G00001

162162

ABSTRACT

Technology for suppressing the data volume of a TRL (terminal revocation list), which is information specifying terminals to be invalidated, in a system structured from a plurality of terminals, a distribution device for acquiring the TRL and distributing data to only those terminals that are not to be invalidated, and a management device for generating the TRL. This object is realized by a system structured from a management device, a content key distribution device and a plurality of terminals. The management device generates and transmits a TRL formed from data that expresses terminal IDs of all terminals to be invalidated (i.e. terminals whose IDs have a common bit string), by only a value and a position of the common bit string in the IDs, to the content key distribution device. Each terminal holds a terminal ID that includes a manufacturer ID, a serial number and the like, and requests the distribution of a content key by sending the terminal ID to the content key distribution device. The content key distribution device refers to the TRL, judges whether the terminal ID transmitted from the terminal is that of an invalidated terminal, and if negative, encrypts and transmits the content key to the terminal.