S3-030776

Considerations on selective encryption and integrity protection for DRM protected PSS and MBMS media streams

Ericsson

Overview

- Summary
- Collaboration and split of work between OMA and 3GPP SA3/SA4
- Selective encryption and associated issues
- Integrity protection of streams
- Extensions for transport of DRM protected streams
  - File format extensions
  - SRTP transform suitable for DRM
- Conclusions

Summary

- **Approved-announcement sent for draft-ietf-avt-srtp (Proposed Standard)**
  - The IESG has approved the document for publication, and the Secretariat has sent out the official approval message to the RFC editor
  - A publicly scrutinized security protocol is available for streaming protection
  - Ericsson proposes that SA3 should view an existing public review of security protocols and features as a **key factor** in the decision process
- **LS 650 from SA3 to OMA and SA4:**
  - "…SA3 is considering solutions for the encryption and integrity protection of MBMS streaming media and it would be **advantageous to consider alignment** of these solutions (and the associated requirements) with the encryption and integrity protection mechanisms for DRM "
  - Ericsson believes that this is also a **key factor** (as already adopted by SA3) considering the compelling negative impact on the terminal should orthogonal solutions for codecs/security protection be chosen for MBMS and DRM
- **SA3 should adopt the principle that also for DRM Integrity protection should be possible to provide with**

Summary

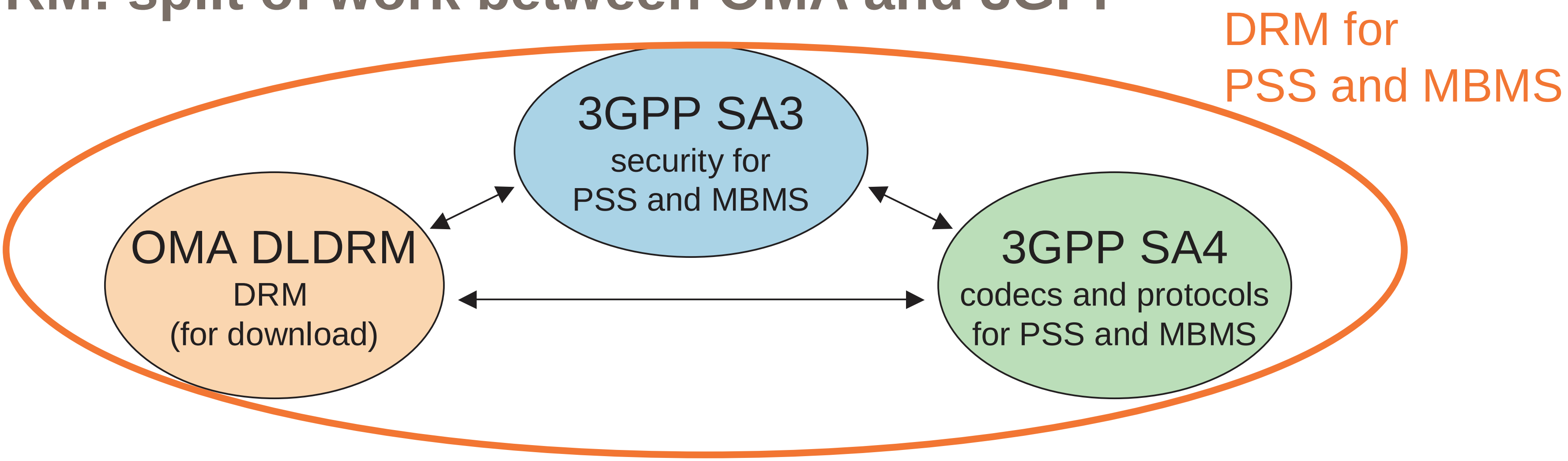
- **Selective encryption creates concerns**
  - Ericsson proposes that SA3 evaluates whether the selective encryption proposal can fulfil the MBMS requirements
  - Privacy concern: It can be possible to link the content with a user for MBMS
  - The potential value with the mechanism from an optimisation point of view is questioned
- **Ericsson proposes a transform of standard SRTP which makes it possible to perform pre-encryption with SRTP for DRM use**
  - This should be a profile that is developed by 3GPP. No further work required in IETF.
  - A proposal is available in the S3-030750 contribution using AES in Counter Mode to this meeting
  - SRTP can fulfil both MBMS and DRM requirements
  - Ericsson is not aware of any security concerns with SRTP whereas some concerns have been raised with the selective encryption approach

Summary

- **Whole solution**
  - Ericsson is proposing that the key management for DRM does not have to be inherited to MBMS services. These technologies are complementary.
  - Ericsson proposes that another **key factor** in the decision process is the availability of a whole solution including a view on protocols and how key management and traffic protection are linked together
- **SA3 should send an LS to SA4 that reflects what is given in this summary and in the Ericsson S3-030750 and S3-030723 contributions**

ERICSSON

DRM: split of work between OMA and 3GPP



- OMA DLDRM concentrates on download DRM (content containers for downloadable objects, DRM key and rights management)
  - OMA DLDRM will adopt the 3GP file format for storage of protected streams and the PSS protected streaming format
  - OMA DLDRM makes a proposal for the protected streaming format in LS S3-030756 (only considering DRM requirements), but will accept what SA3 / SA4 decide/propose
  - Responsibility of SA3/SA4 to consider other requirements and propose a solution that can be used for PSS and MBMS, with and without DRM

Selective Encryption

- Parts (in general packets) of a stream are encrypted, or not
  - Signaled by an encryption flag in the packet
  - Motivation: reduction of computational complexity
  - Typically “intra coded” video frames (I-frames) are encrypted, intermediate predicted frames (P-, B-frames) not
  - OMA DLDRM supports selective encryption (but concerns were expressed in the discussion there)

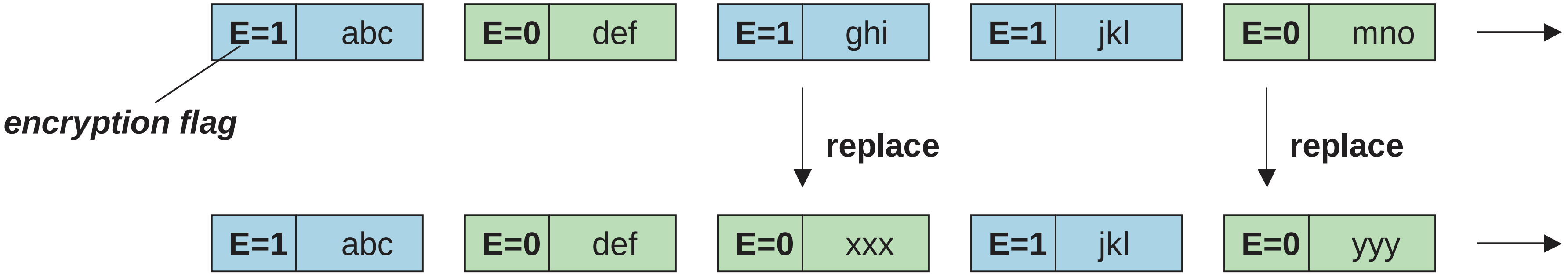
- Streams that are only partially encrypted can be reconstructed with sufficient quality
  - See several scientific papers cited in our input document
  - Often at least possible to understand what the video is about
  - This is a privacy problem

Selective Encryption

- Computational gain is not significant
  - I-frames (that at least need to be encrypted) often make up for 20-40 % of stream rate
  - E.g. Li, Zhang, Tan, Campbell, "Security enhanced MPEG Player", http://choices.cs.uiuc.edu/Papers/Vosaic/se_mpeg_player.pdf, Table 3: encryption of I-frames only decreased the playback speed (in terms of frames per second) of their reference player by 11-16%, encryption of all frames by 14-23%

Selective encryption without integrity protection

- A man-in-the-middle or the legitimate receiver can manipulate the stream
  - Each packet can be replaced by an arbitrary unprotected packet
  - The receiver cannot recognize whether this is the version sent from the content provider, or not



E=1 abc | E=0 def | E=1 ghi | E=1 jkl | E=0 mno

encryption flag

replace **replace**

E=1 abc | E=0 def | E=0 xxx | E=1 jkl | E=0 yyy

  - If there is integrity protection on payload level only, and if integrity is checked for each packet independently of others, packet order can still be modified, or packets replayed
    - Thus, integrity protection must also protect packet headers (packet number, RTP timestamp)

Selective encryption without integrity protection

- “Selective encryption off” must be signaled securely to the receiver
  - If not, a man-in-the-middle can intercept this information and set to “selective encryption on”, and replace packets as described before
  - The secure signaling of DRM information is in general advisable
    - E.g. protection of the URL pointing to the rights issuer that issues OMA rights objects for a stream
  - Can be achieved by protecting stream DRM parameters including “selective encryption on/off” in DRM content container

Using a stream cipher without integrity protection

- The current assumption (based on the liaisons from OMA DLDRM) is that a stream cipher is used for stream encryption
  - This makes modifications trivial
  - This is another good reason for integrity protection

Proposal

- OMA DLDRM are concerned about pirated content, but have not sufficiently considered man-in-the-middle attacks and privacy issues. SA3 should do better.

- Ericsson proposal

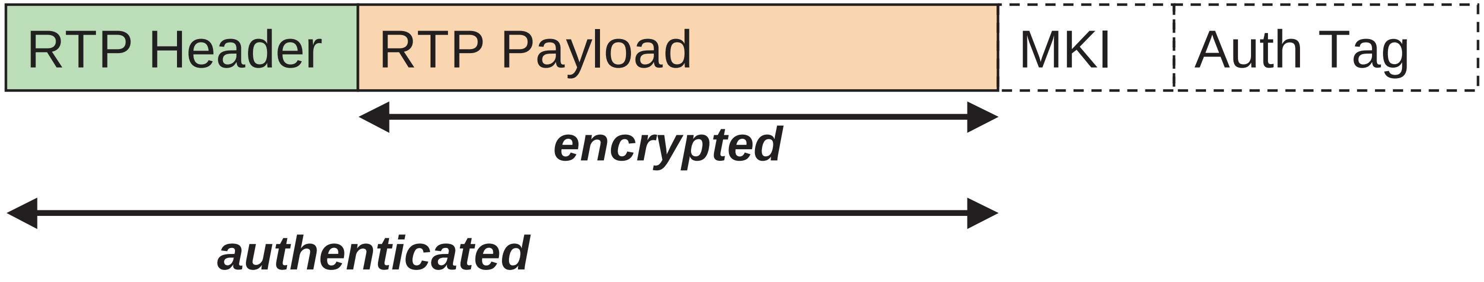
  A. 3GPP should not specify or allow selective encryption for DRM protected streams. (If otherwise, integrity protection of stream and DRM information is essential.)

  B. In general, to avoid e.g. packet replay and allow detection of modifications, 3GPP should specify a mechanism for integrity protection of DRM protected streams (mandatory to implement on servers and clients, optional to use) that integrity protects payload and packet headers

  C. Independently from A. and B., we propose considering the Secure Real-Time Transport Protocol (SRTP) as a possible scrutinized method for integrity and confidentiality protection of streams

SRTP – Secure RTP

- Confidentiality of the RTP payload
  - Default algorithm: AES in Counter Mode, 128 bits key
- Integrity protection of the entire RTP packet & replay protection (optional)
  - Default algorithm: HMAC-SHA1, 128 bits key
- MasterKey Identifier (optional), signals which key to use



IETF draft, approved (Minneapolis) **to become Proposed Standard**

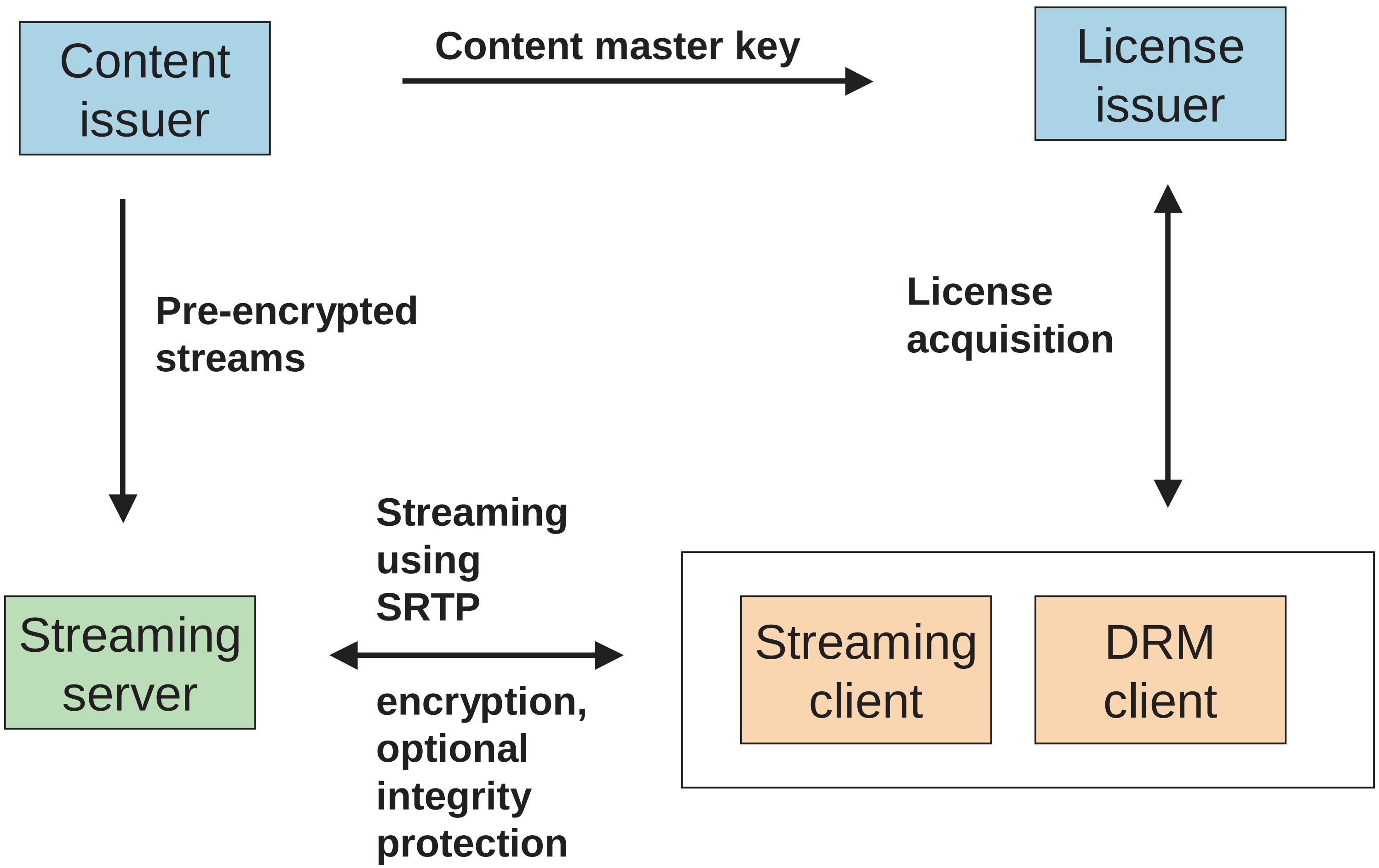
SRTP is a *framework*

- Allows definition of new cryptographic transforms

- Default transform:
  - Encryption/authentication on-the-fly
  - Counter (for AES) derived from RTP headers
  - Does not allow pre-encryption of streams

- New transform detailed in the Ericsson input
  - Complies with the SRTP framework
  - Using default algorithms
  - Explicit counter for AES
  - Allows pre-encryption of streams

Scenario


Content issuer
Content master key
License issuer
Pre-encrypted streams
License acquisition
Streaming using SRTP
encryption, optional integrity protection
Streaming server
Streaming client
DRM client

SRTP advantages

- Extensive security review in IETF
- Approved to become Proposed Standard
- Key establishment of shared keys for **both** encryption and optional integrity protection through the content master key

File format changes

- This attachment was sent FYI and shall be submitted to SA4
  - Changes on the 3GP file format to support storage of encrypted streams, and DRM information
  - 3GP file is the storage format between content provider and streaming server (backend)
  - On content provider discretion, 3GP file can also be downloaded to the client

Conclusions

- OMA DLDRM has proposals concerning protection of 3GPP streams (see S3-030756 and 758), but does not consider all 3GPP relevant requirements including the MBMS considerations as highlighted in the LS 650
- OMA DLDRM has declared it will accept the 3GPP solution for protected 3GP file format and protected streaming format

- Selective encryption is technical legacy and poses problems
- Stream encryption without integrity protection poses problems as well
- Combination of both accumulates problems

- Proposal:
  - Don’t use selective encryption
  - Use integrity protection for DRM protected streams
  - SRTP could be used for protection of PSS and MBMS streams