

DIGITAL RIGHTS MANAGEMENT USING TRUSTED PROCESSING TECHNIQUES

ABSTRACT

The present invention discloses several methods to strengthen the integrity of entities, messages, and processing related to content distribution as defined by the Open Mobile Alliance (OMA) Digital Rights Management (DRM). The methods use techniques related to the Trusted Computing Group (TCG) specifications. A first embodiment uses TCG techniques to verify platform and DRM software integrity or trustworthiness, both with and without modifications to the DRM rights object acquisition protocol (ROAP) and DRM content format specifications. A second embodiment uses TCG techniques to strengthen the integrity of ROAP messages, constituent information, and processing without changing the existing ROAP protocol. A third embodiment uses TCG techniques to strengthen the integrity of the ROAP messages, information, and processing with some changes to the existing ROAP protocol.

Fig. 7