Security Guidelines

- Content encryption
  - Content key length
- Forensic Watermarking
  - Operational impacts

Stransky-Heilkron Philippe
Ultra HD Forum Security Work Group
Senior Vice-President and Chief Architect
Nagra Kudelski Group, Switzerland

Content encryption

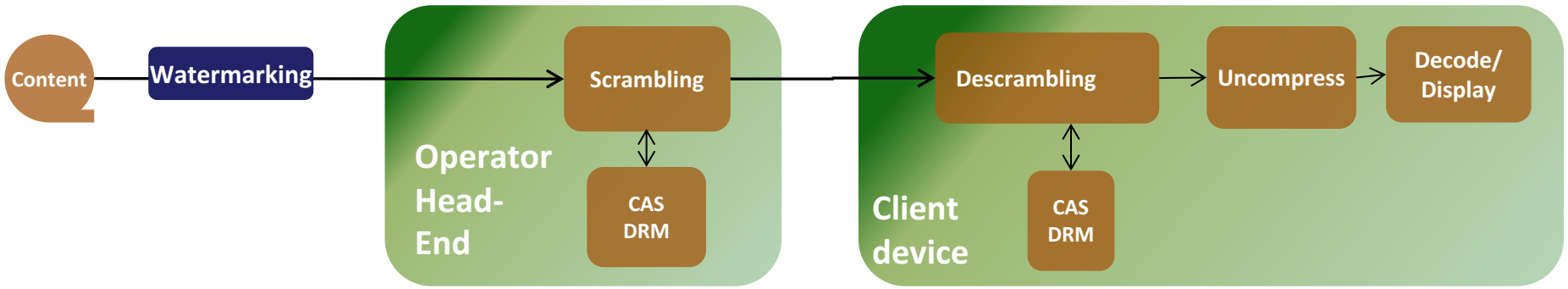
- Content key length should be 128 bits or more
- Algorithms not recommended
  - DES, 3DES are withdrawn from US NIST
  - DVB CSA1 could be reversed in realtime with sufficient but not unreasonable computing resources
- Algorithms recommended
  - AES, DVB-CSA3, DVB CISSA
- DVB CSA2 only during interim period
  - Used mainly for live and linear services
  - Still resistant to sophisticated attacks
  - Can be used while upgrading to DVB CSA3, with crypto-period between 10 and 30 seconds
- Little operational impact for On-Demand services

Forensinc Watermarking

- Helps identifying source of piracy
  - Individualization of copies of video content
  - Imperceptible for a human being
- Various use cases for forensic watermarking
  - Identifying operators
  - Identifying distribution networks
  - Identifying consumer device

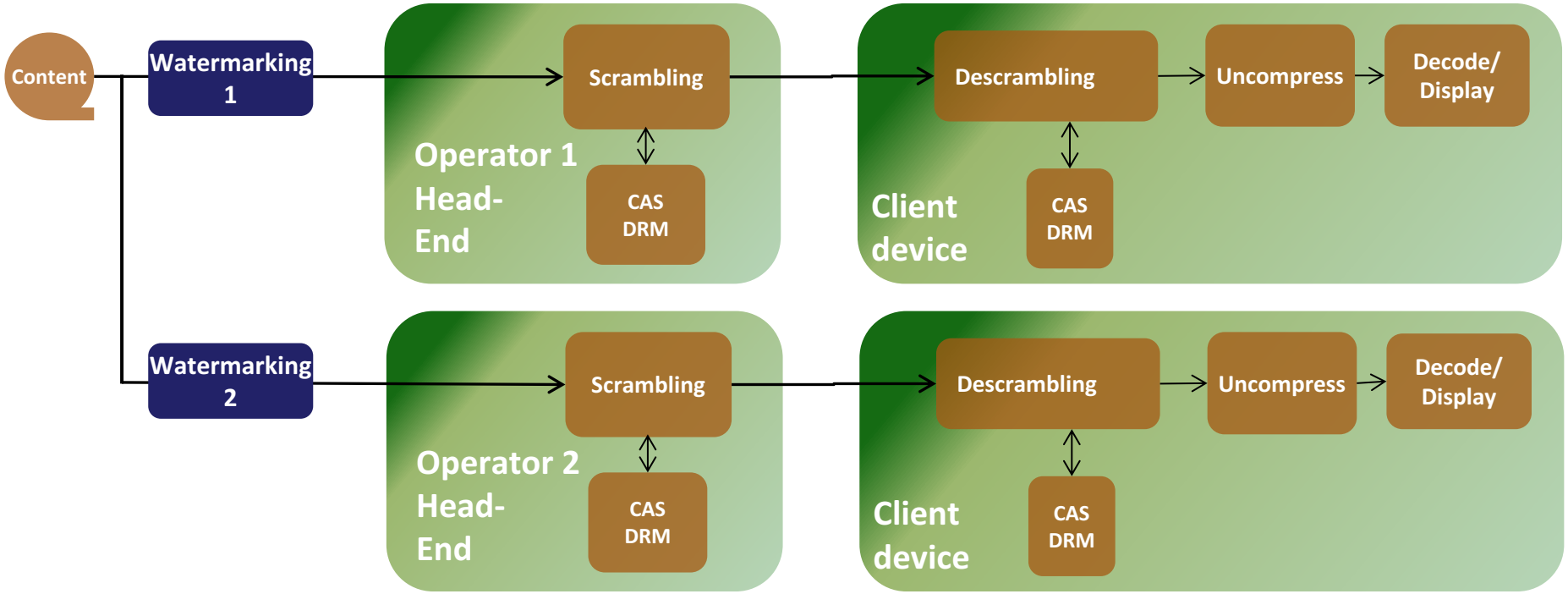
- Note: only high level description is provided here as many solutions are available, with various operational impacts.
  For more details, refer to the Guidelines

Forensic watermarking identifying operators



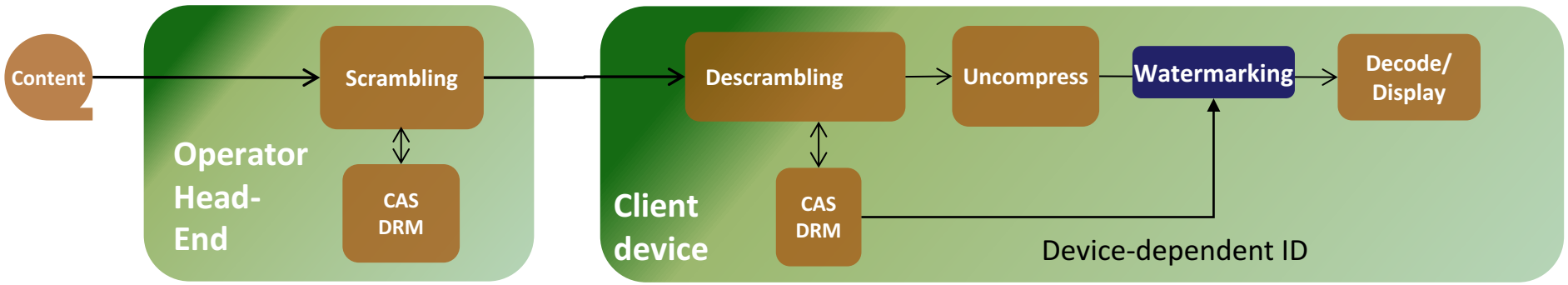
- Identify resellers that have been pirated
- No operational impact on the operator

Forensic watermarking identifying redistribution network



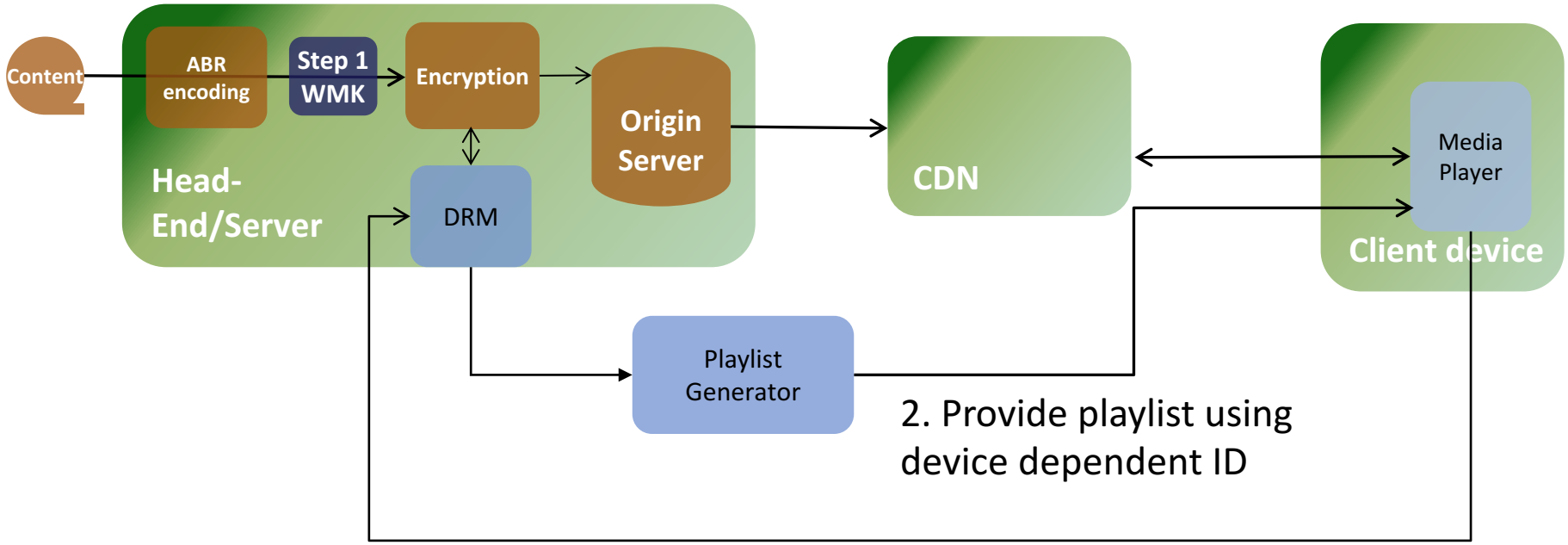
- Identify networks that have been pirated
- No operational impact on the operator

Forensic watermarking identifying consumer devices: 1-step



- Identify source of leakage
- Implementation in client device

Forensic watermarking identifying consumer devices: 2-steps



- Identify source of leakage
- Implementation in server
- Implementation in client device

- Other operational impacts depend on exact implementation

Thank you

- **Stransky-Heilkron Philippe <philippe.stransky@nagra.com>**