

Meeting notes: Dec 14, 2010

Attending:

- Azuki - Rob Sowers
- Pelco - Farzin Aghdasi
- BuyDRM - Christopher Levy
- Verimatrix - Tom Pollard, Steve Christian
- Wowza - Charlie Good , Alex Dobrushin
- MediaExcel - Nikos Kyriopoulos , Patrick Mechali
- Harmonic - Moore MacAulay
- VCF – Daniel Bar-Lev

Discussion:

- Should it be called the Scrambler or Packager. It seems to be industry dependent, to some extent. There seemed to be a general preference for Scrambler, with BuyDRM pushing for Packager but willing to live with it. Issue can be reopened if using 'Scrambler' is confusing for people.
- Authentication:
 - Agreed to have a framework allowing multiple authentication mechanisms between the scrambler and KMS, who should negotiate on which scheme they will use.
 - What are the most popular methods of authentication and include provisions to support these.
- Discussion on using the same key for multiple delivery protocols – this may enable reuse of encrypted data by the Scrambler. Doing this means either that the client tells the KMS that it doesn't need a key (because it has one from a previous request, made for use with another protocol), or that the keys are generated at the Scrambler and sent to the KMS.
- Discussion on KMS latency – decided to just ignore the issue.
- Clarification that the Scrambler is the 'master' (makes the initial request, determines key duration, determines which KMS is primary and which is redundant, etc) and the KMS is the server in the client/server model.
-