## ABSTRACT

The objective of the present invention is to allow the domestic transmission of encrypted data with conditional access without limitation of the type of terminal used, at the same time guaranteeing that this transmission will not be able to go beyond this limit.

This objective is achieved by a transmission method of encrypted data between a local server connected to one or several local peripherals, said local server comprising security means in charge of acquiring a first right of use of these data, characterised in that it consists in:

- transmitting the encrypted data from the local server towards a peripheral,
- extracting from the first right a second right corresponding to the part necessary for the decryption of the data in the peripherals,
- encrypting by the security module the second right by means of a pairing key specific to the couple formed by the security module of the local server and the security module of the peripheral,
- transmitting this encrypted second right to the local peripheral,
- decrypting with the help of the pairing key the second right by the security means of the peripheral,
- decrypting by the peripheral the data encrypted by the second right.

*162162*

*G00002*