reduced use of public key operations



Compliant Device

- Public/private key pair
 - public key certified by manufacturer - device certificate
 - private key stored in tamper-resistant memory
- Unique **Global Device Id (GDI)** included in device certificate



AD Creation

AD Manager

IDDomain

Master Key

List

Index Key GDI

0	K ₀	
:		
I	K _I	
:		
N	K _N	

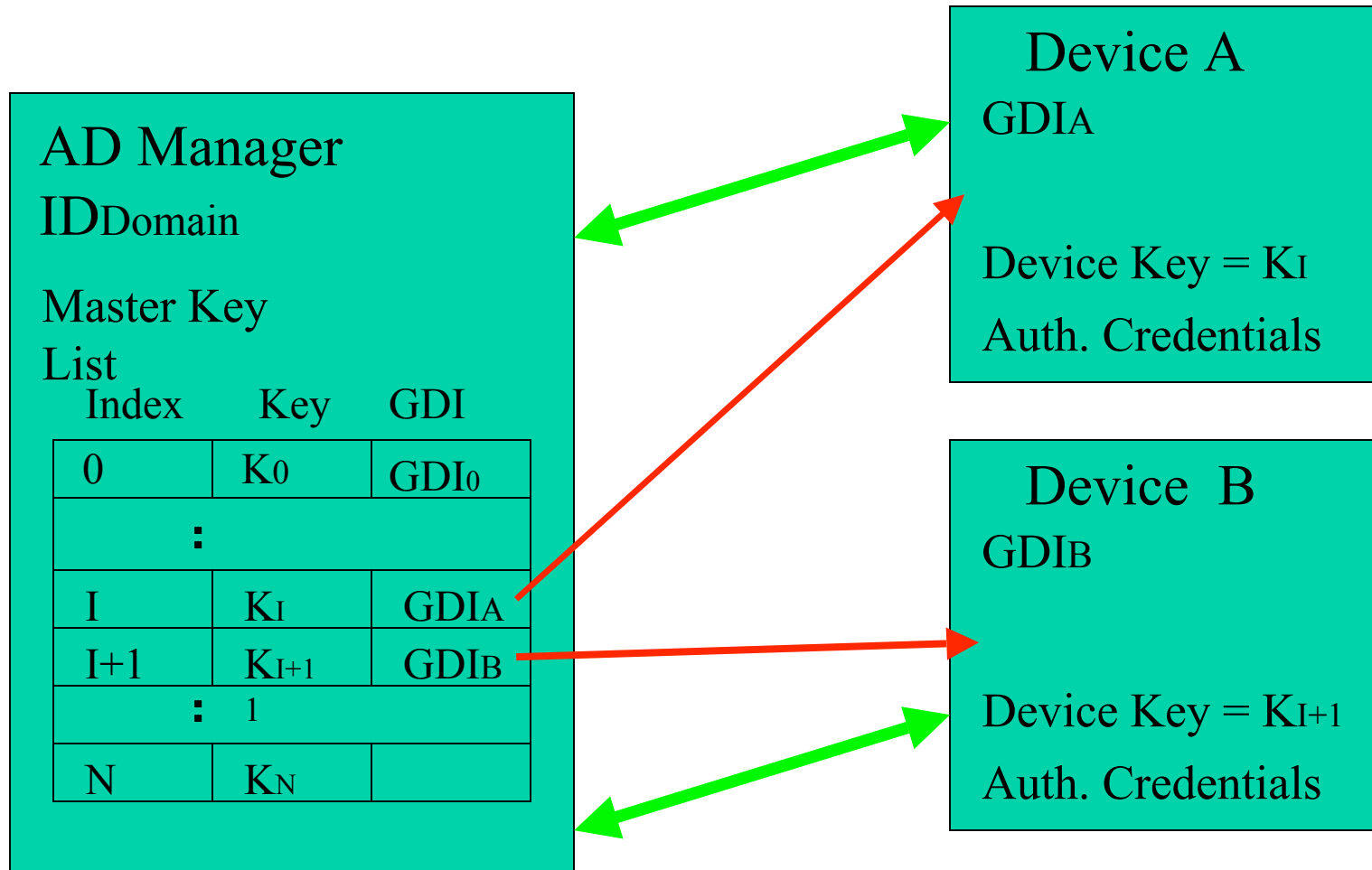
IDDomain must be unique!

K_I – 128b AES key

N = max. devices in domain

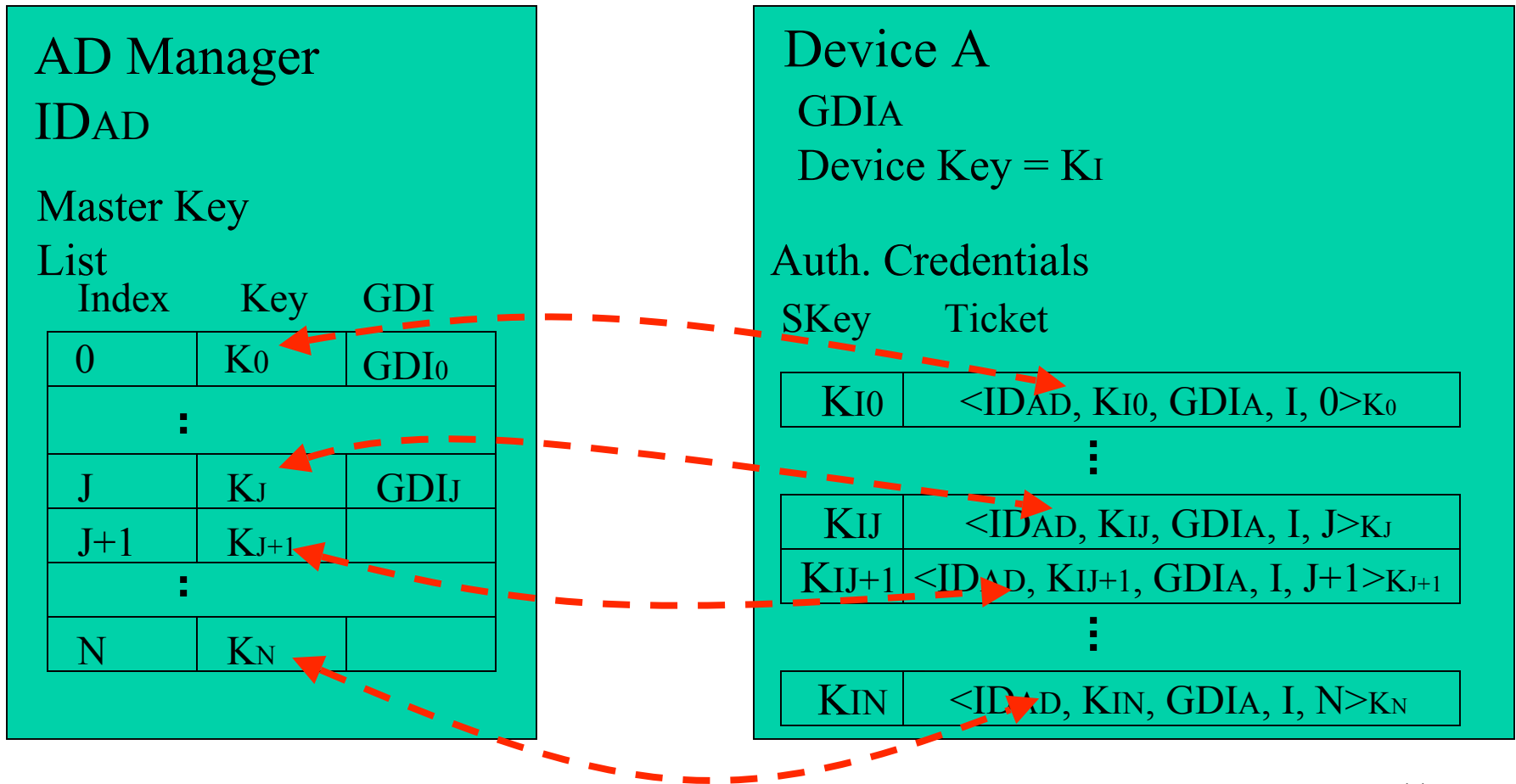


Device Registration



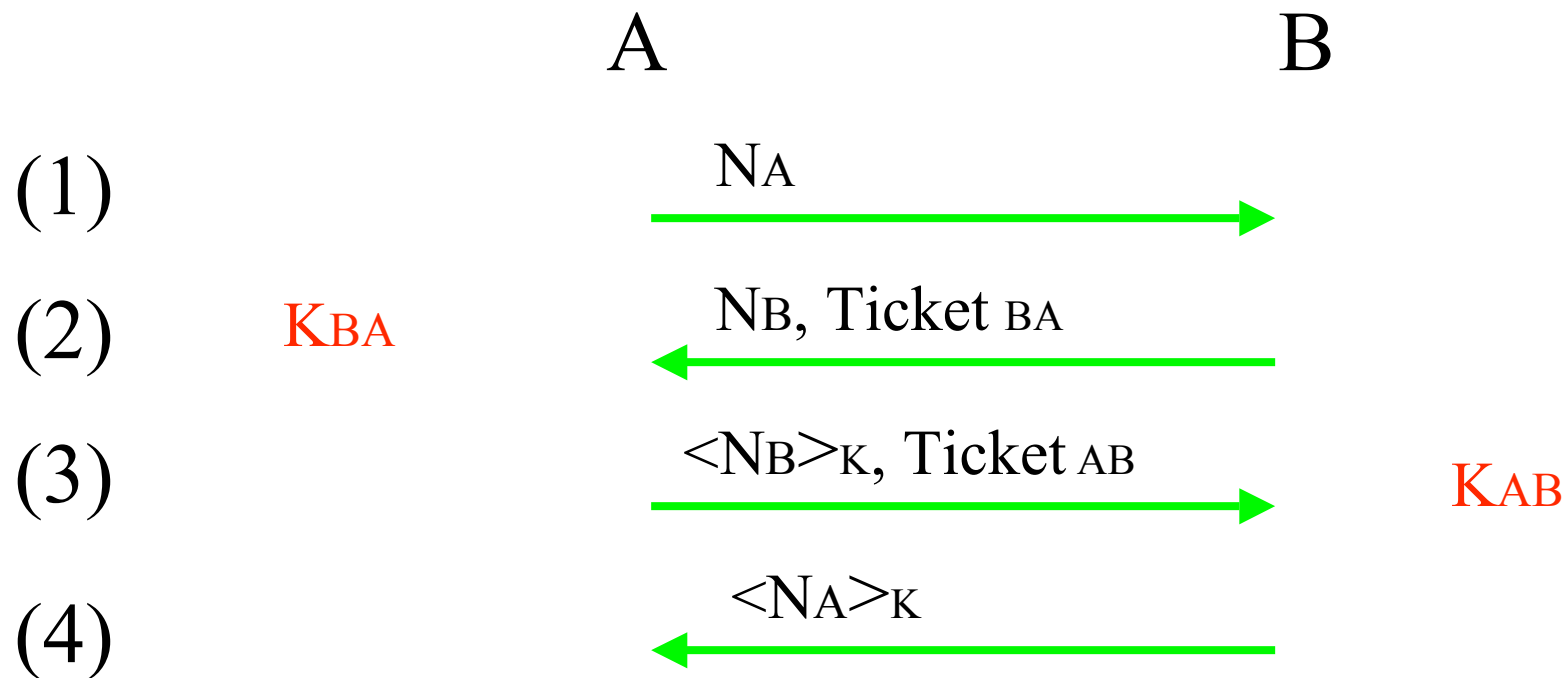


Authentication Credentials





Intra-domain Authentication



$$K = \text{SHA-1}(K_{AB}, K_{BA}, N_A, N_B)$$

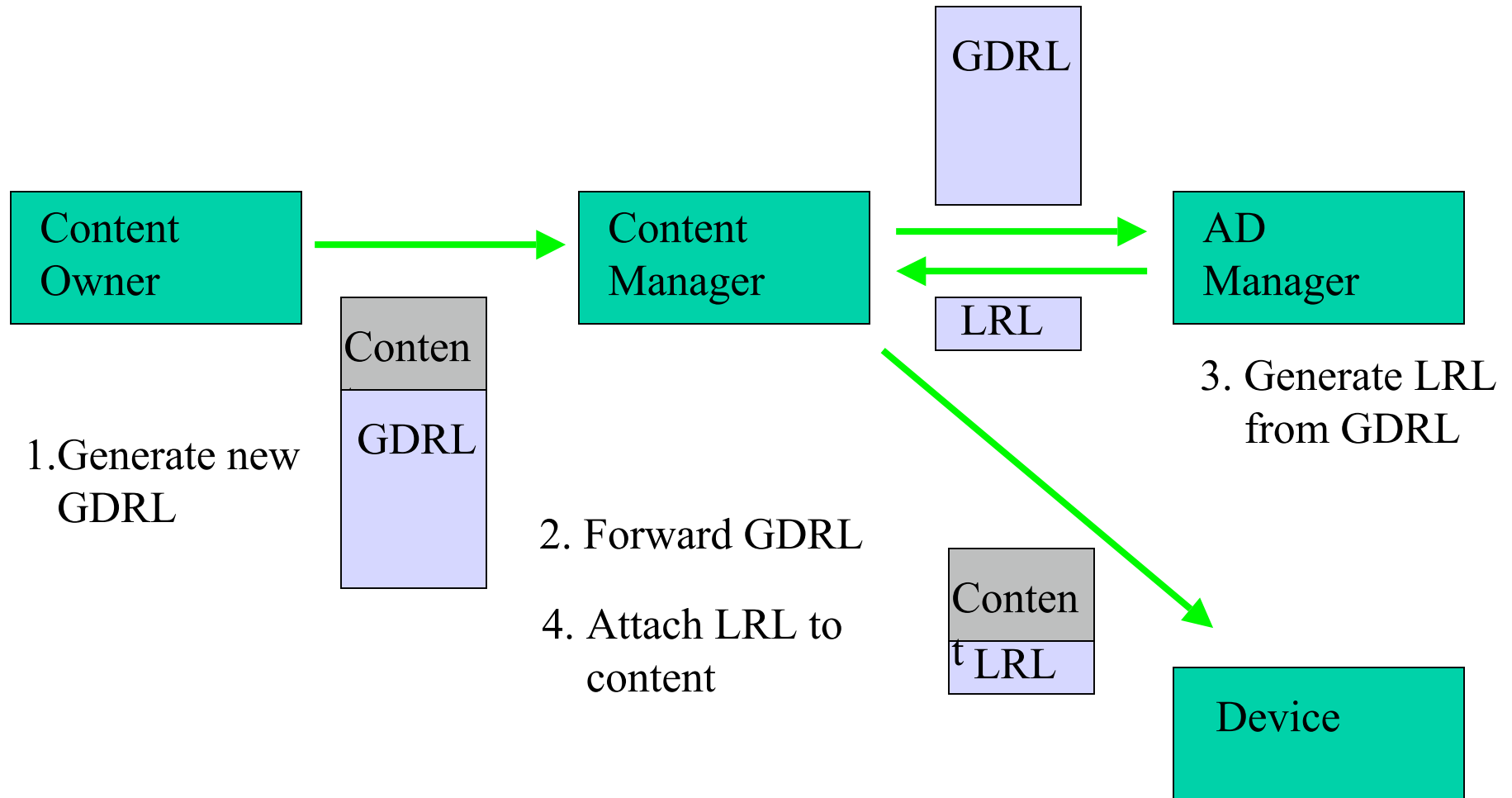


Device Revocation

- GDI of compromised devices published as **GDRL**
 - GDRL can grow very large (> 1MB)
 - Not all devices can process it!
 - Assume domain manager and content managers can deal with it
- Fresh GDRL embedded with content



Device Revocation (2)





Device Revocation (3)

- Local Revocation List (LRL)
 - GDIs of revoked devices **registered with the AD**
 - Much smaller than GDRL (all devices handle it)
 - LRL authentication code for each master key
- Content + LRL = Unrestricted distribution
- Content + GDRL = Restricted distribution



Additional Issues

- Device removal
- AD join/split
- Key update
- Secure content storage



Advantages

- Public key operations only for device registration!
- Crypto hardware accelerators not necessary
- Revocation information can be kept compact
- Continuous network connectivity not necessary



Conclusion

- This is one point in the design space
- By no means the final version of the AD security architecture!
- Feedback please!